GDPR Violation Case Study: National Revenue Agency of Bulgaria

Jearson Alfajardo
Brown Univeristy

Abstract

On July 15, 2019, several media outlets in Bulgaria received an email from a Russian address containing an 11 GB zip file containing the names, personal identification numbers, addresses, telephone numbers, and other personal information of more than 6 million Bulgarian citizens and foreigners, later found to be from the Bulgarian National Revenue Agency's servers. [8] [18] It is the largest data breach to occur Bulgaria and the rest of the Balkan states to date and since then there have been two firings [25] , three arrests [26] , and an official fine issued by the country's Data Protection Authority [18] more than a month later. The events and legal proceedings succeeding the event are still developing today

1 Background

On July 15, 2019, shortly after 10am, dozens of media outlets across Bulgaria received an email from a Russian address containing a zip file of 57 folders containing CSV files totaling 11 GB of personal data from the databases of the Bulgarian National Revenue Agency (NRA).

The email stated that the attached data was only partial and that the complete set was actually 21 GB in total. In addition, it referenced a quote from Wikileaks founder Julian Assange ("Your government is slowly developing. Your state of cybersecurity is parody") and suqsequently called for his release. [23] Verification of the data and press coverage began that day along with investigations by authorities. [24]

The following day, Belgian authorities publicly confirmed the scale and authenticity of the data, estimated to be on around 6 million individuals. [22] An emergency meeting with The Security Council was called by Prime Minister Boyko Borrisov and, on the same day and a suspect was later arrested as the suspected perpetrator. The suspect was later to be identified as 20 year old Christian Boykov, a security penetration tester of the cybersecurity firm TAD Group. [22]

After the arrest a second email was later received by some of the same media outlets at around noon claiming that the breach had been in place for years and that the hacker himself was a Russian male married to a Bulgarian wife. [22] The email also threatened to release the rest of the data on the public internet if the government attempted to hide the truth.

Around a month and a half later, following the firing of two Senior IT sepcialists at the NRA [25] as well as accusations and arrest of two more individuals (the Founder and CEO of the TAD Group, Ivan Todorov and Key Account Manager, Georigi Yankov) as well as the release of pre-trial evidence by the Prosecutor's Office of Bulgaria to support these charges [5] , the nation's Data Protection Agency, the Commission for Personal Data Protection (CPDP) disclosed on August 21 that the NRA will be made to take corrective action and receive the fine of 5.1 million BGN (€2.6 million) on August 29, citing they had not implemented the 'appropriate technical and organizational measures' as a data controller [18]

The NRA motioned to appeal the fine on the same day [11] and the appeal process is still ongoing along with the criminal prosecution of the individuals

2 Details of the Breach

The breach was found to have been done through an NRA Value-Added-Tax (VAT) service active since 2012, months before the email was sent out. [6] It was reportedly used by relatively few taxpayers and, as a result, received no upgrades since. [6]

2.1 The Vulnerability

The lack of upgrades allowed for a simple SQL Injection attack to be carried out at the login page of the VAT service, via its name and password fields. [22] An NRA spokesman reported that the unauthorized access was detected by their security unit at the end of June [6] when unusual activity was detected, leading investigators to assume that this was when the hacker downloaded the data. [22]

2.2 The Data

According the CPDP, the data breach in total held the information of 6,074,140 individuals, 4,104,786 of whom were living data subjects both Bulgarian citizens and foreigners, and 1,959,598 individuals already deceased. [18] The categories of the personal data disclosed were as follows:

i. Names
ii. Personal Identification Numbers of Bulgarian Citizens
iii. Addresses of Bulgarian Citizens
iv. Telephone numbers, email addresses, and other contact details
v. Annual tax return data of individuals
vi. Data on the personal income tax expense on the income statement
vii. Data from insurance declarations
viii. Data on health insurance premiums
ix. Data on issued acts for administrative violations
x. Data on completed payments of taxes and social security liabilities
xi. Data on claimed and refunded Value-Added-Tax paid abroad

3 Details of the Penalty

3.1 Entities Involved

- **Data Subjects**: Bulgarian and foreign citizens, deceased individuals
- **Data Controller**: National Revenue Agency
- **Data Processor**: National Revenue Agency
- **Data Protection Authority**: The Commission for Personal Data Protection of Bulgaria

3.2 Violators and GDPR articles involved

The violator in this case was the National Revenue Agency of Bulgaria, fined by the Commission for Personal and Data Protection for violating Article 32, §1(b) of the GDPR, which states:

> *"Taking into account the state of the art... the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate... the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"* [1]

The CPDP ruled that the

> *"NRA, as a data controller, has not implemented the appropriate technical and organization measures, resulting in a data breach"* [18]

For violating the Article, the CPDP decided to impose corrective action against the data controller (the NRA) as well as impose a pecuniary sanction. [14]

3.3 Corrective Measures

In accordance the with Art. 58, §2 (d) and in connection with Art. 57, §1 (a) and Art. 83, §2 (a)(c)(d)(f) and (g) of the GDPR , the CPDP issued a decision [18] ordering the NRA to take the appropriate technical and organizational measures to be GDPR compliant such as:

- Measures to enhance the protection of personal data processing in applications, providing e-services to citizens;
- Performing risk analysis of systems and processing operations, including established rules and functional obligations for the processing of every single information system;
- Carrying out impact assessments at the event of identifying "high risk" for each system, and the appropriate measures, which have to be taken;
- Performing an impact assessment on the initial launch of new information systems and applications.

and to do so in six months, starting the day the Agency receives the orders. [18]

3.4 Pecuniary Sanction

The penalty fine imposed for violating Article 32, §1(b) of the GDPR was BGN 5,100,000 (€2,607,479), to represent

> *[T]he administrative and criminal responsibility of the NRA, as a data controller, for the unauthorized access and dissemination of personal data* [18]

4 Aftermath

4.1 Effects of the Breach on Data Subjects

According the the NRA, only 189 people had a combination of data contained in the breach such that they needed change IDs. [4] The rest of the 4 million Bulgarians affected by the leak were told to simply be 'more vigilant' with their information. [7] On July 25, 2019, ten days after the breach, a tool and accompanying FAQ were published by the NRA to allow citizens to check if their personal data had been unlawfully disclosed in the breach. [10] [12]

4.2 International Response

As a state taxing agency, the National Revenue Agency normally performs mandatory automatic exchanges of information with the other members of the EU. [12] As of August 30, 2019, the Organisation for Economic Co-operation and Development (OECD) advised for member states to suspend these automatic exchanges from being sent to Bulgaria until a review has been concluded, and stated that the Global Forum on Tax Transparency and Exchange of Information for Tax Purposes be suspended as well.

4.3 Arrests and Firings

Since the breach, two senior IT specialists at the NRA were fired in August. [25] In the same month, and in addition to the arrest of cybersecurity pentester Christian Boykov of the TAG Group, the founder and CEO, Ivan Todorov, and the company's Key account Manager, Georgi Yankov, have also been filed criminal charges by the Sofia City Prosecutor's Office in August. [20] Their trial is still ongoing.

5 Conclusions

Aside from the attempted cyber-racketeering done by the TAG Group to allegedly gain clients, this case seems to be precisely why the GDPR was created. Previous scandals such as the public disclosure of vulnerabilities in the Bulgarian Education Ministry's website in 2017 [26], warnings from the the country's leading business organization, the Bulgarian Industrial Organization, of possible flaws in the governments data protection systems in 2018 [26], and hardware failure that affected the trade registry of the Bulgarian Registry Agency that same year, leaving 25 TB worth of drive data inaccessible for a week and virtually suspending trade turnover and access to company ownership information due primarily to a lack of an adequate backup system. [2] [3].In general, it appears that the government organizations of Bulgaria have a record of neglecting to even maintain, back up, or update their computer systems, much less pay attention to data privacy and security. Measures like the GDPR allow for corrective measures to be imposed and backed by law, as it was in this case.

The CPDP also acted quickly, initiating investigations the day they were made aware of the breach, though likely this was because of its scale and significance. After the initial response, a month long investigation was undertaken, culminating in the release of the CDPR's verdict and fine amount a mere month-and-a-half after the emails were received.

This is the first case of such scale to have ever happened to country of Bulgaria, where the personal information of almost every single working adult in the country had some form of their personal data exposed [19]. This marks the event to definitely be of note in future history books of the country and potentially a catalyst for more responsible data privacy and security practices to be pursued in the future.

6 Chronological Summary of Events

- **July 15**:

  Bulgarian media outlets receive an email containing 11 GB of data from Bulgarian National Revenue Agency (NRA)'s servers from a Russian email address. Verification of the data and press coverage begins, s

- **July 16**:

  Belgian Authorities admit the theft and that 3% of tax information had been leaked and had learned from the media outlets that received the email. [6]

- **July 17**:

  Kristian Boykov, a cybersecurity employee of the TAD Group cybersecurity firm is arrested on suspicion of perpetrating the act. [26] Details are released about Kristian Boykov and his past, including how he made national new in 2017 after exposing flaws in the Bulgarian Educaton Ministry's website (of which he received praise from the Deputy Education Minister) [26] In the coming weeks, Boykov's company the TAD Group is also accused of ordering the hack for cyber-racketteering and poilital reasons. [21]

- **July 24**:

  The NRA reports that only 189 people at most need to change their IDs, while the rest of the 4 million Bulgarians only need to "remain vigilant" [4] [7]

- **August 1**:

  The Prosecutor's Office publicly disseminates evidence against the TAG Group [16]

- **July 30**:

  The founder and CEO of the TAD Group Ivan Todorov is arrested at the Bulgarian Ariport. [9]

- **August 21**:

  Bulgaria's Data Protection Authority, the Commission for Personal Data Protection (CPDP), posts on their website about the NRA breach and the decision reached at meeting held on August 20th to impose a corrective measure on the NRA to comply with GDPR, though the fine amount would be specified at a later date

- **August 23**:

  The Prosecutor's Office of Bulgaria publishes new evidence that accuses the owner of the TAD group, Ivan Todorov, and its sales director, Georgi Yankov, of ordering the hack, while Kristian Boykov is still reported to

be the perpetrator. The text of the second email sent by the hacker was found on Kristian Boykov's computer, as well as a tape recording between Yankov and an employee of the company) [15]

- **August 23**:

  The Minister of Finance, Vladislav Goranov states that the NRA will pay the fine imposed by the CPDP from its own budget [27]

- **August 29**:

  The CPDP posts on their website formally indicting the NRA for "as a data controller" for having not "implemented the appropriate technical and organizational measures, resulting in a data breach". They set the fine to be imposed on the NRA to be BGN 5,100,000 (€2,607,479). [18] The NRA states that they will appeal [25] and fires its two senior IT specialists.

- **August 30**:

  The Organisation for Economic Co-operation and Development (OECD) advises for exchange partners to suspend any data being automatically sent to Bulgaria until a review has been concluded. They also state for the Global Forum on Tax Transparency and Exchange of Information for Tax Purposes suspended exchanges with the country. [17]

- **Sept 13**:

  Ivan Todorov, the owner of the TAD Group, is arrested by the app elate special tribunal on charges of incitement to terrorism, and organizing a criminal group with a useful purpose [13]

References

[1] Regulation (eu) 2016/679 of the european parliament and of the council. *Official Journal of the European Union*, Apr 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[2] 4th day without access to the bulgarian commercial register - dangers and recovery forecasts. *novinite.com*, Aug 2018. https://www.novinite.com/articles/191628/4th+Day+Without+Access+to+the+Bulgarian+Commercial+Register+-+Dangers+and+Recovery+Forecasts.

[3] The trade registry now down a full week, head of the registry agency resigns, npp belene devours a new million. *Mediapool*, Aug 2018. https://www.mediapool.bg/the-trade-registry-now-down-a-full-week-head-of-theeee-registry-agency-resigns-npp-belene-devours-a-new-million.html.

[4] 189 people are most affected by the data leak, the revenue agency said. *Diary*, Jul 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.dnevnik.bg/bulgaria/2019/07/24/3942635_nai-zasegnati_ot_techa_na_danni_sa_189_dushi_obiaviha/&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhgk-FujV5RXlw5l9f0YnHIihT-Wgg.

[5] Bulgaria's national revenue agency said to be appealing fine for data breach. *Fintech Global*, Aug 2019. https://member.fintech.global/2019/08/30/bulgarias-national-revenue-agency-said-to-be-appealin

[6] For now, the authorities only know that the nra was hacked from abroad without understanding. *Mediapool*, Jul 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.mediapool.bg/vlastite-zasega-znayat-samo-che-nap-e-haknata-ot-chuz&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhiARSpBwRZWrIAJgBWrhzbkmU2zwQ.

[7] Revenue agency reassured that no extra action is needed due to data leakage. *Diary*, Jul 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.dnevnik.bg/bulgaria/2019/07/26/3943617_ot_prihodnata_agenciia_otnovo_uspokoiha_che_ne_se/&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhgRh-KHKLTKd_f3eF5LAi8C-IFauQ.

[8] The russian hacker spoke: The system has been hacked for 11 years. *Mediapool.bg*, July 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.mediapool.bg/ruskiyat-haker-progovori-sistemata-e-probita-ot-11-go&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhi5Lw5b-a4UGpKsTbXtbLuPYNlteg.

[9] Tad group owner ivan todorov was arrested at the airport. *Novinite.com*, Jul 2019. https://www.novinite.com/articles/198912/TAD+Group+Owner+Ivan+Todorov+Was+Arrested+at+the+Airport.

[10] National Revenue Agency. Frequently asked questions. https://nap.bg/en/document?id=418.

[11] National Revenue Agency. The nra disputes the cpdp's act, the penal decision is pending. https://translate.google.com/translate?hl=en&sl=auto&tl=en&u=https%3A%2F%2Fnap.bg%2Fnews%3Fid%3D4047&sandb

[12] National Revenue Agency. Unauthorized access to nra data. https://check.nra.bg/check/en.

[13] Inna Drumev. The court finally arrested the owner of tad group for cyber terrorism. *Diary*, Sept 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.dnevnik.bg/bulgaria/2019/09/13/3962921_sudut_okonchatelno_ostavi_v_aresta_sobstvenika_na_tad/&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhgT1VDv-chSfvyT7Sbb8mBwUBtdkA.

[14] Inna Drumev. The personal data protection commission fines millions in revenue. *Diary*, Aug 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.dnevnik.bg/bulgaria/2019/08/21/3953537_komisiiata_za_zashtita_na_lichnite_danni_globiava_s/&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhgjlUqfDSHJv2IJxNppAD-0Mfg_jQ.

[15] Inna Drumev. Prosecutor's office publishes new piece of evidence in tad group investigation. *Diary*, Aug 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.dnevnik.bg/bulgaria/2019/08/23/3954614_prokuraturata_publikuva_nova_porciia_dokazatelstva_po/&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhjWmdyPWwH0RpDEg_VpFRxu7_c4mQ.

[16] Inna Drumev. The prosecutor's office surprisingly disseminated evidence against tad group to defend the prosecution. *Diary*, Aug 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.dnevnik.bg/bulgaria/2019/08/01/3945990_prokuraturata_iznenadvashto_razprostrani_dokazatelstva/&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhhntLzL7PJsI8mnOFEu3QQef6zeOg.

[17] Organisation for Economic Co-operation and Development. Statement on the data breach in the national revenue agency of bulgaria. http://www.oecd.org/tax/transparency/statement-on-the-data-breach-in-the-national-revenue-htm.

[18] Commission for Personal Data Protection. Update on the undertaken inspection at the national revenue agency. https://www.cpdp.bg/en/?p=news_view&aid=1519.

[19] Scott Ikeda. Massive data breach in bulgaria compromises the country's entire adult population. *CPO Magazine*, Jul 2019. https://www.cpomagazine.com/cyber-security/massive-data-breach-in-bulgaria-compromises-the-count

[20] Jeremy Kirk. Breach saga: Bulgarian tax agency fined; pen testers charged. *Bankinfo Security*, Aug 2019. https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged

[21] George Paunowski. The detained christian company is engaged in cyber-racket, announced ivan geshev. *Diary*, Jul 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=auto&sp=nmt4&tl=en&u=https://www.dnevnik.bg/bulgaria/2019/07/23/3941908_firmata_na_zadurjaniia_kristiian_se_zanimava_s_kiber/&xid=25657,15700022,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhjTi3_tCQVa7p6stqG76enbsok1Jg.

[22] Nikolai Stoyanov. The country with the most open data in the world. *Capital*, Jul 2019. https://translate.google.com/translate?hl=en&sl=auto&tl=en&u=https%3A%2F%2Fwww.capital.bg%2Fpolitika_i_ikonomika%2Fbulgaria%2F2019%2F07%2F19%2F3940270_durjavata_s_nai-otvorenite_danni_v_sveta%2F&sandbox=1.

[23] Nikolai Stoyanov. Nra has leaked personal data to millions of bulgarian citizens and businesses. *Capital Newspaper*, July 2019. https://translate.google.com/translate?hl=en&sl=auto&tl=en&u=https%3A%2F%2Fwww.capital.bg%2Fpolitika_i_ikonomika%2Fbulgaria%2F2019%2F07%2F15%2F3938624_ot_nap_sa_iztekli_lichni_danni_na_milioni_bulgarski%2F/.

[24] Veselin Toshkov. Hackers steal millions of bulgarians' data; russian tie seen. *Associated Press*, Jul 2019. https://finance.yahoo.com/news/hackers-steal-millions-bulgarians-data-101555188.html.

[25] Tsvetelia Tsolova. Bulgaria's tax agency fined $3 million over data breach, will appeal. *Reuters*, Aug 2019. https://www.reuters.com/article/us-bulgaria-cybersecurity-fine/bulgarias-tax-agency-fined-3-million-over-data-breach-will-appeal-idUSKCN1VA0TX.

[26] Tsvetelia Tsolova and Angel Krasimirov. 'wizard' cybersecurity expert charged with record hack of bulgarian tax agency. *Reuters*, Jul 2019. https://www.reuters.com/article/us-bulgaria-cybersecurity/wizard-cybersecurity-expert-charged-with-record-hack-of-bulgarian-tax-agency-idUSKCN1UC0GF.

[27] Georgi Zhelyazkov. Goranov: The nra will pay the find from its own budget. *Economic*, Aug 2019. https://translate.googleusercontent.com/translate_c?depth=1&hl=en&rurl=translate.google.com&sl=bg&sp=nmt4&tl=en&u=https://www.economic.bg/bg/news/11/goranov-nap-shte-si-plati-globata-ot-sobstveniya-byud&xid=17259,15700021,15700186,15700190,15700256,15700259,15700262,15700265&usg=ALkJrhi0H92wbqIP6tuJgk2wmOKAhdGYLA.