Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume V, 353-361

Key Takeaways from the Most Significant GDPR Personal Data Breaches in the Republic of Bulgaria

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

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

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*—The present research paper focuses on the most significant personal data breaches under the EU General Data Protection Regulation 2016/679 (GDPR) that took place in the Republic of Bulgaria since the GDPR became applicable in 2018. These include *inter alia* the data breaches that affected the National Revenue Agency, the Bulgarian Posts, one of the Bulgarian banks and other organizations from the public and the private sector. The analysis of these cases is important, because they had an impact on thousands and sometimes millions of people and resulted in severe sanctions reaching thousands and sometimes millions of Bulgarian leva. This problem is especially relevant in the modern information society where the collection and processing of data are fundamental for the economic growth and societal well-being. By examining the available public documentary sources on these cases such as the practice of the Bulgarian Commission for Personal Data Protection Commission the authors aim to derive key takeaways regarding the reasons for these data breaches, the gaps in the data protection and information security practices of the affected organizations and possibly to synthesize recommendations and advice for the future how such breaches could be avoided or at least mitigated. These results will play a valuable part in a broader scientific research project dedicated to management of the data breach response reaction processes of the Bulgarian organizations funded by the Bulgarian Science Fund with the Ministry of Education where the authors form the research team.**

***Keywords*— Bulgarian organizations, data breach, GDPR, gaps.**

I. INTRODUCTION

The present study aims to explore the most significant personal data breach cases that affected organizations from the public and private sector in the Republic of Bulgaria – a Member State of the EU. The goal of this analysis is to find the main reasons that led to the said data breaches and to systematize key takeaways from these unfortunate events. Ultimately, the present paper argues that the data breach cases subject to the research are caused by a variety of factors and that their understanding and addressing is an important precondition so that in future such breaches could be prevented or at least, the severity of the consequences arising out of them could be limited.

The background of this research lies in the EU the General Data Protection Regulation 2016/679 (the Regulation/GDPR) [1] that was adopted with the idea to enhance the protection of the individuals in the context of the drastically increased data processing activities in the era of digital transformation and to foster the scrutiny of the organizations that collect and process personal data by

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8482

envisaging new data obligations for the controllers and processors, by expanding existing ones and by providing for broader data subjects' rights. Among other things, GDPR introduced reporting obligations in case of data breaches towards the supervisory authority (Article 33) and in certain cases – towards the affected individuals (Article 34). The doctrine explains that as follows: *"This obligation shall protect the rights and freedoms of the data subject by way of a better level of transparency."* [2]. The data breach reporting *"through notifications and communications is essentially a transparency requirement that shines the spotlight on operational failure and the resulting risks"* [3]. This new obligation enabled the society in general to find out about significant data breaches that affected various organizations which ultimately made the present research possible.

II. Materials and methods

The results of the present study were obtained after applying scientific methods such as:

Documentary method – consisting in analyzing and synthesizing information about the legal regime for GDPR data breach reporting and from various documentary sources – e.g. from the secondary EU law, from Bulgarian national legislation, from the practice of the Bulgarian data protection authority and from other publicly available (including online) sources, as well as in the systematization and summarization of this information.

Deductive and inductive reasoning – these methods are used with regard to the deriving of certain conclusions/scientific observations from the specific cases to the general and *vice versa*.

Comparative analysis – this method consists of comparing the common and the different between separate phenomena. In this report, this method is used to highlight some common reasons and mistakes that led to the occurrence of data breaches.

Case study – this method is used for analyzing real cases in order to collect new knowledge regarding the reasons for occurrence of data breaches and the measures to mitigate such breaches.

III. Results and discussion

Among the most notable cases are the data breaches that impacted the National Revenue Agency, Bulgarian Posts and one of the leading private banks in the country. These breaches resulted in the exposure of personal data, including special categories of data, affecting millions or hundreds of thousands of individuals and prompting investigations and sanctions by the Bulgarian Commission for Personal Data Protection (CPDP). This section provides an overview of these incidents, highlighting their impact and the following regulatory response.

A. The Data Breach in the Bulgarian National Revenue Agency

In August 2019 the CPDP imposed the biggest fine under GDPR in Bulgaria to the National Revenue Agency (NRA) for infringement of Article 32, para. 1, lit. b) of the Regulation [4]. Along with the fine, the CPDP issued an order to the NRA to undertake appropriate technical and organizational measures [5] (on the basis of Article 58, para. 2, lit. d) in conjunction with Article 57, par. 1, lit. a) and Article 83, para. 2, lit. a), c), d), f) and g) of the Regulation).

The data breach was a result of a cyberattack on the NRA's systems. Databases of around 11 gigabytes were sent anonymously to different Bulgarian media outlets, as well as made public online, and after further investigation it was confirmed that they contained personal data of more than 5 million persons from the NRA's systems (later the number was confirmed to be 4 104 786 active Bulgarian and foreign citizens). The prosecutor's office initiated criminal proceedings against two persons (one of the proceedings is ongoing as of 14 February 2025) [6]. The CPDP started an investigation upon notification of the data breach it received from the NRA on 17 July 2019. Following the investigation, numerous individuals initiated court proceedings for compensation for the infringement of their rights under the Regulation. One of the damage claim proceedings [7] led to a preliminary request to the Court of Justice of the European Union (CJEU) on which it issued a ruling interpreting the Regulation. In addition, collective claim proceedings were initiated.

a) Penalty Order and Fine

On 28.08.2019 the CPDP issued a penalty order to the NRA and imposed a fine of BGN 5 100 000 (approx. EUR 2 607 500) for failure to comply with the requirements of Article 32, para.1, lit. b) of GDPR. The order itself is not public, but according to CPDP's bulletin [8] the penalty was based on unauthorized access, unauthorized disclosure and dissemination of personal data of individuals from the information databases maintained by the NRA. The penalty order was confirmed by the first level court in subsequent proceedings, then revoked by the second level court, and then again revoked due to expiry of the statute of limitations. The first level court stipulated that on the factual and legal side the acts described in the penalty order were indisputably established and that the sanction imposed was correctly determined [9]. The second level court revoked the first level court's decision due to the expiry of the statute of limitations without discussing the case in essence [10].

Key takeaway: these proceedings did not lead to any final conclusion on whether NRA complied with its obligation to apply appropriate technical and organisational measures.

b) Decision for Adoption of Appropriate Technical and Organisational Measures

On 22.08.2019 the CPDP issued a decision [5] enlisting twenty data protection measures to be adopted by the NRA. They included: to establish clear rules, responsibilities, and interaction procedures for different system users; to improve the security of personal data in e-service applications; to develop comprehensive data protection

policies for all the NRA information systems; to ensure restrictive access policies to databases; to introduce audit logs and systems for managing privileged access and security event analysis; to develop a risk management methodology, including threat identification and periodic risk assessments; to conduct risk analysis and establish operational rules for data processing systems; to perform impact assessments for systems identified as high-risk; to set procedures for data protection impact assessments when launching new systems; to adapt information systems to the GDPR requirements, including risk management procedures for new or modified systems; to upgrade outdated operating systems and database management systems to mitigate security risks; to establish a disaster recovery center for real-time system recovery; to define policies for processing of special categories of data; to create policies for handling children's data; to develop encryption strategies for archived and one-time query data; to update the job description and responsibilities of the Data Protection Officer, ensuring direct reporting to the executive director; to revise employee job descriptions to include data processing responsibilities; to establish internal training programs for the NRA employees on handling personal data breaches.

The decision was later revoked partially by the first level court [11]. During the court proceedings the NRA presented information and documents on its data protection measures prior and following the data breach and appealed the decision on numerous grounds, including short deadlines for completion, general and unclear wording, incorrect findings and conclusions of the inspection team. The court repealed the decision in the parts concerning measures imposed by the CPDP. In respect to the performance of a risk analysis of systems and processing operations the court pointed out that risk analysis was performed on a regular basis in accordance with a procedure established by the executive director of the NRA. Regarding the requirements to establish policies for the re-use of subjects' personal data, including children's data, the court stipulated that the Regulation and the Bulgarian data protection legislation lack legal norms regulating the necessity and grounds for the creation of special rights for the re-use of personal data. In addition the court found that the NRA had developed rules for archiving data and the court did not find a need to explicitly introduce additional anonymisation, archiving and destruction rules for electronic data used on a one-time basis. Finally the court found that actions to establish audit records of the individual events and logs for privileged usershad already been implemented.

However, this decision was partially repealed by the second level court [12] due to procedural infringements of the first level court and the case was returned to the first level for re-examination (as of 14 February 2024 no final decision has been issued).

Key takeaway: no final decision on whether the NRA applied appropriate technical and organisational measures, however, the second level court adopted partially the arguments of the NRA against the measures imposed by the CPDP.

c) Claims for Damages by Individuals

Following the data breach, numerous affected persons filed claims for compensation for damages caused by the NRA as data controller. While some of the claims were successful before the first level court, the second level court mainly stipulated that "*the mere fact of unauthorized access to the NRA's information system does not prove the defendant's failure to protect it"*. This view was later confirmed by the CJEU in a preliminary ruling (see lit. e) below). The court also based its decision on its lack of expertise on the matter: "*since the court does not have special knowledge to assess what was done, whether what was done was sufficient, whether the hacker attack could have been avoided and if yes, what else should have been done, the court should have (….) ex officio admitted the hearing of forensic technical expertise on this issue*" [13]. In other words, in most of the proceedings the second level court stipulated that the first level court did not carry out the necessary procedural actions to assess whether there was wrongdoing on behalf of the NRA. As a result, it returned the proceedings to the first level court for re-examination. The re-examination led to varying end results. After forensic technical expertises were carried out, it was established that the NRA had developed various adequate rules and policies concerning network and information security, but they were not effectively implemented in practice. Given this, the court found that there was unlawful inaction on the part of the NRA in fulfilling the obligations arising from the relevant legal provisions to ensure the reliability and security of its information system. As a controller, the NRA was required to take effective measures to prevent malicious access to personal data, including crimes, and it failed to do so. However, the court did not rule in favor of the claimants in all cases, as in some cases it stipulated that there was no proof of damages (for example no proof of leakage of personal data of the particular claimant). Other proceedings were terminated due to expiry of the statute of limitations or on procedural grounds. The compensations, where granted, were in small amounts up to BGN 500 (EUR 255).

Key takeaway: varying final decisions, but generally the re-examination of the cases led to confirmation of unlawful inaction by the NRA and granting of compensations, albeit in small amounts.

d) Collective Claims

In addition to the individual claims, there have been collective claims aimed at forcing the state to take appropriate measures for personal data protection in the NRA's systems. The proceedings on one of these collective claims started in November 2024 and it is expected that the court will allow claimants to join until March 2025 [14], while others have already been terminated due to procedural reasons [15].

Key takeaway: it is to be seen whether the current proceedings will lead to imposition of further obligations for personal data protection on the NRA.

e) Preliminary Ruling of the CJEU

One of the individual claims against the NRA led to the decision of the Supreme Administrative Court to request a preliminary ruling of the CJEU [16]. All court proceedings related to the data breach were suspended until the CJEU issued its ruling and the re-examination decisions of the first level court described above were issued after the proceedings were renewed (there may be exceptions). In the ruling, the CJEU stipulated that unauthorised disclosure of personal data or unauthorised access to those data by a 'third party' are not sufficient, in themselves, for it to be held that the technical and organisational measures implemented by the controller in question were not 'appropriate'. The appropriateness of the measures must be assessed by the national courts in a concrete manner, by taking into account the risks associated with the processing concerned and by assessing whether the nature, content and implementation of those measures are appropriate to those risks. In addition, the CJEU stipulated that the principle of accountability must be interpreted as meaning that, in an action for damages the controller bears the burden of proving that the security measures implemented by it are appropriate. In order to assess the appropriateness of the security measures an expert's report cannot constitute a systematically necessary and sufficient means of proof. The controller cannot be exempt from its obligation to pay compensation for the damage suffered by a data subject solely because that damage is a result of unauthorised disclosure of, or access to, personal data by a third party in which case that controller must then prove that it is in no way responsible for the event. The fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of that regulation is capable, in itself, of constituting 'non-material damage' within the meaning of the Regulation.

Key takeaway: due to the NRA data breach proceedings the CJEU cleared out in what cases controllers shall compensate individuals in case of unauthorised disclosure to a third party and how the application of appropriate technical and organizational measures shall be assessed.

The NRA data breach happened undoubtedly due to lack of cybersecurity measures capable of stopping a particular attack on the systems. However, there is no definitive answer on whether the NRA failed to apply 'suitable' measures and on whether it infringed the GDPR. There is also no definitive decision on what measures the NRA applied successfully, what measures it failed to apply prior to the data breach, and what measures it must start applying in the future. The judicial proceedings following the NRA breach indicated that the Bulgarian court system was not prepared to apply data protection legislation to a case of such a scale. This led to multiple procedural conundrums, contradicting conclusions, delays and even expiry of the statute of limitations.

d) The Bulgarian National Revenue Agency Data Breach – Recommendations for Improvement

The case provides several key takeaways in different directions. First, the case demonstrates the necessity of independent oversight and stricter accountability mechanisms for public institutions handling significant quantities of personal data. While for some controllers the risk of intentional attacks is lower, the NRA data breach clearly demonstrates that public institutions in Bulgaria must be extra aware of malicious and intentional actions against their systems, and to apply proactive approach. The case outlines the necessity for public institutions to constantly keep up to date with most recent developments in technologies and data protection, or else it may be hard to argue that they took appropriate protection measures. From another point of view, the case demosntrates the supervisory's approach to high-impact matters, which may need improvement in the future – as numerous of the objections of the supervised institution NRA were upheld in court. Lastly, the examined data breach sheds a light on the approach of courts to such matters. As a key takeaway from the judicial proceedings, each data breach resulting from external actions must be carefully and thoroughly examined, including by technical experts. Courts must not stipulate that an attacked entity did not apply appropriate measures solely because the attack was successful; however, any conclusion that the attacked entity is not at fault solely because the data breach was caused by external intentional actions must also be considered ill-grounded.

Hopefully, the accumulated case law and the ruling of the CJEU will aid judges in similar cases in the future in Bulgaria and other EU Member States.

B. The Bulgarian Posts and a Leading Bulgarian Bank Data Breaches

In April 2022, the national postal service provider, Bulgarian Posts, suffered a severe cyberattack that disrupted its operations and compromised the personal data of 675,393 people whose identification was made possible through the affected personal data. The attack, reportedly a ransomware incident, led to system outages, preventing the processing of financial transactions, pension payments, and mail deliveries for an extended period of time. The breach exposed customers' personal data, including personal identification numbers and addresses, as well as information about financial transactions and people's health status.

Investigations indicated that the attack exploited vulnerabilities in Bulgarian Posts' outdated IT infrastructure. Due to insufficient cybersecurity measures and a lack of proper incident response strategies, the attackers managed to paralyse critical services, highlighting the weaknesses in the National Post's security framework. The attack was identified as being carried out using the Mimikatz malware, a credential theft tool, allowing unauthorised access to administrative accounts. Hackers infiltrated the SQL cluster containing personal

data, encrypted large portions of databases, and even encrypted backup files, rendering data recovery practically impossible [17].

The compromised information included personal identification numbers, addresses, financial data, pension details, and even medical records indicating the level of a person's disability. In total, approximately 4.67 million records were affected. The attack leveraged a security vulnerability in the Post's not-up-to-date Microsoft email server, enabling the hackers to gain full access to the virtual infrastructure and encrypt the backup data storage [18].

a) Regulatory and Institutional Response to the Bulgarian Post's Data Breach

The CPDP, as the regulatory body responsible for overseeing data protection in the country, launched an immediate investigation into the breach, focusing on compliance with the GDPR and the applicable national data protection laws. The findings revealed serious deficiencies in the organisation's cybersecurity preparedness, including outdated software, insufficient monitoring, a lack of timely risk assessments regarding the Post's backup and log file policies, and a low level of password management among the personnel. These impaired Bulgarian Post's ability to ensure continued confidentiality, availability, integrity, and resilience of the data processing systems and services and promptly restore availability and access to personal data.

As a result, the CPDP determined that Bulgarian Posts had failed to implement appropriate technical and organisational measures, violating specific articles of the GDPR. These include Article 32, para. 1, lit. b), c), and d), which outline the security measures that data controllers must implement to protect personal data, and para. 2, in connection with Article 5, para. 1, lit. e) of the GDPR, which requires data controllers to ensure the security and integrity of personal data. Furthermore, the CPDP deemed it most appropriate to apply the measure under Article 58, para. 2, lit. d) of the GDPR, namely, to issue specific instructions to the controller, including guidance on how to rectify the identified violations, and a sanction in the among of BGN 1,000,000 (approximately EUR 511,000). The CPDP's Administrative Sanctions Decision (Decision No. PAIKD-13-20/22 of 06.10.2022, issued by the Commission for Personal Data Protection was later challenged in court by Bulgarian Posts but upheld by the Administrative Court of Sofia as lawful. [17], [18].

In 2019, a major private bank in Bulgaria suffered a severe data breach affecting approximately 33,500 customers. The breach involved unauthorised access to 23,270 credit dossiers containing personal data, including special categories of data and financial information. Unlike the Bulgarian Posts case, which resulted from an external cyberattack, the private bank breach was due to internal security failures, particularly in data handling practices during an outsourced document digitisation process [19].

The CPDP investigation following the data breach determined that the bank, as a data controller, failed to implement suitable technical and organisational measures to protect the confidentiality, integrity, availability, and resilience of personal data processing systems.

The breach resulted in unauthorised access to a broad range of personal data, including names, national identification numbers, citizenship status, and addresses; copies of personal identification documents, including biometric data; tax documents detailing income and health insurance status; medical data, including official medical disability decisions; bank account numbers and transaction records; notarial deed registration numbers and signatures [19].

The investigation revealed that the breach stemmed from inadequate security measures during a large-scale credit dossier digitisation project, which took place between 2014 and 2016. The bank had outsourced the process but failed to enforce proper oversight and secure the deletion of scanned records, leaving sensitive information accessible on the scanning devices. This subsequently led to unauthorised third parties obtaining copies of credit dossiers.

b) The Bulgarian Post's Data Breach – Recommendations for Improvement

The cyberattack on the Bulgarian Posts highlighted severe deficiencies in cybersecurity preparedness, particularly in the organisation's outdated IT infrastructure, lack of proper monitoring, and ineffective incident response strategies. To prevent similar incidents in the future, it is essential to adopt a comprehensive cybersecurity strategy that includes regular software updates, security patching, and continuous penetration testing to identify and mitigate vulnerabilities before they can be exploited. Strengthening access control measures through the implementation of a suitable security model would significantly reduce the risk of unauthorised access. This approach ensures that all users, whether internal or external, are continuously verified and granted only the minimum necessary access to perform their tasks.

Furthermore, the attack was particularly damaging because the hackers managed to encrypt backup files, rendering data recovery nearly impossible. To address this risk, Bulgarian Posts and other public institutions should implement a multi-layered backup strategy that includes offline backups and immutable storage solutions. These measures would ensure that, even in the event of a ransomware attack, data recovery remains possible. Additionally, given that inadequate password management and poor security awareness among employees contributed to the breach, the introduction of mandatory cybersecurity training programs should be a priority. Regular training on phishing threats, secure password management, and incident response protocols would significantly enhance the organisation's ability to prevent and contain future attacks.

To prevent similar incidents in the postal sector, the implementation of sector-specific cybersecurity strategies is essential. *Admass et al.* recommend not only technical protections like encryption and intrusion detection but also

fostering collaborative cybersecurity ecosystems across public institutions to ensure readiness and rapid response to threats [20].

c) Regulatory and Institutional Response to the Private Bank's Data Breach

The CPDP concluded that the private bank violated Article 32 of GDPR, failing to ensure adequate data protection measures. Key security lapses included a lack of encryption for scanned documents, inadequate access controls and oversight over the scanning process and a failure to delete customer data from scanning devices after the digitisation project ended.

As a result, the CPDP imposed a fine of BGN 1,000,000 BGN (approximately EUR 511,000) on the private bank for unlawfully exposing the personal data of 33,492 clients, as well as an unknown number of third-party individuals linked to them, such as spouses, sellers, legal heirs, and guarantors.

The bank appealed the fine, arguing that it had followed industry-standard security practices and that liability should be shared with the external contractor. However, after multiple court reviews, the Administrative Court of Sofia City upheld the penalty, affirming that the bank bore ultimate responsibility as the data controller [21].

Key takeaway: due to the Bulgarian Posts and the private bank data breach proceedings, the CPDP clarified the obligations of both public institutions and financial entities in implementing technical and organizational measures to prevent unauthorized access, emphasizing, among other things, the importance of secure data management, encryption, and oversight in outsourced processes to ensure GDPR compliance.

d) The Private Bank Data Breach – Recommendations for Improvement

The data breach at one of Bulgaria's leading private banks revealed critical weaknesses in the oversight of third-party service providers, as well as in the bank's internal data security practices. Given that the breach stemmed from an outsourced document digitisation process, financial institutions must enforce strict contractual obligations for external service providers, ensuring that all third parties handling sensitive data comply with internationally recognised security standards, such as ISO 27001 or NIST cybersecurity frameworks. Regular audits and security assessments should be required to verify that these providers implement and maintain appropriate technical and organisational measures.

To further mitigate risks associated with outsourcing and third-party access to sensitive personal data, banks must implement robust master data management (MDM) systems and data governance frameworks. As *Martins et al.* argue, compliance with international standards like BCBS 239 requires banks to develop centralised, well-documented data architectures with clearly assigned ownership and lifecycle controls, supported by board-level governance structures and internal audits [22] (The "BCBS 239" concept refers to the "Principles for Effective Risk Data Aggregation and Risk Reporting" by the Bank of International Settlement. made publicly available by the Basel Committee on Banking Supervision in early 2013. From a structural perspective, BCBS 239 is organised around a set of 14 Principles that draw attention to the diverse obligations and concerns that must be addressed when managing risk in banking institutions [22]). This approach could not only enhance compliance, but also enables risk-based decision-making and transparency across all data domains.

Additionally, the bank's failure to securely delete scanned documents after the completion of the digitisation process demonstrates the need for strict data retention and deletion policies. Automated data lifecycle management should be implemented to ensure that unnecessary data is permanently removed once it is no longer required for business or regulatory purposes.

The slow response to the breach further underscores the necessity of a well-defined and regularly tested incident response plan. Banks and other financial institutions should conduct periodic cybersecurity drills and tabletop exercises to ensure that their teams can respond swiftly and effectively to potential data breaches. Strengthening these security measures would not only improve compliance with GDPR but also reinforce public trust in the banking sector's ability to safeguard sensitive personal and financial information.

C. Other Significant Data Breach Cases in Bulgaria

After analyzing the cases related to the massive data breach at the NRA, as well as the incidents at Bulgarian Posts and one of the Bulgarian banks, it becomes clear that insufficient security measures and risk management remain a serious problem in both the public and private sectors. In addition to these examples, a few more notorious data breach case seem relevant for the purposes of the present analysis.

a) The Data Breach in the Supreme Administrative Court

Bulgaria recently witnessed another major incident related to the security of judicial institutions. A hacker attack affected the Supreme Administrative Court (SAC) and all administrative courts in the country, leading to a temporary disruption of the Unified Administrative Court Case Management System and raising questions about the level of cybersecurity in the judicial system [23].

Subsequently, it became clear that the hacker group Ransomhouse took responsibility for the attack by posting a message on the Dark Web and stating that they had copies of data from the SAC. To support their claims, the hackers released part of the compromised information, including personal data of judicial employees, which according to specialized sources was already accessible to hundreds of users on illegal platforms.

This attack differs from traditional ransomware attacks because instead of encrypting files, Ransomhouse uses an

extortion model based on threats of public distribution of the stolen data. An additional concern is that the attack was carried out using one of the most sophisticated malware, White Rabbit, which is believed to have penetrated the system due to human error. This not only reveals vulnerabilities in the cybersecurity of judicial institutions but also underscores the lack of effective protocols for prevention and response to such incidents. Although the SAC received emergency funding to improve its infrastructure, the attack raises serious questions about the overall resilience of state information systems against organized cybercrime groups.

This attack is further evidence of the increasing risks to data protection in the public sector and highlights the need for stricter preventive measures, including better control over access to critical systems, regular training to recognize phishing attacks, and strategic investments in cyber resilience. Considering the cases already analyzed, attention should also be paid to other significant breaches that differ in nature but nonetheless reveal similar weaknesses in the approach to personal data protection. In this context, the next two cases focus on the Inspectorate to the Supreme Judicial Council (ISJC) and a violation related to the unauthorized publication of sensitive personal data, as well as on a case of lapses in information access management in the educational and accounting sectors [24].

b) The Data Breaches in the Inspectorate to the Supreme Judicial Council and in the Areas of Education and Accounting

In July 2019, the ISJC in its capacity as a personal data controller published in its electronic register 4420 declarations of assets and interests for 2018 of judges, prosecutors, and investigators. In some of these declarations (pertaining to 20 judges, prosecutors, and investigators and the related 19 spouses and 11 minors), personal data were disclosed that were not minimized, including personal identification numbers, ID card numbers, addresses, telephone numbers, and social information. This represents a violation of Article 5, para. 1, lit. e) and Article 32, para. 1, lit. b) and c) of the GDPR, as well as Article 66, para. 1 of the Bulgarian Personal Data Protection Act [25].

The main reason for the incident appears to be a combination of inadequate organizational measures to protect personal data and a lack of automated mechanisms to minimize sensitive information before its publication. There may have been insufficient control over the process of anonymizing personal data, leading to their unintentional disclosure. Also, the publication of such a volume of information in such a short period suggests that there may have been pressure to fulfill administrative obligations without sufficient technological and expert resources for verification. The ISJC was imposed an administrative penalty of 2000 BGN (approximately EUR 1000), according to Article 87, para. 3 of the Bulgarian Personal Data Protection Act. Although this penalty may seem insignificant, it underscores the need for improving control mechanisms in public institutions.

The second case involves two private schools and an accounting firm, which reported a personal data breach to the CPDP under Article 33 of the GDPR. During the investigation, it was found that the schools had provided access to their information system to the accounting firm without ensuring appropriate technical and organizational security measures. As a result, there was a real risk of unauthorized access and disclosure of personal data for 188 individuals and 33 legal entities serviced by the accounting firm. This represents a “breach of confidentiality” within the meaning of Article 33 of the Regulation [26].

The main reason for the breach was the lack of adequate control over access to the schools’ information system. It is possible that the administration did not perform a comprehensive risk analysis before granting access to the external accounting firm. There might also be a lack of a clearly written information system security policy that includes mechanisms to limit access only to strictly necessary data. The accounting firm, for its part, is responsible for improper data storage, which led to the disclosure of personal information of clients and employees. This highlights the need for better control mechanisms in the processing of personal data by external organizations. The CPDP has imposed a monetary penalty on the accounting firm and a warning corrective measure on the private schools. This demonstrates a differentiation in responsibility between the two types of administrators, with the accounting firm being more severely sanctioned for the specific incident.

The analysis of the cases reviewed reveals several key issues in the field of personal data protection. The main problem is related to the lack of adequate mechanisms for control and protection of personal data. The publication of sensitive information (by the ISJC) and unsecured access (schools and accounting firm) reveal weaknesses in security management. A second issue is that personal data controllers have not conducted a detailed assessment of potential risks before taking certain actions, such as publishing declarations or providing access to external parties. In the case of the ISJC, the violation is due to the non-compliance with the data minimization principle, which led to unauthorized disclosure of information about judges, prosecutors, and their families. The hacker attack against the SAC and administrative courts shows that not only human errors but also external malicious actions can compromise information systems. This underscores the need for better incident response protocols.

While in the public sector (the ISJC, the SAC) there are weaknesses related to administrative pressure and insufficient control over published information, in the private sector (schools and accounting firm), the violations are mainly related to unsecured external access and poor practices in managing information infrastructure. In the cases of the ISJC and schools, the violation stems from management decisions, while the attack against the SAC

reveals technological vulnerabilities exploited by third parties.

Key takeaway: To enhance the effectiveness of personal data protection, several key measures need to be taken. Firstly, organizations should improve their technical security mechanisms by implementing automated systems for controlling published information and encrypting sensitive data. Additionally, regular audits and monitoring will help identify potential vulnerabilities and ensure timely response to incidents. Further, employee training in cybersecurity should be strengthened to minimize risks associated with human factors. This includes developing awareness programs about threats and implementing good practices for personal data protection. Finally, regulatory bodies should impose stricter penalties for systemic violations to ensure more effective compliance with legal requirements. Implementing these recommendations will contribute to significant improvements in risk management, both in the public and private sectors, and will minimize the likelihood of future incidents related to breaches of personal data protection.

c) Other Significant Data Breaches – Recommendations for Improvement

The identified gaps – including insufficient organizational preparedness, technical vulnerabilities, and lack of preventive measures – reveal the need for stricter regulatory intervention and investments in the security of information systems. It is particularly concerning that both human errors and malicious cyberattacks compromise sensitive information, underscoring the importance of a proactive approach to risk management. Effective implementation of technical measures, regular audits, and training to enhance cybersecurity are among the most necessary steps to minimize threats. Regulatory bodies also need to strengthen their sanctioning policy and apply proportional yet decisive measures against systemic violations. The introduction of stricter control mechanisms, as well as encouraging organizations to adhere to best practices, will be crucial for ensuring a high level of personal data protection in Bulgaria and within the context of European regulations.

Considering the analysis of all cases examined thus far, it becomes evident that there is a clear necessity to develop a unified model and a clearly defined algorithm for responding to personal data breaches, applicable to both the public and private sectors. This model should encompass minimum standards and action procedures, including technical and organizational measures, prevention methods, and effective incident response mechanisms. Creating and implementing such a unified approach should be a priority for future research and practical efforts in order to ensure a high level of personal data protection in compliance with European and national regulatory requirements.

CONCLUSIONS

In conclusion, it is evident that the organizations from the public and private sector in the Republic of Bulgaria have significant gaps in their internal processes related to handling data breaches. The analysed data breaches are a result of complex of factors such as insufficient technical and organisational measures implemented to ensure the security of the processed personal data, outdated technical equipment and information systems, lack of knowledge of the personnel how to react in such cases, missing internal procedures for reaction and data breach counteraction/consequence limitation, etc. It is evident that the organisations in Bulgaria need a working model defining clear algorithm how to react in case of data breaches and this will be subject to future work of the research team that co-authored the present analysis.

The analysis of the data breaches at Bulgarian Posts and the private bank underscores systemic weaknesses in both the public and private sectors when it comes to cybersecurity and data protection. One of the most pressing issues is the reliance on outdated IT infrastructure and the lack of proactive risk assessments, which make institutions vulnerable to cyberattacks. A key lesson from these cases is that organisations must prioritize continuous security evaluations and modernise their digital infrastructure to keep pace with evolving threats.

The above is also applicable to the case of the NRA data breach, with the additional reccomendations outlined in respect to the courts and the supervisory authority. Each data breach resulting from external actions must be carefully and thoroughly examined, including by technical experts, and any regulatory or judicial decisions on the appropriateness of technical and organisational mesures need to be specific, well-grounded and drafted after careful examination of all circumstances in order to comply with the views of the CJEU.

Furthermore, Bulgarian organizations must urgently adopt structured protocols for incident management and introduce mandatory cybersecurity training for their personnel. Regulatory oversight should be strengthened by ensuring regular compliance audits and imposing proportionate yet effective sanctions in case of systematic breaches. Addressing these areas proactively will significantly improve the resilience of both the public and private sectors against future cybersecurity incidents.

ACKNOWLEDGMENTS

The present paper was prepared as a result of the scientific research activities conducted within 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 with the Ministry of Education“, “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] Official Journal of the European Union, L 119, pp. 1–88, May 4, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed: Feb. 20, 2025].

[2] P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing AG, 2017, p. 65.

[3] S. Room, "Security of Personal Data," in European Data Protection: Law and Practice, 3rd ed., E. Ustaran, Ed. Hyde Park Publishing Services: IAPP, 2023, p. 228.

[4] Commission for Personal Data Protection, Penal Order No 004/28.08.2019.

[5] Commission for Personal Data Protection, Decision No PPN-02-399/22.08.2019.

[6] Lex News, The court refused for the second time the agreement of the prosecution with Christian Boykov for "NRA Leaks", 01.11.2024 [Online]. Available: https://news.lex.bg. [Accessed: Feb. 20, 2025].

[7] Administrative Court Sofia City, Motion Order of 14.05.2021 rendered in Case 1037/2021, V Department.

[8] Commission for Personal Data Protection, Information Bulletin, vol. 5, no. 80, Sept. 2019. [Online]. Available: https://cpdp.bg/userfiles/file/Bulletin/KZLD_Bulletin_5_80_September_2019.pdf. [Accessed: Feb. 20, 2025].

[9] Sofia District Court, Decision of 26.10.2023, rendered in Case No 14811/2019.

[10] Administrative Court Sofia City, Decision No. 1247/26.02.2024, rendered in administrative case No. 12334/2023.

[11] Administrative Court Sofia City, Decision No. 565/02.02.2023, rendered in administrative case No. 10477/2019.

[12] Supreme Administrative Court, Decision No. 1398 of 07.02.2024 in administrative case No. 3781/2023, V Department.

[13] Supreme Administrative Court, Decision No. 9399 of 13.09.2021 in administrative case No. 11029/2020, II Department, Decision No. 9414 of 15.09.2021 in administrative case No. 9871/2020, III Department, Decision No. 9417 of 15.09.2021 in administrative case No. 11283/2020, III Department, Decision No. 9420 of 15.09.2021 in administrative case No. 10793/2020, III Department, Decision No. 9421 of 15.09.2021 in administrative case No. 8825/2020, III Department.

[14] Lex News, The court gave the go-ahead to a class action lawsuit against the NRA over the data leak, 27.11.2024 [Online]. Available: https://news.lex.bg. [Accessed: Feb. 20, 2025].

[15] Sofia District Court, Order No 348 of 10.01.2023, rendered in Case No 13344/2021, Appelate Court Sofia, Order No 549 of 28.02.2023, rendered in Case No 473/2023,

[16] Court of Justice of the European Union, Judgment of the Court (Third Chamber) of 14 December 2023 (request for a preliminary ruling from the Varhoven administrativen sad – Bulgaria) – VB v Natsionalna agentsia za prihodite, Case C-340/21, Natsionalna agentsia za prihodite.

[17] Commission for Personal Data Protection, Annual Report 2022. Sofia, Bulgaria: CPDP, 2022. [Online]. Available: https://cpdp.bg/wp-content/uploads/2023/11/Annual-report_2022_CPDP.pdf. [Accessed: Feb. 20, 2025].

[18] Administrative Court Sofia City, Court Decision No. 505/18.01.2024, rendered in administrative case No. 9929/2022.

[19] Commission for Personal Data Protection, Annual Report 2019. Sofia, Bulgaria: CPDP, 2019. [Online]. Available: https://cpdp.bg/userfiles/file/Annual%20Reports/Annual_Report_2019_CPDP.pdf. [Accessed: Feb. 20, 2025].

[20] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, 100031, 2024. [Online]. Available: https://doi.org/10.1016/j.csa.2023.100031. [Accessed: Mar. 25, 2025].

[21] Administrative Court Sofia City, Court Decision No. 300/11.01.2024, rendered in administrative case No. 11485/2023.

[22] J. Martins, H. S. Mamede, and J. Correia, "Risk compliance and master data management in banking – A novel BCBS 239 compliance action-plan proposal," *Heliyon*, vol. 8, no. 7, e09627, 2022. [Online]. Available: https://doi.org/10.1016/j.heliyon.2022.e09627. [Accessed: Mar. 25, 2025].

[23] Lex News, A cyberattack has crashed the information system of all administrative courts, Jan. 27, 2025. [Online]. Available: https://news.lex.bg. [Accessed: Feb. 3, 2025].

[24] Lex News, A hacker group announced that it has the data leaked from the Supreme Administrative Court – publishing a portion as proof, Feb. 20, 2025. [Online]. Available: https://news.lex.bg. [Accessed: Feb. 22, 2025].

[25] Commission for Personal Data Protection, Annual Report 2019. Sofia, Bulgaria: CPDP, 2019. [Online]. Available: https://cpdp.bg/userfiles/file/Annual%20Reports/Annual_Report_2019_CPDP.pdf. [Accessed: Feb. 3, 2025].

[26] Commission for Personal Data Protection, Annual Report 2023. Sofia, Bulgaria: CPDP, 2023. [Online]. Available: https://cpdp.bg/wp-content/uploads/2024/03/Annual-report_2023_CPDP.pdf. [Accessed: Feb. 3, 2025].