DINOVA RUSEV & PARTNERS

LEGAL ALERT, NOVEMBER 2018

THE NEW BULGARIAN CYBERSECURITY ACT

I. Introduction

Bulgarian State Gazette No. 94 of 13.11.2018 introduced a new legislative act – the Cybersecurity Act, implementing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

The new legislation is focused mainly on creating obligations for public administrative bodies regarding provision of high level of cybersecurity. However, some private entities also fall within its scope.

II. Obliged persons from the private sector

The following groups of private legal entities are to comply with the new Cybersecurity Act:

1. Operators of essential services in the following sectors: energy (including oil and gas), transportation, banking, financial market infrastructures, health sector, drinking water supply/distribution and digital infrastructure;

2. Digital service providers;

3. Organizations providing electronic administrative public services. This third group covers a large number of legal entities and it is expected more the business activities meeting this criteria to be further clarified.

III. Obligations

The new Cybersecurity Act provides for two main groups of obligations for compliance:

1. Implementation of cybersecurity measures

Basically, the obliged persons are to ensure proper measures for:

- technical and organisational security risk management of their networks and information systems used on the territory of the Republic of Bulgaria; and
- measures for prevention and minimisation of security breaches.

The matters regarding accountability and compliance with this requirement are expected to be additionally specified with the issuance of a new order by the Council of Ministers by the middle of May 2019 (if the term remains unchanged).

For more information please contact:

Anelia Dinova – Partner

Anelia.Dinova@drp-legal.com

Vesela Kabatliyska – Partner

Vesela.Kabatliyska@drp-legal.com

P: +359 (0)2 943 4350

2. Notification of incidents

The persons per Item II above are obliged to notify the respective authorities competent for the specific business activity in case of cyber security incident. These competent authorities (computer security incident response teams or 'CSIRTs') will be established within 4 months as of the entry into force of the Cybersecurity Act, i.e. in March 2019.

The Cybersecurity Act provides for very short terms for security incidents notification, namely:

- initial notification within **two hours** from the ascertainment of the incident; and
- provision of the full information regarding the incident – **within five business days**.

III. Sanctions under the Cybersecurity Act

The new legislation provides for fines (for individuals) and monetary sanctions (for legal entities) in the range from BGN 1,000 to 15,000 (for first infringement) and from BGN 2,000 to 25,000 (for second infringement).

The sanctions are to be imposed in the following cases:

1. Non-compliance with the notification requirements;

2. Non-provision of information or non-compliance with given instructions; and

3. Other infringements of the Cybersecurity Act.

For more information please contact:

Anelia Dinova – Partner

Anelia.Dinova@drp-legal.com

Vesela Kabatliyska – Partner

Vesela.Kabatliyska@drp-legal.com

P: +359 (0)2 943 4350