Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume III, 349-354

Empirical Study of Incident Response Practices for Personal Data Breaches in Bulgarian Organizations

Martin Zahariev
Faculty of Information Sciences, National Security Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
m.zahariev@unibit.bg

Daniela Pavlova
Faculty of Information Sciences, Computer Sciences Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
d.pavlova@unibit.bg

Panayot Gindev
Information Systems and Technologies Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
p.gindev@unibit.bg

George Dimitrov
Faculty of Information Sciences, Computer Sciences Department
University of Library Studies and Information Technologies
Sofia, Bulgaria
g.g.dimitrov@unibit.bg

Vyara Savova
University of Library Studies and Information Technologies
Sofia, Bulgaria
vyara.savova@yahoo.com

Radoslava Makshutova
Institute for the State and the Law Bulgarian Academy of Sciences
Sofia, Bulgaria
r.makshutova@gmail.com

***Abstract*—This paper presents an empirical study of incident response practices related to personal data breaches in Bulgarian organizations. The study examines how organizations detect, assess, and manage incidents involving personal data in accordance with personal data protection requirements. The research is based on data collected through a survey conducted among organizations from different economic sectors in Bulgaria. The analysis focuses on the existence of internal incident response procedures, the level of organizational preparedness, and the awareness of obligations arising from personal data breach incidents. The results reveal differences among organizations in terms of organizational measures, staff training, and incident management practices. Based on the analysis, conclusions are drawn regarding the implementation of incident response procedures and the management of personal data breach incidents in an organizational environment.**

Keywords—data protection, incident management, incident response, personal data breach.

I. INTRODUCTION

In the contemporary digital environment, organizations process and store substantial volumes of personal data as part of their operations. The use of information systems, electronic services, and various technological solutions enhances the capabilities for data exchange and processing, while simultaneously creating conditions for the occurrence of incidents related to personal data breaches. Such incidents may result in unauthorized access, loss, disclosure, or misuse of information containing personal data.

Under these conditions, organizations are required to implement appropriate organizational and technical measures to prevent and manage such incidents. These measures include the development of internal incident response procedures, staff training, and the implementation of mechanisms for the detection and analysis of personal data breaches. The management of such incidents necessitates clearly defined processes for identification, assessment, and response in the event of a breach.

The present study aims to analyze incident response practices related to personal data breaches in Bulgarian organizations. The study is based on data collected through a survey and examines issues related to the existence of incident response procedures, organizational preparedness, and approaches to managing such situations. The obtained results make it possible to identify observed practices and to draw conclusions regarding how organizations approach the management of personal data incidents.

A. Literature Review

The primary legal framework governing the management and notification of personal data breaches in the European Union is Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), which defines the

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol3.70

concept of a "personal data breach" and establishes the obligation to notify the supervisory authority within 72 hours where there is a risk to the rights and freedoms of natural persons, as well as the requirement to internally document all identified breaches [1]. The guidelines of the European Data Protection Board (EDPB) further complement this framework by specifying the criteria for determining risk and high risk, the content of notifications, and the point at which the controller is considered to have become aware of a breach [2]. In addition, example breach scenarios—such as ransomware attacks, data leaks, human error, and lost devices—are examined to support organizations in risk assessment and decision-making regarding notification to supervisory authorities and affected individuals [3]. Practical application of these requirements can also be observed in the guidance issued by national supervisory authorities, where the minimum elements of internal documentation and the possibility of phased information provision during notification are outlined [4].

Incident response is also considered an organizational and technological process encompassing preparation, detection, containment, recovery, and post-incident analysis of root causes. In this context, the incident management framework of the National Institute of Standards and Technology (NIST) conceptualizes incident response as part of broader cybersecurity risk management activities and emphasizes the need for clearly defined roles, coordination among involved teams, and established mechanisms for communication and accountability [5]. In parallel, studies by the European Union Agency for Cybersecurity (ENISA) indicate that data security breaches often result from both malicious actions and human error, while delayed detection and limited visibility into incidents hinder their containment and subsequent recovery [6]. These findings suggest that effective incident response requires a combination of technical monitoring mechanisms and organizational procedures for incident management and reporting.

The scientific literature in the field of incident management indicates that organizational practices can be structured into phases encompassing preparation, response, and subsequent process improvement in incident management [7]. Despite the existence of established models and recommended practices, a number of studies note that their implementation within organizational environments is often uneven and accompanied by practical challenges. In the Bulgarian context, examples of formalized internal procedures for managing personal data breaches can also be identified, introducing criteria for risk assessment, breach categorization, and internal reporting mechanisms [8]. Nevertheless, the extent to which organizations in Bulgaria maintain consistent processes that integrate technical incident response with risk assessment and notification decision-making in the event of personal data breaches remains an open question. This gap highlights the need for empirical research into organizational practices in this area.

From a comparative perspective, the 72-hour notification deadline is a common GDPR requirement, but the practical tools for submitting notifications vary among national supervisory authorities. The European Data Protection Board (EDPB) maintains a consolidated page with guidance on notifying data breaches to the competent data protection authority [9]. In Ireland, the Data Protection Commission (DPC) requires breach notifications to be submitted through a dedicated Breach Notification Form and asks controllers to identify cross-border breaches in the relevant part of the form [10]. In France, the Commission nationale de l'informatique et des libertés (CNIL) emphasizes internal documentation, notification to the supervisory authority within 72 hours where there is a risk, and communication to data subjects where the risk is high [11]. In Spain, the Agencia Española de Protección de Datos (AEPD) provides guidance on risk assessment and indicates that notification to the supervisory authority is required where a risk exists and must be made within 72 hours [12]. These examples show that the need for clear forms, guidance, and practical decision-support tools is not specific to Bulgaria, although the present findings indicate that this need is especially visible among Bulgarian organizations.

II. Materials and Methods

The present study was conducted within the framework of a research initiative aimed at analyzing organizational practices in incident response related to personal data breaches.

To collect empirical data, a standardized survey method was employed. A structured questionnaire was used, comprising closed-ended, semi-closed, and a limited number of open-ended questions. The questions were designed to identify organizational practices regarding internal reporting, risk assessment, the existence of incident response procedures, the application of guidelines and methodological documents, as well as the perception and use of available tools for incident notification and management.

The study included 49 valid responses from representatives of various types of organizations. These comprised private for-profit organizations, public institutions, non-profit organizations, as well as external consultants acting on behalf of specific organizations. In terms of organizational size, micro, small, medium, and large enterprises were represented, including a significant proportion of organizations with more than 250 employees. This diversity allows for observations to be made both with regard to organizational type and the scale of operations.

The participants were reached through a purposive, non-probability dissemination of the questionnaire among professional groups and individuals involved in personal data protection, legal compliance, information security, and incident response. The target audience included Data Protection Officers, legal advisers, lawyers, consultants, information technology specialists, and other persons involved in data protection processes within organizations. Because the questionnaire was distributed through

professional contacts and could be further forwarded, the exact number of persons reached by the invitation cannot be determined. Therefore, a response rate was not calculated. The 49 valid responses are treated as a sufficient empirical basis for an exploratory analysis of observed practices, difficulties, and tendencies, but not as a nationally representative sample.

The questionnaire was designed for the purposes of the present exploratory study and was structured around several thematic groups. The first group included questions related to the general profile of the organization. The second group focused on the existence of internal rules, procedures, and mechanisms for responding to incidents involving personal data. The third group addressed awareness and application of guidelines, recommendations, and methodological documents. The fourth group examined practical aspects of notification, internal coordination, and the perceived applicability of available tools. The final section provided respondents with the opportunity to offer additional comments and recommendations.

The present paper examines the results of the survey conducted among Bulgarian specialists and representatives of organizations involved in personal data protection, with a focus on the preparedness of organizations in Bulgaria to respond to personal data breaches. A separate survey among foreign specialists from other European Union Member States is planned within the broader research work. At the time of preparing this manuscript, that survey had not been completed; therefore, its results are not included in the present analysis. Consequently, the comparative observations in this paper are limited to publicly available guidance and procedures of selected supervisory authorities.

Data processing was conducted using descriptive analysis based on the frequency distribution of responses and comparisons across different groups of respondents. The analysis was aimed at identifying recurring patterns in organizational practices, differences among categories of organizations, and areas where challenges, insufficient awareness of procedures, or a lack of clearly defined internal mechanisms are observed.

In addition to the frequency-based presentation of the results, basic statistical checks were carried out for selected survey indicators. Their purpose is to show which observed proportions are clearly high or low. These checks are complementary and should be interpreted cautiously due to the limited sample size.

III. Results and Discussion

The conducted survey includes 49 valid responses from representatives of organizations with diverse profiles and scales of operation. The sample is predominantly composed of public organizations (49.0%) and private for-profit organizations (40.8%), while in terms of size, the largest share is represented by organizations with 250 or more employees (59.2%). This distribution allows for the examination of incident response practices in organizations where personal data processing is relatively well institutionalized and presupposes the existence of internal rules, defined responsibilities, and a more structured management framework. The profile of the sample is summarized in Table 1.

TABLE I. SAMPLE PROFILE (N = 49)

Group	Category	n	%
Type of organization	Public organization	24	49.0
	Private for-profit organization	20	40.8
	Other profiles	5	10.2
Size of organization	250 or more employees	29	59.2
	50–249 employees	12	24.5
	Other sizes	8	16.3

At the level of formal organizational preparedness, the results indicate a relatively good degree of initial compliance with personal data protection requirements. The presence of a Data Protection Officer was reported in 69.4% of organizations, 65.3% indicated that they have a designated individual or team responsible for incident response, 93.9% stated that they are familiar with the definition of a personal data breach under the GDPR, and 83.7% correctly recognized that all scenarios listed in the survey may constitute such a breach. These findings suggest that baseline regulatory awareness is relatively high and that, in a significant proportion of organizations, the minimum structural prerequisites for incident response have already been established. At the same time, the mere existence of formal mechanisms is not sufficient to conclude that a uniformly high level of practical preparedness is in place.

A more detailed examination of organizational and technical measures reveals a more heterogeneous picture. The highest values are observed in the implementation of technical measures such as encryption, network security, and access control (87.8%), as well as in restricting access based on job roles (79.6%). Relatively strong results are also recorded in the clear classification of sensitive data (73.5%), employee training to recognize and report potential breaches (71.4%), maintenance of records of processing activities (67.3%), and the existence of a written incident response plan (63.3%). In contrast, the more operational elements of preparedness remain significantly less developed. Only 53.1% of organizations use a system for incident logging and tracking, 51.0% conduct regular cybersecurity testing, 46.9% have a system for monitoring access to sensitive data, 42.9% use Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDS)-type solutions, and only 26.5% carry out simulations or training exercises based on breach scenarios. This disparity indicates that, in many organizations, documented compliance measures are in place, but far fewer have been translated into regularly tested and repeatable practical response mechanisms. The main indicators of formal and operational preparedness are summarized in Table 2.

TABLE II. MAIN INDICATORS OF FORMAL AND OPERATIONAL PREPAREDNESS

Indicator	n	%
Presence of a Data Protection Officer	34	69.4
Designated individual/team for incident response	32	65.3
Existence of a written incident response plan	31	63.3
Employee training to recognize and report breaches	35	71.4
Implementation of appropriate technical security measures	43	87.8
Access restriction based on job roles	39	79.6
Incident logging and tracking system	26	53.1
Regular cybersecurity testing	25	51.0
Monitoring of access to sensitive data	23	46.9
Use of SIEM/IDS-type solutions	21	42.9
Simulations/training exercises	13	26.5

The results of the basic statistical checks are presented in Table 3.

TABLE III. BASIC STATISTICAL CHECKS FOR SELECTED INDICATORS

Indicator	Result
GDPR breach definition	46/49 (93.9%) CI 83.5-97.9 p<0.001
Technical security measures	43/49 (87.8%) CI 75.8-94.3 p<0.001
72-hour deadline awareness	35/49 (71.4%) CI 57.6-82.2 p=0.004
Simulations/training exercises	13/49 (26.5%) CI 16.2-40.3 p=0.001
Use of Guidelines 9/2022	7/49 (14.3%) CI 7.1-26.7 p<0.001
Notification of data subjects	4/49 (8.2%) CI 3.2-19.2 p<0.001

Note: CI denotes a 95% confidence interval calculated using the Wilson score method. Exact binomial tests were used as exploratory checks against a reference proportion of 0.50. Due to the limited and non-probability sample, the results should be interpreted cautiously.

The basic statistical checks are consistent with the descriptive findings. Indicators such as familiarity with the GDPR breach definition, the implementation of technical measures, and awareness of the 72-hour notification deadline show clearly high values. In contrast, indicators such as simulations, the practical application of Guidelines 9/2022, and actual notification of data subjects show clearly low values. This supports the conclusion that organizations are more likely to have baseline legal and technical preparedness than tested practical response mechanisms.

Responses related to actual incident experience and notification obligations further confirm this trend. Only 24.5% of respondents indicate that incidents involving potential personal data breaches have occurred in their organizations over the past two years, while 22.4% report that they are unable to assess whether such cases have taken place. At the same time, 71.4% are aware of the 72-hour notification deadline, 65.3% report the existence of a written procedure or policy for notifying the Commission for Personal Data Protection (CPDP), and 79.6% recognize that, under certain conditions, affected data subjects must also be notified. However, only 8.2% indicate that notification of data subjects has actually been carried out in practice within their organizations. The contrast between the relatively broad awareness of legal requirements and the more limited practical experience suggests that organizations appear better prepared to describe the applicable rules than to execute the full sequence of actions in real situations characterized by tight deadlines, incomplete information, and the need for rapid internal coordination. In the same direction, 67.3% consider a standardized template for notifying data subjects of a breach to be necessary. Key indicators related to notification are summarized in Table 4.

TABLE IV. NOTIFICATION PRACTICES IN THE EVENT OF A SECURITY BREACH

Indicator	n	%
Organizations with incidents in the past two years	12	24.5
Awareness of the 72-hour notification deadline	35	71.4
Written procedure/policy for notification to the Commission for Personal Data Protection	32	65.3
Awareness of the obligation to notify data subjects	39	79.6
Actual notification of data subjects in practice	4	8.2
Need for a standardized notification template	33	67.3

Particularly indicative are the results concerning awareness and application of Guidelines 9/2022 of the European Data Protection Board and the methodology of the Commission for Personal Data Protection for determining the level of risk in personal data breaches. Partial or full awareness of Guidelines 9/2022 was reported by 69.4% of respondents; however, only 14.3% have actually used them in incident notification. Nevertheless, among those who are at least partially familiar with the Guidelines, 76.5% consider them useful, and the same proportion indicate the need for additional practical guidance from the national supervisory authority. Even more indicative are the findings related to the methodology of the Commission for Personal Data Protection. Only 46.9% are aware of its existence and content; among them, 47.8% perceive it as useful, 56.5% believe that it should be revised and simplified, 73.9% indicate the need for additional explanations and training, 91.3% would participate in specialized training, and 95.7% regard the publication of such a methodology as a useful initiative. These results suggest that the issue does not lie in the rejection of methodological and regulatory instruments, but rather in their limited practical applicability and the need to translate them into more accessible procedures, examples, and actionable models. The data on the guidelines, the methodology, and the expressed need for additional support are summarized in Table 5.

TABLE V. GUIDELINES 9/2022, METHODOLOGY OF THE COMMISSION FOR PERSONAL DATA PROTECTION AND NEED FOR ADDITIONAL SUPPORT

Indicator	n	%
Awareness (at least partial) of Guidelines 9/2022	34/49	69.4
Application of Guidelines 9/2022 in incident notification	7/49	14.3
Perception of Guidelines 9/2022 as useful (among those aware)	26/34	76.5
Awareness of the methodology of the Commission for Personal Data Protection	23/49	46.9
Perception of the methodology as useful (among those aware)	11/23	47.8
Opinion that the methodology should be simplified	13/23	56.5
Indicated need for additional training	17/23	73.9
Willingness to participate in specialized training	21/23	91.3
Perception of the publication of the methodology as a useful initiative	22/23	95.7

Additional questions related to training, resources, and self-assessment of preparedness further confirm the existence of a clear distinction between basic and advanced organizational readiness. Regular training on GDPR and incident response is conducted in 53.1% of organizations, onboarding training on personal data protection for new employees is provided in 59.2%, cybersecurity training for information technology (IT) teams is implemented in 57.1%, and two-factor authentication is used in 63.3% of cases. At the same time, simulations and training exercises are conducted comprehensively in only 26.5% of organizations. Self-assessment of preparedness also reveals differences across employee groups. The highest level of preparedness is attributed to IT teams, with 73.5% rating their level as "good" or "very good," followed by legal departments and consultants at 59.2%, while among other employees handling personal data this share is significantly lower, at 42.9%. Furthermore, 65.3% of respondents do not consider the public and private sectors to be equally well prepared, 75.5% indicate that their organizations follow news and guidance on the topic, and 79.6% express the need for more practical examples from competent authorities. These findings suggest that the most vulnerable aspect of incident response is not solely the technical infrastructure, but the organization's ability to consistently apply knowledge across all units.

In summary, the obtained results suggest that Bulgarian organizations demonstrate a relatively high level of formal awareness regarding personal data breaches; however, this awareness is not equally supported by a well-developed level of practical preparedness. A clear discrepancy exists between the presence of basic legal knowledge and documented internal rules, on the one hand, and the ability to ensure a rapid, coordinated, and procedurally sound response to actual incidents, on the other. This finding is consistent with the scientific and applied literature discussed in the theoretical section, which emphasizes that effective incident response extends beyond formal compliance and requires preparation, internal coordination, monitoring, training, testing, and subsequent organizational analysis. The empirical results indicate that the main challenges lie precisely at the level of operational execution and practical implementation, highlighting the need for clearer procedures, practical guidance, and more targeted training initiatives.

IV. CONCLUSIONS

The present study demonstrates that Bulgarian organizations exhibit a relatively good level of initial awareness regarding personal data breaches and the key obligations arising from the applicable legal framework. A significant proportion of organizations have appointed a Data Protection Officer, have defined internal responsibilities, implement technical security measures, and are aware of their obligations to notify the supervisory authority. At the same time, however, the results clearly indicate that practical preparedness for incident management remains unevenly developed. The less developed elements are precisely those that transform formal compliance into an effective response capability—namely, incident tracking systems, access monitoring, regular testing, simulations, practically applicable methodologies, and adequately trained personnel beyond specialized legal and IT functions.

The obtained data provide grounds to conclude that the main issue is not the absence of a regulatory framework or a complete lack of awareness, but rather the difficulty in translating requirements into clear internal actions and consistent organizational practices. Particularly indicative in this regard are the limited practical application of Guidelines 9/2022, the low level of awareness of the methodology of the Commission for Personal Data Protection, and the clearly expressed need for additional explanations, templates, practical guidance, and training.

Therefore, it can be argued that organizations require not only legal information, but also an applicable response model that integrates early incident detection, risk assessment, internal role allocation, documentation, notification, and post-incident analysis into a coherent and consistent process.

Several limitations should be noted. First, the sample includes 49 valid responses and has a non-probability character; therefore, the results should not be interpreted as nationally representative of all organizations in Bulgaria. Second, due to the dissemination procedure, the exact number of persons reached by the invitation cannot be determined, and a response rate was not calculated. Third, the data are based on respondents' self-assessment, which means that differences may exist between declared practices and actual organizational behavior during a specific incident. Despite these limitations, the results provide a useful empirical basis for identifying recurring difficulties and for formulating subsequent recommendations for managing responses to personal data breaches.

Nevertheless, the conducted research provides a valuable empirical basis for the formulation of future

recommendations, the development of practically oriented models for responding to personal data breaches, and further comparative studies on the characteristics of national notification procedures across different European Union Member States. In this sense, the study fulfills its primary scientific objective—to identify key challenges in organizational practice and to indicate directions for the development of more effective solutions for managing incidents involving personal data.

ACKNOWLEDGMENTS

The present paper was prepared as a result of the scientific research activities conducted within the scientific project "Managing Personal Data Breach Response Processes in the Activities of Organisations in the Republic of Bulgaria," financed by the Bulgarian National Science Fund under the "Competition for financing fundamental scientific research – 2024," Contract No. КП-06-Н85/10 (BG-175467353-2024-11-0016-C01), dated 05.12.2024.

REFERENCES

[1] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 (General Data Protection Regulation)," *Official Journal of the European Union*, Apr. 27, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[2] European Data Protection Board, "Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0," Mar. 28, 2023. [Online]. Available: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

[3] European Data Protection Board, "Guidelines 01/2021 on examples regarding personal data breach notification, Version 2.0," Dec. 14, 2021. [Online]. Available: https://www.edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

[4] Commission Nationale de l'Informatique et des Libertés, "Notify a personal data breach," May 24, 2018. [Online]. Available: https://www.cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles

[5] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile," *NIST Special Publication 800-61r3*, Apr. 2025. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[6] European Union Agency for Cybersecurity, "ENISA threat landscape 2020 – data breach," Oct. 20, 2020. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20Data%20Breach%20A4.pdf

[7] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Computers & Security*, vol. 45, pp. 42–57, 2014, doi: 10.1016/j.cose.2014.05.003.

[8] Supreme Court of Cassation of the Republic of Bulgaria, "Actions in case of a personal data security breach," internal procedure, 2023. [Online]. Available: https://www.vks.bg/dokumneti-zzld/vks-zapoved-2023-808-procedura-narushenie.pdf

[9] European Data Protection Board, "How to notify a data breach to your Data Protection Authority (DPA)," n.d. [Online]. Available: https://www.edpb.europa.eu/notify-data-breach_en

[10] Data Protection Commission, "Breach Notification," n.d. [Online]. Available: https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification

[11] Commission Nationale de l'Informatique et des Libertés, "Cybersecurity 2024," 2024. [Online]. Available: https://www.cnil.fr/sites/cnil/files/2024-05/cnil_cybersecurity_2024_en.pdf

[12] Agencia Española de Protección de Datos, "Notification of a personal data breach to the Supervisory Authority," Dec. 11, 2025. [Online]. Available: https://www.aepd.es/en/rights-and-duties/fulfill-your-duties/measures-compliance/notification-of-personal-data-breach-to-the-supervisory-authority