

## Key actors

### Kaldamukov, Dinev, Bliznakova & Mandazhieva Legal Services (KDBM Law)

KDBM Law is an independent law firm based in Bulgaria. Its legal advisers carry out work across a range of areas and industries throughout the EU. KDBM lawyers hold notable expertise in information technology, e-commerce, data protection and intellectual property.

### Digital Republic

Digital Republic is a Bulgarian NGO that brings together internet users, authors, computer specialists, entrepreneurs and lawyers. Its mission is to stand up for the rights of internet users and to uphold access to information. Its aim is to support the development of technology for the benefit of society and to uphold civil and human rights.

### Bulgarian citizens

There are a growing number of Bulgarians who are supporting this collective action. They are not seeking financial compensation for the harm caused by the data leak, but instead want to compel the Bulgarian government to review the way that it stores personal data and ensure that adequate security measures are put in place in the future.

DFF

Digital  
Freedom Fund

The Digital Freedom Fund (DFF) supports partners in Europe to advance digital rights through strategic litigation. This is one of a series of case studies, which highlight the work of DFF's grantees working to protect digital rights.

## Class Action Case Against the Bulgarian National Revenue Agency

Case facts at a glance

### Court:

Sofia City Court

### Filing date:

KDBM Law has the court documents drafted and will be ready to file the case as soon as they have established sufficient public support.

### Case goal:

A successful outcome in this case would compel the Bulgarian government to improve the way it stores and protects its citizens' personal data. It would also help Bulgarians to understand that their personal data is important and yet currently not adequately protected. The hope is that this case will force the Bulgarian National Revenue Agency (NRA) to review how a hacker was able to breach its security systems and explain this to the millions of people who were affected by the attack.

## Background to the case

On 15 July 2019, Bulgaria experienced its worst ever cyberattack. An anonymous hacker breached the security systems of the Bulgarian National Revenue Agency (NRA) and downloaded personal information and financial details of nearly every working adult in the country. The data included social security information, addresses, incomes, and names. The hacker then released the information to local news outlets and online media.

Bulgaria's National Data Protection Authority (NDPA) carried out an investigation and concluded that the NRA had committed gross violations of personal data security. It fined the NRA 5.1 million BGN (which equates to 2.6 million EUR).

Lawyers from KDBM Law are bringing a case against the NRA because of its failure to protect people's data. They are arguing that the NRA violated the Bulgarian Data Protection Act and the General Data Protection Regulation (GDPR). KDBM Law want to show that government institutions should put in place robust systems to prevent cyberattacks. But they also want to make it clear that citizens deserve to be told about a data breach and to be informed about the action that is being taken to address the situation.

“Every institution can be hacked, and people know this. But people were very upset about the government's reaction to the leak. The data breach is just a sign that we have a bigger problem in this country.”

Dimitar Kaldamukov, lawyer, KDBM Law

## Diffusing the ticking time bomb of weak cyber security

Cyberattacks are worryingly all too common throughout the world and are becoming increasingly sophisticated and dangerous. Europe has been hit hard, not just in Bulgaria but with serious security breaches recently in North Macedonia, Turkey and Greece. The damage these malicious attacks cause is extremely harmful resulting in interruptions to business, potential theft and malicious use of personal data. These attacks also generate a deep mistrust of government institutions when they are entrusted with personal data but fail to keep it safe.

In an age where so much personal data is collected and stored digitally, it is a reasonable expectation that this information will be protected and kept secure. And yet not enough is being done to prioritise safe and secure measures to store data, particularly by government institutions. What is particularly worrying in the Bulgarian case is that some experts believe the hacker used relatively basic techniques to obtain the data.

There are now hundreds of individual claims for damages being directed at the Bulgarian government. But KDBM Law's collective action case has a broader objective. It wants Bulgarian citizens to understand how vitally important it is that their data is protected securely and it wants to compel the Bulgarian government to explain the actions they will take to put in place necessary security protections in the future.

**“ Bulgarians are being deprived of state administrative services. This data breach shows that our government is not ready to provide even basic data protection in 2020.**

Dimitar Kaldamukov, KDBM Law

### Strength in numbers – the power of collective action

This case is distinctive because of how far-reaching the attack was. The majority of adults had their data stolen – it affected 5 million people in a country of only 7 million. KDBM Law are filing a collective claim against the NRA on behalf of all the people who have had their data stolen.

In Bulgaria, there is a formal requirement to prove sufficient public support for a collective action case to proceed. KDBM Law is actively publicising the case and has created a website that allows people to sign a petition to support the case or formally join the litigation. It is working with the NGO Digital Republic and already has a number of people committed to the case. This is an unusual type of claim as it will not result in compensation being awarded, instead it will compel the NRA to protect people's data in the future.

Overwhelmingly, there is considerable outrage and indignation from the general public about how such a serious breach could have taken place. KDBM Law recognises that there is strength in numbers and is taking steps to create greater awareness of the case. Its advocacy campaign is seeking to show how the case could result in people's data being more securely stored and protected in the future.

**“ We want to show people that when the government commits such a gross omission and negligent breach of personal data, they have the power to protect themselves through the courts.**

Dimitar Kaldamukov, lawyer, KDBM Law

### DFF's role



#### Financial assistance

DFF provided financial support to KDBM Law so that it could take on this case. This was essential as KDBM Law needed to prove to the Court that it had sufficient resources to take on the case, pay for experts, publications and other case materials.



#### Support for collective action

To file a collective claim in Bulgaria, the Court imposes a requirement that the claimant must demonstrate it has sufficient finances to bring the case. Without DFF's support this collective action would not be possible.