Ministerstwo Zdrowia
Sekretarz Stanu
Waldemar Kraska

Warszawa, 11 sierpnia 2022 r.

DI.553.7.2022.PM

**Pan**
**Tomasz Grodzki**
**Marszałek Senatu RP**

*Szanowny Panie Marszałku,*

w nawiązaniu do oświadczenia złożonego przez senatora Wojciecha Koniecznego podczas 45. posiedzenia Senatu RP w dniu 30 czerwca 2022 r. (znak BPS/043-45-1740/22) uprzejmie proszę o przyjęcie poniższych wyjaśnień.

Celem ustawy o krajowym systemie cyberbezpieczeństwa[1] (dalej: KSC) było opracowanie uregulowań prawnych umożliwiających implementację Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[2] (dyrektywy: NIS) oraz utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego na poziomie krajowym. Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w szczególności :

- niezakłóconego świadczenia usług kluczowych i usług cyfrowych,
- osiągnięcia odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług.

Należy zauważyć, że KSC wprowadza pewien system zarządzania cyberbezpieczeństwem na poziomie krajowym, jednak już wcześniej ustawą o informatyzacji[3] z 2005 roku, jak również rozporządzeniem o Krajowych Ramach

[1] Ustawa z dnia 5 lipca 1018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z2020 r., poz. 1369 z późn. zm.)
[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Directive concerning measures for a high common level of security of network and information systems across the Union) (Dz. U. L 194 z 19.7.2016)
[3] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070, z 2022 r. poz. 1087).

Ministerstwo Zdrowia
ul. Miodowa 15
00-952 Warszawa
Telefon: +48 22 53 00 261
fax: +48 22 831 21 66
e-mail: sekretariat-wk@mz.gov.pl
www.gov.pl/zdrowie

Interoperacyjności[4] z 2012 r. (dalej: KRI) zostały określone obowiązki związane z zapewnieniem bezpieczeństwa informacji. Obowiązki te zostały nałożone na szereg podmiotów publicznych, w tym na samodzielne publiczne zakłady opieki zdrowotnej (SPZOZ) oraz spółki wykonujące działalność leczniczą, w rozumieniu przepisów o działalności leczniczej (pełen katalog w art. 2. ustawy o informatyzacji). W intencji ustawodawcy KSC podmioty, które podlegają ustawie o informatyzacji, wdrażające usługi świadczone drogą elektroniczną, powinny dołożyć należytej staranności celem zapewnienia bezpiecznego funkcjonowania tych usług. W procesie projektowym oraz utrzymania usług koszty zapewnienia cyberbezpieczeństwa są naliczane normatywnie. Trzeba mieć także na uwadze, że SPZOZ, co do zasady mają zaimplementowany system zarządzania bezpieczeństwem informacji (SZBI).

Chcąc wspomóc szpitale w podniesieniu poziomu cyberbezpieczeństwa Minister Zdrowia, wspólnie z pełnomocnikiem Rządu do Spraw Cyberbezpieczeństwa, przeznaczył 500 mln zł na dofinansowanie szpitali w realizacji działań związanych z bezpieczeństwem. Realizacja zadania dystrybucji środków została zlecona Narodowemu Funduszowi Zdrowia. Zasady uzyskania dofinansowania reguluje zarządzenie nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia. Biorąc pod uwagę obowiązki wynikające z KRI, ciążące na SPZOZ, powyższy fundusz ma za zadanie dofinansować szpitale, a nie pokrywać pełne koszty zapewnienia cyberbezpieczeństwa, które powinny być uwzględnione już na etapie wdrażania systemów lub usług elektronicznych.

Warto także zauważyć, że podmioty lecznicze powinny zapewnić cyberbezpieczeństwo swoich systemów teleinformatycznych i urządzeń medycznych kontrolowanych przez systemy teleinformatyczne nienależnie od wymogów prawnych. Podejście takie jest zgodne ze sztuką inżynierii komputerowej oraz dobrymi praktykami zarządzania IT.

Niezależnie od powyższego podejmowane są działania mające na celu wspieranie podmiotów w realizacji ich obowiązków. Poza wspomnianym powyżej dofinansowaniem, wynikającym z zarządzenia nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia, zachęcamy podmioty do zapoznawania się z zasadami ubiegania się o środki pochodzące ze źródeł unijnych i aplikowania o dofinansowanie projektów dedykowanych cyberbezpieczeństwu m.in. w Krajowym Planie Odbudowy, Funduszach Europejskich na Rozwój Cyfrowy (FERC) czy też Regionalnych Programach Operacyjnych.

[4] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych ( Dz. U. poz. 526 z późn. zm.).

*Z poważaniem*

Waldemar Kraska

Sekretarz Stanu

/dokument podpisany elektronicznie/