DATA PROTECTION newsletter
4 December 2018

New cybersecurity law imposes security and reporting obligations to Operators of Essential Services and Digital Service Providers

The Greek Parliament recently enacted Law 4577/2018, the purpose of which is to transpose Directive (EU) 2016/1148 on security of network and information systems (the NIS Directive) into Greek law.

Which enterprises are affected?

The new cybersecurity law sets a range of network and information security requirements which apply to Operators of Essential Services (OESs) and Digital Service Providers (DSPs).

OESs include enterprises in the energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure sectors. The identified OESs established in Greece will be set forth by a decision of the Minister of Digital Policy, Telecommunications and Information following the opinion of the National Cybersecurity Authority (NCA).

DSPs include cloud service providers, online marketplaces and search engines.

Which are the competent authorities?

The law designates as the National Cybersecurity Authority the already existing Cybersecurity Directorate of the General Secretariat of Digital Policy of the Ministry of Digital Policy, Telecommunications and Information. Its role is to monitor application of the new cybersecurity regime and to serve as national single point of contact for network and information security, acting also as liaison ensuring cross-border inter-regulatory cooperation within the EU.

Moreover, the Cyberdefence Directorate of the Hellenic National Defense General Staff is appointed as the national Computer Security Incident Response Team (CSIRT) and is responsible for risk and incident handling at national level.

NCA will work together with the CSIRT to evaluate the technical and organisational measures implemented by OESs and DSPs and their adequacy for the prevention and minimisation of an incident's impact on the security of their information systems.

When should a security incident be notified and how?

Pursuant to the law, OESs are obliged, under certain circumstances, to notify incidents in their security and information systems that have a significant impact on the continuity of their essential services. DSPs should notify incidents that have a substantial impact on the provision of the services that they offer. The process to be followed for an incident notification will be determined by the NCA and the CSIRT. Additionally, it is not clear whether OEDs and DSPs should notify a security incident only to CSIRT or both to CSIRT and the NCA. We note that personal data breach notifications according to the GDPR remain unaffected.

What are the sanctions?

Violations of the law may result in the imposition of administrative fines imposed by the Minister of Digital Policy, Telecommunications and Information, following proposal by the NCA. Fines range from Euro 15,000 to Euro 200,000 depending on their gravity and repetitiveness.

For further details please contact:

Takis Kakouris
T (+30) 210 69 67 000
E t.kakouris@zeya.com

Mary Deligianni
T (+30) 210 69 67 000
E m.deligianni@zeya.com