www.privacyromania.ro

January 29-30, 2021

PRIVACY ROMANIA 2021

Romanian National Conference on Privacy and Data Protection

IMPLEMENTATION OF THE NIS DIRECTIVE IN ROMANIA - COMMON GROUND WITH GDPR

ASCPD

Asociația Specialiștilor în Confidențialitate și Protecția Datelor

Daniela SIMIONOVICI

Vice President of ASCPD Romania

Senior Partner NeoPrivacy Romania

ASCPD

Asociația Specialiștilor
în Confidențialitate
și Protecția Datelor

ASCPD | Asociația Specialiștilor în Confidențialitate și Protecția Datelor

www.ascpd.ro

IMPLEMENTATION OF THE NIS DIRECTIVE IN ROMANIA - COMMON GROUND WITH GDPR

Daniela Simionovici
Vicepresident ASCPD
Senior partner Neoprivacy Romania

29.01.2021

The adoption of 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, reflects the constant concerns of the Community authorities in recent years regarding the increasing resilience of IT&C infrastructures belonging to the operators of essential services and digital service providers in the Member States.

The NIS Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

- The NIS directive is NOT a new cyber security law!
- The NIS directive is NOT about national defence and security.
- The NIS directive targets the market and services!

The Directive focuses on the risks posed by security incidents to the conduct of economic activities, the potential financial losses that companies, citizens or administrations of the Member States may incur, and the intentional or unintentional disruption of networks / information systems that support essential services for society and which may affect several Member States at the same time.

The transposition in the national legislation of the NIS Directive was made by Law no. 362/2018 on ensuring a high common level of security of networks and information systems and entered into force on 12 January 2019.

The normative act has a special importance for Romania, because it transposes at national level the NIS Directive no. 1148/2016 and aligns Romania to a common European framework for responding to cyber security incidents.

Simply put, the implementation of the provisions of the NIS Directive by transposing them into national NIS laws creates the framework to ensure the continuity of essential services whose provision depends on networks and information systems.

Next, we will analyse the provision of essential services, insofar as the provisions of the NIS Directive are intertwined with those of the GDPR.

The importance of personal data protection from the perspective of the NIS Directive can be immediately noticed from the fact that one of the first articles of the Directive, more precisely art. 2 refers to the protection of personal data.

The Law 362/2018 applies to entities providing services in the following sectors: energy, transport, banking, financial market infrastructure, health sector, drinking water supply and distribution and digital infrastructure.

We can easily identify the sectors in which a large volume of personal data is processed (such as the sectors that supply electricity, natural gas or drinking water to final beneficiaries, the banking sector or the financial markets infrastructure sector), as well as a large volume of personal sensitive data (such as health data and more).

For example, regarding the segments and the way in which the NIS and GDPR Law intertwine, we will use the health sector.

In Romania, the National Cyber Security Incident Response Center - CERT-RO is the competent national authority for the security of networks and information systems that provide essential services or provide digital services identified under the NIS law.

By Order 601/2019 for the approval of the Methodology for establishing the significant disruptive effect of incidents at the level of networks and information systems of the operators of essential services, no thresholds / limits were set for the health sector, and consequently no threshold values are established for a certain service (P = "No"), which shows that the degree of disruption resulting from the interruption of the provision of essential services in the health sector is significant, namely, HIGH.

Even if there are operators in the medical sector whose activity does NOT depend on a network or an information system (such as a dental office with a single dental unit, which uses only one phone for patient appointments, and has not signed a contract with the national health insurance house, therefore the provision of the medical service and its payment does not depend on an internet connection and an application connected to the national health insurance system), the simple fact that no threshold values have been provided for this sector means that ALL operators in this sector are operators of essential services - OESs and the services provided by them ARE essential services - ESs and fall under the provisions of the NIS law.

Therefore, any disruption in the provision of these services is considered to have a significant negative impact in the community / society, and operators are required to ensure a high level of security of the networks and information systems they use.

Networks and information systems are no longer used in a hospital, for example, only for the administrative management of its activity (registration of patients, management of medical procedures or medicines, preparation and issuance of medical documents, intra-institutional electronic communication, etc.), but are also used for the activation and use of configurable devices [including computed tomography (CT) systems, ultrasound systems, anesthesia systems, physiological monitoring systems, radiological information systems (CRS)], or for activating control equipment and devices, and management of access to operating rooms (access might be allowed on the use of personalized access cards, and the opening of a door might depend on an application / computer system, but also on the power supply, therefore, even if the network / computer system is not the victim of a hardware malfunction or a cyber attack, may be the victim of a common power outage, with equally significant negative effects, especially when the interruption of the provision of essential services, even for extremely short periods, can make a difference for a patient in serious condition, regardless of whether the interruption was due to a broken computer, a "frozen" application or a power failure).

The common and largest ground on which the NIS and GDPR Act meet and interfere is that of technical and organizational measures for the security of networks and information systems.

Both legislative norms have clear provisions regarding the aspect of ensuring the security of networks and information systems which, in the case of the NIS Law refers to ensuring the continuity of essential services under art. 10, para. 1, lit. b) of the NIS Law: "[*operators of essential services*] implement appropriate measures to prevent and minimize the impact of incidents that affect the security of the networks and information systems used for the provision of these essential services, in order to ensure the continuity of those services, established under the provisions of art. 25 para. (3) ", and in the case of GDPR it refers especially to the compliance with the principle of "integrity and confidentiality" - art. 5, para. 1, lit. f) GDPR, which makes explicit reference to the fact that personal data are "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

29.01.2021

Both legislative norms have clear provisions regarding the identification and notification of security incidents, but in this chapter there is also the first difference between the two normative acts: GDPR applies to security breaches that generate “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed” - art. 32, para. 2 GDPR, regardless of the number of data subjects affected, while, according to the NIS Law, operators of essential services “c) immediately notify CERT-RO as a national Computer Security Incident Response Team - CSIRT of incidents that have a significant impact on the continuity of essential services by providing at least the information provided in art. 26 para. (3);" - art. 10, para. 1, lit. b) of the NIS Law.

The significant impact on the continuity of essential services could imply that if the incident did not fall into this category ("significant impact"), there would be no obligation to notify it to CERT-RO.

On the other hand, given the "0" threshold value for the health sector mentioned above, it would follow that any security incident resulting in the interruption of the provision of medical services, regardless of the number of patients affected, should be reported to CERT -RO (for example, if the interruption of the provision of medical services endangers the health or the life of even a single person, or results in the death of a patient, we consider that we are facing a significant impact of the security incident).

It is unclear, however, whether the CERT-RO notification is required in this scenario of only one patient affected, or not. It is also unclear whether the interruption of the provision of essential services in the same scenario proposed by us falls into the category of security breach and requires notification of the supervisory authority, given that we could face a situation where personal data availability.

Another common segment of the two normative acts is that of notification / information to data subjects (GDPR) / general public (NIS) in case of an incident / security breach but the common ground stops here.

In the case of the NIS Law, art. 29 states that "(1) CERT-RO may notify the public, when information is necessary to prevent an incident or to manage an ongoing incident. (2) For incidents affecting an operator of essential services or a digital service provider, the information referred to in para. (1) shall be carried out after prior consultation with him/she [*operator of essential services*] on the content of the notification.".

We consider that this provision of the national law is a transposition of recital (59) of the EU-NIS Directive: "(59) [...] Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the operators of essential services and digital service providers reporting incidents. [...] ".

We note that CERT-RO may notify the public for the prevention of a security incident or for the management of an ongoing incident, only after consulting with the operators of essential services on the content of this notification, i.e. on what and how much can be made public.

With regard to the notification of the data subject, the GDPR is much more sharp and obvious in favour of the data subject, and this can be easily seen in the official statements on the GDPR fines imposed, in the sense that the controllers reputation seems to be the last concern of the national supervisory authorities.

In order to support all those targeted by the NIS Law, but also of practitioners in personal data protection, together with my colleague, Marius Dumitrescu, I developed, for the first time in Romania, a course support that was, in fact, the basis to my presentation today.

The implementation course of the NIS Law that we propose also involves a certification, which can be obtained by passing a test based on 100 questions from the NIS Directive, from Law 362/2018, from our course support, but also from the other normative acts and guides provided by CERT-RO.

The course support is very detailed and explicit and was made from the perspective of the practitioner, who is obliged to always answer the question "HOW do I apply what the law requires?". The answer to this question under the NIS law is very similar, moreover, with respect to the principle of responsibility in the GDPR.

ASCPD | Asociația Specialiștilor în Confidențialitate și Protecția Datelor

www.ascpd.ro

29.01.2021

As a general conclusion, we can say that at least the Law 362/2018 may suffer further, even substantial improvements in some respects, for a real and an effective harmonization with the provisions of GDPR.

As we have demonstrated during this presentation, not only the NIS Law has a significant impact on the GDPR, but also non-compliance with technical and organizational measures for the protection of personal data can have a significant negative impact on the provision of essential services covered by the NIS Law.

The two normative acts do not intersect at a single point, after which “each goes his own way”, or do not have parallel paths, but intertwine, and impact each other on a very consistent and important part for the society, as a whole, and for individuals, in their uniqueness.

Daniela Simionovici

Email: daniela.simionovici@ascpd.ro

Mulțumesc