# CYBERBEZPIECZEŃSTWO W SAMORZĄDZIE TERYTORIALNYM

## Praktyczny przewodnik

Wojciech Dziomdziora

Wolters Kluwer

# CYBERBEZPIECZEŃSTWO W SAMORZĄDZIE TERYTORIALNYM

## Praktyczny przewodnik

# CYBERBEZPIECZEŃSTWO W SAMORZĄDZIE TERYTORIALNYM

## Praktyczny przewodnik

Wojciech Dziomdziora

Wolters Kluwer

WARSZAWA 2021

Stan prawny na 1 stycznia 2021 r.

Wydawca
Anna Kubuj-Kacperek

Redaktor prowadzący
Paulina Ambroży

Opracowanie redakcyjne
Agnieszka Witczak

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski



ISBN 978-83-8223-413-8 *ISBN PDF-a: 978-83-8223-958-4*

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

Pracę tę poświęcam
nieodżałowanemu prof. Michałowi Kuleszy,
mojemu nauczycielowi

# SPIS TREŚCI

# WYKAZ SKRÓTÓW

## Akty prawne

**dyrektywa NIS** – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1)

**RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)

**rozp. KRI** – rozporządzenie Rady Ministrów z 12.04.2012 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. z 2017 r. poz. 2247)

**u.ABW** – ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2020 r. poz. 27 ze zm.)

**u.i.d.p.** – ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r. poz. 346 ze zm.)

**u.k.s.c.** – ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 ze zm.)

**WIIP** – uchwała nr 97 Rady Ministrów z 11.09.2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (M.P. poz. 862)

## Inne

| | | |
|---|---|---|
| **CSIRT** | – | Computer Security Incident Response Team (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) |
| **Dz.U.** | – | Dziennik Ustaw |
| **Dz.Urz. Min. Fin.** | – | Dziennik Urzędowy Ministra Finansów |
| **Dz.Urz. UE** | – | Dziennik Urzędowy Unii Europejskiej |
| **EOG** | – | Europejski Obszar Gospodarczy |
| **ePUAP** | – | Elektroniczna Platforma Usług Administracji Publicznej |
| **MAiC** | – | Ministerstwo Administracji i Cyfryzacji |
| **MF** | – | Ministerstwo Finansów |
| **M.P.** | – | Monitor Polski |
| **NIST** | – | National Institute of Standards and Technology |
| **PBI** | – | polityka bezpieczeństwa informacji |
| **SCCO** | – | Standardy Cyberbezpieczeństwa Chmur Obliczeniowych |
| **UODO** | – | Urząd Ochrony Danych Osobowych |

# WSTĘP

Stan cyberbezpieczeństwa, w szczególności bezpieczeństwa informacji, w jednostkach samorządu terytorialnego jest niewystarczający, co potwierdzają oficjalne dokumenty[1]. Jednocześnie aktywność cyberprzestępców rośnie, a jednostki samorządu terytorialnego stają się ich coraz łatwiejszym i atrakcyjniejszym łupem. Wraz z wejściem w życie ustawy o krajowym systemie cyberbezpieczeństwa oraz RODO i towarzyszącej mu nowej ustawy o ochronie danych osobowych pojawiły się nowe narzędzia prawne dotyczące cyberbezpieczeństwa. Dzięki aktywności NASK-u oraz takim inicjatywom, jak Rządowa Chmura Obliczeniowa jednostki samorządu terytorialnego zyskują coraz więcej skutecznych narzędzi do dbania o swoje cyberbezpieczeństwo.

Niniejszy poradnik ma na celu pomóc w realizacji zadań z zakresu cyberbezpieczeństwa, wskazując przede wszystkim jego aspekty prawne. We wprowadzeniu (rozdział 1) przedstawiono zarys ram prawnych cyberbezpieczeństwa i wskazano na konieczność koordynacji stosowania przepisów różnych aktów prawnych, w szczególności ustawy o krajowym systemie cyberbezpieczeństwa, Krajowych Ram Interoperacyjności oraz RODO. Ten wątek przewija się również w innych częściach poradnika. W rozdziale 2 omówiono definicję cyberbezpieczeństwa oraz typowe rodzaje ataków cybernetycznych.

[1] Informacja o wynikach kontroli – *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, Najwyższa Izba Kontroli, 10.05.2019 r., https://www.nik.gov.pl/kontrole/P/18/006/ (dostęp: 20.11.2020 r.).

Rozdział 3 zawiera omówienie przepisów ustawy o krajowym systemie cyberbezpieczeństwa dotyczących jednostek samorządu terytorialnego. Kolejny rozdział poświęcony został analizie postanowień Krajowych Ram Interoperacyjności, które stanowią dopełnienie regulacji zawartych w ustawie o krajowym systemie cyberbezpieczeństwa. Rozdział 5 ukazuje ścisłe relacje, jakie występują między przepisami o cyberbezpieczeństwie a przepisami regulującymi ochronę danych osobowych. Celem było podkreślenie, że w dużej mierze są to te same procesy i nie wolno patrzeć na te dwie sfery w sposób odmienny. Rozdział 6 przedstawia kwestie prawne związane z korzystaniem z chmury obliczeniowej, które może w sposób znaczny przyczynić się zarówno do podniesienia poziomu usług informatycznych, jak i do zwiększenia cyberbezpieczeństwa w jednostkach samorządu terytorialnego. W rozdziale 7 przedstawiono zasady dbania o bezpieczeństwo informacji, jakimi powinni kierować się prawnicy w swojej codziennej pracy. Podsumowanie zaś przyjęło formę pytań i odpowiedzi.