The personal data of millions hacked in Bulgaria.
What exactly happened?

The BBC reported on 17th of July, 2019 that personal data belonging to millions of Bulgarians has been stolen in a cyber-attack on the country's National Revenue Agency (NRA). The files, sorted into 57 folders, included numerous personal details, amongst which were names, addresses and even information about the personal income. The local media reported on the hacking which happened in July 2019. The hacking occurred when a link was sent to Bulgarian media via email of a free Russian email service. The news broke afterward.

As reported by the *Tax Notes Today International*, a non-profit daily tax publisher, the hacking 'involved financial account information shared among countries under the Organization for Economic Cooperation and Development common reporting standard'. The media concluded that 'this breach compromised personal, tax and social security information of about four million Bulgarian citizens. This was the first leak of the kind under the common reporting standard and it shows how difficult it is to protect data in this day and age'.

According to the National Revenue Agency (NRA), the breach exposed the data of 5.1 million Bulgarians, including 1.1 million deceased.

The country's finance minister, Vladislav Goranov, apologised in parliament for the breach. In August 2019, as reported by the Commission for Personal Data Protection, the National Revenue Agency was fined USD 2.9 million for failing to stop the data breach.

Bozhidar Bozhanov, national security specialist in his blog *bozho.net* discusses in greater detail how and why most possibly the personal data breach occurred. Bozhanoz says that one of the reasons for the inadequate information protection and failures is that the proposals of information security experts consulting the state institutions were blocked. In the light of this Bozhanov recommends a series of information security measures to be taken on board. According to him, there is a key GDPR principle that must be followed in order to escape abuse of data - the principle of minimizing databases available and keeping these databases only until they are needed. Opposing this, the agency tends to make copies of databases from other administrations on a daily basis and they are kept forever.

Another good model of handling data recommended by the GDPR is information encryption. According to Bozhanov, if the sensitive data leaked by NRA had been encrypted in a certain way, the hack, in case it was an SQL injection, would not have happened.

Project Number 762128
CALL: H2020-ICT-2016-2017
TOPIC: ICT-19-2017

Specialists such as Bozhanov emphasize the necessity of a full audit implemented for all administrative security systems, not just related to the Ministry of Finance, but-on a general state level. Information security and data protection training for all employees in the respective IT directorates should be carried out regularly. Another recommended measure is the so called responsible disclosure, according to which Bozhanov adds, people with found vulnerabilities can report without the fear that they will be sanctioned.

An essential conclusion reported by the experts is that Bulgarian business has factually invested a lot in order to comply with the GDPR requirements. However, it turned out that state institutions remained the most unprepared for the changes entailed by the execution of the new European regulation at the end of the day.

Compiled by Media 21 Foundation from:

- **https://www.bbc.com/news/technology-49015511**
- **https://www.novinite.com/articles/198593/SUMMARY%3A+Hackers+have+Penetrated+the+Bulgarian+National+Revenue+Agency+through+the+Tax+Refund+System**
- **https://www.bnt.bg/en/a/check-launched-into-revenue-agency-over-taxpayers-data-leak-after-hacker-attack**
- **https://www.mediapool.bg/personal-data-of-millions-of-bulgarians-leaked-after-cyber-attack-against-national-revenue-agency-procedure-for-electing-new-p-news295924.html**