Track Changes

September 2019

BULGARIA: FINES IN MILLIONS FOR PERSONAL DATA BREACHES

On 29 August 2019 the Bulgarian Commission for Personal Data Protection ("**CPDP**") announced first significant fines under the GDPR[1] for data processing breaches. The fines, which in total are more than 6 million Bulgarian levs (approx. 3 million EUR), clearly indicate the CPDP intention for strong measures in cases of data leakages, irrespective of whether they concern public authorities or private entities.

BACKGROUND OF THE CASES

– National Revenue Agency ("**NRA**")

On 15 July 2019 an anonymous hacker successfully breached the security systems of the Bulgarian National Revenue Agency ("**NRA**") and downloaded the personal data of over 5 million Bulgarian citizens. Part of the hacked information (about 11 GB) was leaked to local media. This is the biggest personal data breach in Bulgaria up to present date. After the initiated inspection and discovery of highly insufficient measures for protection of personal data the CPDP fined the Bulgarian NRA with a 5.1 million BGN (about 2.5 million EUR).

– OTP Group subsidiary

In the second case, the CPDP fined Bulgaria's DSK Bank (part of the OTP Group) for a data breach as a result of which personal data of more than 30 000 clients were unlawfully accessed by third parties. The affected personal data include identification data (name and PIN), as well as copies of ID cards, addresses, social security and tax data, bank accounts, personal data of third related parties (e.g. spouses, guarantors, etc.). The amount of the sanction imposed by the CPDP is 1 million BGN (approx. 500 000 EUR).

These recent events once again evidence that all organizations – public and private, are exposed to the increasing risk of cyberattacks and data breaches. According to the statistics of the CPDP, during the period 25 May 2018 - 31 March 2019 a total of 53 data breach cases were reported. The recent fines show that organizations can further a stringent approach by the local regulator and significant sanctions.

No company can completely eliminate the risk of a data breach regardless of the efforts and

[1] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**")

diligence in ensuring internal organization and security measures. Thus, the question arises on the most adequate steps in case of a data breach and what actions can possibly mitigate the adverse effects.

WHAT IS A "PERSONAL DATA BREACH"?

Under the GDPR, personal data breach refers to *any breach* of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (**"Data Breach"**). Although Data Breaches are usually related to targeted cyber-attacks, a variety of different circumstances and even some unintentional actions can result in a Data Breach (e.g. loss of company phone, laptop or USB; breakdown of IT systems or hardware; physical destruction of data (in case of fire, theft), etc.)[2]. Data Breaches may affect the personal data of the organizations' own employees, business partners, clients and their employees, as well as any other individuals the company interacts with.

WHAT ACTIONS SHOULD BE UNDERTAKEN UPON A DATA BREACH?

1. Becoming aware of a Data Breach

All notification and further obligations of a data controller in case of a Data Breach under the GDPR and the Bulgarian data protection legislation are triggered after an organization becomes aware of a Data Breach. To ensure compliance with GDPR and local legislation, it is critical to know when a data controller is considered "aware" of the Data Breach. Within the meaning of the GDPR, the data controller will be regarded as "becoming aware" when it has established with a reasonable degree of certainty the occurrence of a security incident that has resulted in the compromising of personal data. As the exact moment of "becoming aware" would depend on the specific facts and circumstances, in all cases of suspicion of a Data Breach organization should immediately focus on investigating the incident to determine whether and to what extend any personal data have been affected.

2. Immediate actions within the first 24 hours

The GDPR leaves the initial assessment of a Data Breach to self-estimation of the data controller and its internal policies and procedures. However, although not regulated, the initial steps of the data controller are subject to the supervision of the CPDP for efficiency and adequacy as they pre-determine any follow up actions to counteract to the Data Breach. In order to promptly manage and contain a Data Breach, an organization may consider taking the following immediate practical steps within the first 24 hours[3]:

- notify the Data Protection Officer/other responsible person within the organisation and provide him/her with all available information about the incident;

---

2 Pursuant to the CPDP's statistics, in Bulgaria the majority of the reported Data Breaches were related to unauthorised disclosures of personal data to third parties, caused by (i) technical mistakes by a person within the organization; (ii) technical issues with the IT systems; (iii) unauthorised access of external parties by way of malicious attacks to the company systems; (iv) different types of cyber-crimes. Another part of the reported Data Breaches was caused by natural disasters, such as fires in the company buildings or premises where the systems for personal data processing are located.

3 The WP29 Guidelines on Personal data breach notification were endorsed by the European Data Protection Board during its first plenary meeting.

- carry out an initial investigation and assessment of the Data Breach and the potential risk to the rights of the individuals concerned;
- implement appropriate technical and organizational measures to seize and mitigate the Data Breach – amongst others such measures can include: freeze all affected devices in order to limit further exposure; isolate the impacted systems to minimize the risk of further damage; change all passwords and log-on credentials; contact the system administrator to activate additional IT-security software, etc.;
- properly document all steps and actions concerning the Data Breach throughout the investigation and remedial process, as the competent supervisory authority may use this documentation to supervise compliance with the GDPR.

3. Actions within the first 72 hours

If the initial assessment of the Data Breach has evidenced that the Data Breach creates "a risk" to the rights and freedoms of natural persons[4], the data controller will be obliged to notify the competent lead supervisory authority not later than 72 hours as of becoming aware of the Data Breach. If for any reason the 72 hours term cannot be met the delay should be justified to the supervisory authority. Otherwise the latter can impose a fine at the amount of the highest of 10 million Euros or 2 % of the global turnover of the controller.

The notification of the Data Breach should contain at least the following information:

- the nature of the Data Breach, and where possible, the categories and approximate number of data subjects concerned/categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the Data Breach;
- the measures taken or proposed to be taken to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

In case it is impossible to provide the above information at once in its entirety, it is recommendable to file an initial notification containing the available part of the required information in order to keep the 72 hours deadline and provide the supervisory authority with the remaining details of the Data Breach at a later stage. In such way, the controller may mitigate the risk of the abovementioned sanction for delay in notification.

4. Follow-up actions vis-à-vis the affected data subject(s)

If the initial assessment of the Data Breach shows that there is a *high* risk[5] for the rights and freedoms of the natural persons, the data subjects affected by the breach should also be

---

4 Recital 85 of the GDPR explains that such risk exists if the Data Breach may result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

5 Pursuant to the WP29 Guidelines on Personal data breach notification, a high risk exists in the cases where the Data Breach has a more severe potential or actual impact on individuals and the likelihood of the negative consequences to the natural persons is greater, based on the type of breach, the nature, sensitivity and volume of the affected personal data, the special characteristic of the data controller or the data subjects and the number of the affected individuals.

notified without undue delay in addition to the notification to the competent supervisory authority. The notification to the data subjects should describe in *clear* and *plain* language the nature of the data breach and contain at least the same information as the notification to the competent supervisory authority (see letter b) above), as well as specific recommendations on how to mitigate the adverse effects of the Data Breach.

Even where the Data Breach results in a high risk for the rights and freedoms of the natural persons, a notification to the affected data subjects would not be required where:

- the data controller has implemented and applied appropriate technical and organisational protection measures to the affected personal data (in particular measures rendering the personal data unintelligible to any person who is not authorised to access it);
- the data controller has taken subsequent measures ensuring that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- it would involve disproportionate efforts for the data controller to notify the affected data subjects; instead, a public communication (or other similar measures) should be made to effectively inform the affected data subjects.

In addition, it should also be considered if any other notification requirements under applicable legislation may also be triggered by the Data Breach.[6]

WHAT IF WE FAIL TO COMPLY WITH THE NOTIFICATION REQUIREMENTS?

Organizations should be aware that failure to comply with the notification requirements under the GDPR may have serious negative consequences:

i. an administrative fine of up to 10 million euros or 2% of the company's global turnover;
ii. exercise by the competent supervisory authority of its investigative and corrective powers (e.g. data protection audits, issuance of mandatory instructions, limitation of data processing operations, etc.);
iii. direct claims by the affected data subjects before the Bulgarian administrative courts for any damages suffered as a result of the Data Breach;
iv. reputational damages for the company.

As reference, for the period 25 May 2018 - 31 March 2019 the CPDP has exercised its investigative powers to obtain access to premises only in 6 Data Breach cases, whereas in 17 cases the authority reviewed the incident based only on the provided documentation. In 30 of the 53 reported Data Breach cases the CPDP did not impose any corrective measures due to the low risk for affected individuals as a result of the breach.

6 For example, if the data controller is also an operator of essential services (e.g. in the energy, healthcare, banking sectors, etc.), if it provides digital services (namely online marketplaces, online search engines and cloud computing services) or if it provides public services (such as educational, health, telecommunications, financial services, etc.) and also provides on-line administrative services, it should also notify all cybersecurity incidents that affect the uninterruptedness of the provided services to the competent cybersecurity sector response team within 2 hours as of establishment of the Data Breach. Within the following five days a second notification containing all available information concerning the Data Breach should be submitted to the competent cyberattack sector reaction team with the State Agency "Electronic governance".

TAKEAWAYS

To limit the risks of Data Breaches, it is recommended for organisations to carry out a reassessment of their internal security procedures and identify any weak spots in the implemented technical and organisational security measures. It is important for the business to remain proactive about data security and make continuous efforts to ensure the protection of the commercial information and personal data processed in the scope of the business operations of the company.

About WOLF THEISS

Wolf Theiss is one of the leading law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We have built our reputation on a combination of unrivalled local knowledge and strong international capability. We opened our first office in Vienna almost 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region.

For more information about our services, please contact:

Anna Rizova
Partner
anna.rizova@wolftheiss.com
T: +359 (0)2 8613 700

Hristina Dzhevlekova
Senior Associate
hristina.dzhevlekova@wolftheiss.com
T: +359 (0)2 8613 700

Contributors:

Zhulieta Markova
Associate
zhulieta.markova@wolftheiss.com
T: +359 (0)2 8613 700