Ustawa o ochronie informacji niejawnych. Komentarz

Ustawa o ochronie informacji niejawnych

z dnia 5 sierpnia 2010 r. (Dz.U. Nr 182, poz. 1228)

Tekst jednolity z dnia 15 marca 2019 r. (Dz.U. z 2019 r. poz. 742)[1]

(zm.: Dz.U. 2022, poz. 655, poz. 1933)

Rozdział 1. Przepisy ogólne

Literatura: *S. Hoc*, Ustawa o ochronie informacji niejawnych. Komentarz, Warszawa 2010; *T.T. Kaczmarek*, Ryzyko i zarządzanie ryzykiem – ujęcie interdyscyplinarne, Warszawa 2008; *K.M. Klimczak*, Perceived Collaborative Risk in Small and Medium Technology Enterprises, Rochester, New York, August 2019; *I. Stankowska*, Ustawa o ochronie informacji niejawnych. Komentarz, Warszawa 2014; *T. Szewc*, Ochrona informacji niejawnych. Komentarz, Warszawa 2006; *S. Zalewski*, Dylematy ochrony informacji niejawnych, Katowice 2009.

Art. 1. [Zakres stosowania ustawy]

1. Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zwanych dalej „informacjami niejawnymi", to jest zasady:

1) **klasyfikowania informacji niejawnych;**
2) **organizowania ochrony informacji niejawnych;**
3) **przetwarzania informacji niejawnych;**
4) **postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio „postępowaniem sprawdzającym" lub „kontrolnym postępowaniem sprawdzającym";**

[1] Tekst jednolity ogłoszono dnia 23.04.2019 r.

5) postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwanego dalej „postępowaniem bezpieczeństwa przemysłowego";
6) organizacji kontroli stanu zabezpieczenia informacji niejawnych;
7) ochrony informacji niejawnych w systemach teleinformatycznych;
8) stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

2. Przepisy ustawy mają zastosowanie do:
1) organów władzy publicznej, w szczególności:
a) Sejmu i Senatu,
b) Prezydenta Rzeczypospolitej Polskiej,
c) organów administracji rządowej,
d) organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych,
e) sądów i trybunałów,
f) organów kontroli państwowej i ochrony prawa;
2) jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
3) Narodowego Banku Polskiego;
4) państwowych osób prawnych i innych niż wymienione w pkt 1–3 państwowych jednostek organizacyjnych;
5) jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy;
6) przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

3. Przepisy ustawy o ochronie informacji niejawnych nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych, z zastrzeżeniem art. 5.

4. Do danych osobowych stanowiących informacje niejawne nie stosuje się przepisów o ochronie danych osobowych.

5. Do danych osobowych stanowiących informacje niejawne stosuje się przepisy niniejszej ustawy.

Spis treści

1. **Przedmiot ochrony.** Przedmiot ochrony komentowanej ustawy stanowią **1**
informacje niejawne. Ustawodawca wyjaśnił, że są to takie informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla RP albo byłoby z punktu widzenia jej interesów niekorzystne. Dotyczy to także informacji będących w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania. Taka regulacja pozwala na przyjęcie materialnego rozumienia informacji niejawnych (*T. Szewc*, Ochrona informacji, s. 65). Także w orzecznictwie sądów administracyjnych podkreśla się, że dla uznania informacji za niejawną wystarczająca jest przesłanka materialna określona w art. 1 ust. 1 OchrInfU (wyr. NSA z 28.4.2016 r., I OSK 2620/14, Legalis; wyr. NSA z 6.9.2016 r., I OSK 210/15, Legalis).

2. **Pojęcie ujawnienia informacji.** Informacje niejawne podlegają ochronie **2**
przed ich nieuprawnionym ujawnieniem. Ujawnienie nieuprawnione to takie, które odbywa się bez prawnej legitymizacji, a w konsekwencji spowodowałoby lub mogłoby spowodować szkody dla RP albo byłoby z punktu widzenia jej interesów niekorzystne. Ujawnienie informacji niejawnej może przybrać różnorodne postacie, m.in. może polegać na wyjawieniu drugiej osobie, rozpowszechnieniu, opublikowaniu czy zakomunikowaniu w inny sposób. Działanie to nie musi mieć charakteru ciągłego, wystarczające jest więc działanie jednorazowe poprzez uczynienie informacji niejawnej informacją jawną dla jej odbiorcy (kolejnych jej odbiorców). Ustawodawca nie sprecyzował formy, w jakiej informacja może zostać ujawniona. W braku ograniczeń w tym zakresie należy przyjąć, że może to nastąpić w każdej możliwej formie, tj. w formie ustnej wypowiedzi (osobiście lub przy pomocy urządzeń komunikacji elektronicznej), za pośrednictwem środków masowego przekazu, w postaci ujawnienia dokumentu mającego postać pisemną, przez okazanie (np. dokumentu) czy przekazanie informacji za pośrednictwem technicznych środków przekazu, np. faksu. Niekiedy forma przekazania informacji może być mniej oczywista i jednoznaczna dla ogółu. Istotne, aby przekaz był czytelny i nie budził wątpliwości po stronie jego odbiorcy.

W tym zakresie SN wskazał, że formą ujawnienia informacji może być także znak lub gest (zob. wyr. SN z 17.3.1971 r., III KR 260/70, OSNKW 1971, Nr 10, poz. 151). Istotne dla bezprawnego charakteru ujawnienia informacji niejawnej jest to, aby została przekazana poza krąg prawnie określonych jej odbiorców. Wymaga odnotowania, że bezprawne ujawnienie informacji niejawnej może spowodować uruchomienie postępowania karnego. W art. 265 KK został bowiem określony czyn w postaci ujawnienia lub wykorzystania informacji niejawnych. Jednym z warunków poniesienia odpowiedzialności na podstawie tego przepisu jest jednak faktyczne zapoznanie się z treścią ujawnionej informacji przez osobę nieuprawnioną.

3 3. **Katalog zasad.** W ust. 1 komentowanego przepisu, w pkt 1–8 ustawodawca wskazał na zagadnienia, które reguluje ustawa, określając je mianem zasad. Do zasad tych należą: klasyfikowanie informacji niejawnych; organizowanie ochrony informacji niejawnych; przetwarzanie informacji niejawnych; postępowanie sprawdzające prowadzone w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwane dalej odpowiednio „postępowaniem sprawdzającym" lub „kontrolnym postępowaniem sprawdzającym"; postępowanie prowadzone w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwane dalej „postępowaniem bezpieczeństwa przemysłowego"; organizacja kontroli stanu zabezpieczenia informacji niejawnych; ochrona informacji niejawnych w systemach teleinformatycznych; stosowanie środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych. Należy odnotować, że ustawowe uregulowanie znalazło również kilka zagadnień nieujętych we wskazanym katalogu zasad, m.in. kwestie dotyczące zagadnień opisanych w rozdziale 4 OchrInfU, tj. szkoleń w zakresie informacji niejawnych, czy kwestie, o których mowa w rozdziale 10 OchrInfU, tj. ewidencji i udostępniania danych oraz akt postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego.

4 4. **Akty wykonawcze do ustawy.** Ustawowe regulacje w zakresie ochrony informacji niejawnych uzupełniają liczne akty wykonawcze do ustawy. Do ich wydania upoważniają następujące artykuły:

1) art. 6 ust. 9 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także trybu i sposobu zmiany lub znoszenia nadanej klauzuli – właściwym aktem jest rozp. Prezesa RM z 22.12.2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. Nr 288, poz. 1692);

2) art. 11 ust. 6 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia zakresu, trybu i sposobu współdziałania Szefa ABW i Szefa SKW w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa przez Szefa ABW – właściwym aktem jest rozp. Prezesa RM z 4.10.2011 r. w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa (Dz.U. Nr 220, poz. 1302);
3) art. 12 ust. 6 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia sposobu przygotowania oraz zakresu i trybu przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych, trybu uzgodnienia terminu kontroli w stosunku do Kancelarii Sejmu, Kancelarii Senatu oraz Kancelarii Prezydenta RP, zadań funkcjonariuszy ABW oraz funkcjonariuszy lub żołnierzy SKW nadzorujących i wykonujących czynności kontrolne, sposobu dokumentowania czynności kontrolnych oraz sporządzania protokołu kontroli, wystąpienia pokontrolnego i informacji o wynikach kontroli – właściwym aktem jest rozp. Prezesa RM z 27.4.2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz.U. Nr 93, poz. 541);
4) art. 13 ust. 4 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia szczegółowego zakresu, warunków, sposobu i trybu przekazywania przez kierowników jednostek organizacyjnych służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego informacji, o których mowa w art. 13 ust. 1 i 3 OchrInfU, oraz udostępniania im dokumentów niezbędnych dla celów tych postępowań, a także do określenia szczegółowego zakresu, warunków, sposobu i trybu udzielania przez CBA, Policję, Straż Graniczną, Żandarmerię Wojskową oraz organy kontroli skarbowej niezbędnej pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego przy wykonywaniu czynności w ramach tych postępowań – właściwym aktem jest rozp. Prezesa RM z 7.12.2017 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz.U. z 2017 r. poz. 2334);

5) art. 18 OchrInfU – upoważnienie dla MON do określenia w drodze rozporządzenia szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych jemu podległych i przez niego nadzorowanych, szczegółowych wymagań dotyczących stosowania środków bezpieczeństwa fizycznego przeznaczonych do ochrony informacji niejawnych, miejsca i roli Pełnomocnika Ministra Obrony Narodowej do Spraw Ochrony Informacji Niejawnych oraz pełnomocników ochrony kierowników bezpośrednio nadrzędnych jednostek organizacyjnych w resortowym systemie ochrony informacji niejawnych, zakresu, trybu i sposobu współdziałania pełnomocników ochrony w zakresie ochrony informacji niejawnych z SKW, rodzajów, szczegółowych celów oraz sposobu organizacji szkoleń w zakresie ochrony informacji niejawnych, zakresu stosowania środków bezpieczeństwa fizycznego oraz kryteriów tworzenia stref ochronnych, trybu opracowywania oraz niezbędnych elementów planu ochrony informacji niejawnych, w tym postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą „tajne" lub „ściśle tajne" w razie wprowadzenia stanu nadzwyczajnego, a także sposobu nadzorowania ich realizacji – właściwym aktem jest rozp. MON z 19.12.2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (t.j. Dz.U. z 2022 r. poz. 322);
6) art. 20 ust. 2 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów, o których mowa w art. 19 ust. 4 OchrInfU – właściwym aktem jest rozp. Prezesa RM z 9.7.2020 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz.U. z 2020 r. poz. 1256);
7) art. 29 ust. 6 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia wzorów poświadczenia bezpieczeństwa oraz poświadczeń bezpieczeństwa organizacji międzynarodowych – właściwym aktem jest rozp. Prezesa RM z 28.12.2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (t.j. Dz.U. z 2015 r. poz. 220);
8) art. 30 ust. 8 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia wzoru decyzji o odmowie wydania poświad-

czenia bezpieczeństwa – właściwym aktem jest rozp. Prezesa RM z 28.12.2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U. Nr 258, poz. 1753);

9) art. 33 ust. 12 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa – właściwym aktem jest rozp. Prezesa RM z 28.12.2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U. Nr 258, poz. 1754);
10) art. 47 ust. 1 OchrInfU – upoważnienie dla RM do określenia w drodze rozporządzenia podstawowych kryteriów i sposobu określania poziomu zagrożeń oraz doboru środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń, wymagań w zakresie organizacji i funkcjonowania kancelarii tajnych, rodzajów zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń, podstawowych elementów, które powinien zawierać plan ochrony informacji niejawnych, zakresu stosowania środków bezpieczeństwa fizycznego, kryteriów tworzenia stref ochronnych, struktury organizacyjnej kancelarii tajnej, z uwzględnieniem możliwości tworzenia jej oddziałów, podstawowych zadań kierownika kancelarii, sposobu i trybu przetwarzania informacji niejawnych, wzoru karty zapoznania się z dokumentem, wzorów dzienników ewidencji – właściwym aktem jest rozp. RM z 29.5.2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U. z 2012 r. poz. 683 ze zm.);
11) art. 47 ust. 3 OchrInfU – upoważnienie dla ministrów właściwych do spraw wewnętrznych, informatyzacji, administracji publicznej, spraw zagranicznych, finansów publicznych, budżetu i instytucji finansowych, MON, MS, Prezesa Narodowego Banku Polskiego, Prezesa NIK, Pierwszego Prezesa SN, Prokuratora Generalnego, Szefów Kancelarii Prezydenta RP, Sejmu, Senatu oraz Prezesa RM, Szefa ABW, Szefa AW, Szefa SKW, Szefa SWW, Szefa CBA, Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta Służby Ochrony Państwa, a także Prezesa Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu do określenia w drodze zarządzenia, każdy w zakresie swojego działania, szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz komórek organizacyjnych, o których mowa w art. 44 ust. 1 OchrInfU, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego – właściwymi aktami są następujące

zarządzenia: zarz. MS z 29.12.2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz niektórych komórek organizacyjnych innych niż kancelaria tajna, a także sposobu i trybu przetwarzania informacji niejawnych (Dz.Urz. MS z 2012 r. poz. 13); zarz. MS z 23.1.2014 r. w sprawie doboru i zakresu stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.Urz. MS z 2014 r. poz. 32); zarz. Nr 14 Ministra Spraw Zagranicznych z 25.7.2013 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Ministerstwie Spraw Zagranicznych oraz placówkach zagranicznych (Dz.Urz. MSZ z 2013 r. poz. 18 ze zm.); zarz. Nr 3 Ministra Spraw Wewnętrznych z 9.12.2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego (Dz.Urz. MSW Nr 1, poz. 2); zarz. Nr 47/2012 Szefa SWW z 20.12.2012 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych, niż kancelaria tajna, komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Służbie Wywiadu Wojskowego (Dz.Urz. MON z 2013 r. poz. 79); zarz. Nr 46/MON MON z 24.12.2013 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz.Urz. MON z 2013 r. poz. 401); zarz. Nr 58/MON MON z 11.12.2017 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych (Dz.Urz. MON z 2017 r. poz. 226); zarz. Nr 59/MON MON z 11.12.2017 r. w sprawie doboru i stosowania środków bezpieczeństwa fizycznego do ochrony informacji niejawnych (Dz.Urz. MON z 2017 r. poz. 227); zarz. Nr 54 Ministra Finansów z 28.12.2011 r. w sprawie kancelarii tajnych, innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych oraz przetwarzania informacji niejawnych (Dz.Urz. MF Nr 9, poz. 47); zarz. Nr 32 Ministra Finansów z 27.7.2012 r. w sprawie doboru i zakresu

stosowania środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (t.j. Dz.Urz. MF z 2018 r. poz. 28); zarz. Nr 31 Ministra Cyfryzacji z 18.8.2016 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnej oraz doboru i stosowania środków bezpieczeństwa fizycznego (Dz.Urz. MC z 2016 r. poz. 34 ze zm.); zarz. Nr 53 Komendanta Głównego Straży Granicznej z 23.12.2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego (Dz.Urz. KGSG Nr 17, poz. 56 ze zm.); zarz. Nr 2020 Komendanta Głównego Policji z 30.12.2010 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych i innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego informacji niejawnych w Policji (Dz.Urz. KGP z 2011 r. Nr 1, poz. 5 ze zm.); zarz. Nr 132 Komendanta Głównego Policji z 5.10.2012 r. zmieniające zarządzenie w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych i innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego informacji niejawnych w Policji (Dz.Urz. KGP z 2012 r. poz. 52); zarz. Nr 30/20 Szefa CBA z 29.12.2020 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnej, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego w Centralnym Biurze Antykorupcyjnym (Dz.Urz. CBA z 2020 r. poz. 31 ze zm.); zarz. Nr 21/21 Szefa CBA z 23.9.2021 r. w sprawie utworzenia kancelarii tajnej międzynarodowej w Centralnym Biurze Antykorupcyjnym (Dz.Urz. CBA z 2021 r. poz. 21); zarz. Nr 4 Szefa ABW z 18.1.2011 r. w sprawie szczególnych zasad organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych i jawnych w Agencji Bezpieczeństwa Wewnętrznego (Dz.Urz. ABW Nr 1, poz. 3);

12) art. 47 ust. 4 OchrInfU – upoważnienie dla ministra właściwego do spraw kultury i ochrony dziedzictwa narodowego do określenia w drodze zarządzenia dla archiwów państwowych szczególnego sposobu i trybu

przetwarzania informacji niejawnych wchodzących w skład zasobu archiwalnego tych archiwów, doboru i stosowania środków bezpieczeństwa fizycznego oraz organizacji komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych – właściwym aktem jest zarz. Ministra Kultury i Dziedzictwa Narodowego z 10.11.2016 r. w sprawie szczególnego sposobu i trybu przetwarzania informacji niejawnych wchodzących w skład zasobu archiwalnego archiwów państwowych, doboru i stosowania środków bezpieczeństwa fizycznego oraz organizacji komórek organizacyjnych odpowiedzialnych za przetwarzanie materiałów niejawnych (Dz.Urz. MKiDN z 2016 r. poz. 65);

13) art. 47 ust. 5 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia trybu i sposobu nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów, sposobu postępowania nadawców przesyłek zawierających informacje niejawne oraz wymogów, jakie muszą spełniać te przesyłki, sposobu postępowania podmiotów, które wykonują zadania przewoźników tych materiałów, z przesyłkami zawierającymi informacje niejawne, sposobu dokumentowania przyjmowania przez przewoźników przesyłek oraz ich wydawania adresatom, wraz z załącznikami w postaci wzorów niezbędnych formularzy, warunków ochrony i sposobów zabezpieczania przesyłek przez przewoźnika oraz warunków, jakie muszą spełniać wykorzystywane przez niego środki transportu i uczestniczące w konwojach osoby, sposobu postępowania w przypadku zaistnienia nieprzewidzianych okoliczności mogących mieć wpływ na bezpieczeństwo przesyłki, warunków przewożenia materiałów poza granicami RP – właściwym aktem jest rozp. Prezesa RM z 7.12.2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. Nr 271, poz. 1603);
14) art. 48 ust. 13 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego – właściwym aktem jest rozp. Prezesa RM z 20.7.2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz.U. Nr 156, poz. 926);
15) art. 49 ust. 9 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia podstawowych wymagań bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne, niezbędnych danych, jakie powinna zawierać dokumentacja bezpieczeństwa systemów informatycznych, oraz sposobu opracowania tej

dokumentacji – właściwym aktem jest rozp. Prezesa RM z 20.7.2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. Nr 159, poz. 948);

16) art. 53 ust. 4 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia szczegółowego sposobu i trybu ustalania wysokości oraz poboru opłat, o których mowa w art. 53 ust. 1 OchrInfU – właściwym aktem jest rozp. Prezesa RM z 9.7.2020 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego (Dz.U. z 2020 r. poz. 1236);
17) art. 61 ust. 2 OchrInfU – upoważnienie dla Prezesa RM do określenia w drodze rozporządzenia wysokości zryczałtowanych kosztów, o których mowa w art. 61 ust. 1 OchrInfU, oraz trybu ich zwrotu, uwzględniając, że wysokość kosztów nie powinna przekroczyć 7-krotności kwoty przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłaty nagród z zysku za ubiegły rok, ogłoszonego przez Prezesa GUS na podstawie art. 60 pkt 5 ustawy z 15.7.2011 r. o zawodach pielęgniarki i położnej (t.j. Dz.U. z 2022 r. poz. 2702) – właściwym aktem jest rozp. Prezesa RM z 13.1.2021 r. w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających (Dz.U. z 2021 r. poz. 84);
18) art. 68 ust. 1 OchrInfU – upoważnienie dla RM do określenia w drodze rozporządzenia wzorów: kwestionariusza, świadectwa, decyzji o odmowie wydania świadectwa, decyzji o cofnięciu świadectwa – właściwym aktem jest rozp. RM z 16.5.2019 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz.U. z 2019 r. poz. 1103).

5. **Podmiotowy zakres ustawy.** W ust. 2 komentowanego przepisu ustawo- **5**
dawca określił katalog podmiotów, w stosunku do których przepisy ustawy znajdują zastosowanie. W tym zakresie wskazanych zostało 6 kategorii podmiotów. Pierwsza ma najbardziej obszerny charakter, bowiem dotyczy organów władzy publicznej. Ustawodawca jedynie przykładowo wymienił tu Sejm i Senat, Prezydenta RP, organy administracji rządowej, organy jednostek samorządu terytorialnego, a także inne podległe im jednostki organizacyjne

lub przez nie nadzorowane, sądy i trybunały oraz organy kontroli państwowej i ochrony prawa. O przykładowym charakterze ww. katalogu świadczy poprzedzenie go zwrotem „w szczególności". Kolejne wskazane przez ustawodawcę kategorie podmiotów to: jednostki organizacyjne podległe MON lub przez niego nadzorowane; Narodowy Bank Polski; państwowe osoby prawne i inne – niż wcześniej wymienione – jednostki organizacyjne; jednostki organizacyjne podległe organom władzy publicznej lub nadzorowane przez te organy; przedsiębiorcy zamierzający ubiegać się albo ubiegający się o zawarcie umów związanych z dostępem do informacji. Ustawodawca wykluczył również teoretyczny konflikt przepisów o ochronie informacji niejawnych oraz przepisów o ochronie danych osobowych. Wskazał mianowicie, że do danych osobowych stanowiących jednocześnie informacje niejawne zastosowanie mają przepisy OchrInfU, zaś przepisy o ochronie danych osobowych nie znajdują zastosowania (ust. 4 i 5 komentowanego przepisu). Jednocześnie ustawodawca zastrzegł, że przepisy OchrInfU – poza wspomnianą kwestią danych osobowych – nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych (art. 1 ust. 3 OchrInfU).

Art. 2. [Definicje pojęć]

W rozumieniu ustawy:

1) **jednostką organizacyjną – jest podmiot wymieniony w art. 1 ust. 2;**
2) **rękojmią zachowania tajemnicy – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;**
3) **dokumentem – jest każda utrwalona informacja niejawna;**
4) **materiałem – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;**
5) **przetwarzaniem informacji niejawnych – są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;**
6) **systemem teleinformatycznym – jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2019 r. poz. 123);**

7) dokumentem szczególnych wymagań bezpieczeństwa – jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;

8) dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego – jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp;

9) dokumentacją bezpieczeństwa systemu teleinformatycznego – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;

10) akredytacją bezpieczeństwa teleinformatycznego – jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;

11) certyfikacją – jest proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych;

12) audytem bezpieczeństwa systemu teleinformatycznego – jest weryfikacja poprawności realizacji wymagań i procedur, określonych w dokumentacji bezpieczeństwa systemu teleinformatycznego;

13) przedsiębiorcą – jest przedsiębiorca w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz.U. poz. 646, 1479, 1629, 1633 i 2212) lub każda inna jednostka organizacyjna, niezależnie od formy własności, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa;

14) kierownikiem przedsiębiorcy – jest członek jednoosobowego zarządu lub innego jednoosobowego organu zarządzającego, a jeżeli organ jest wieloosobowy – cały organ albo członek lub członkowie tego organu wyznaczeni co najmniej uchwałą zarządu do pełnienia funkcji kierownika przedsiębiorcy, z wyłączeniem pełnomocników ustanowionych przez ten organ lub jednostkę; w przypadku spółki jawnej i spółki cywilnej kierownikiem przedsiębiorcy są wspólnicy prowadzący sprawy spółki, w przypadku spółki partnerskiej – wspólnicy prowadzący sprawy spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej – komplemen-

tariusze prowadzący sprawy spółki; w przypadku osoby fizycznej prowadzącej działalność gospodarczą kierownikiem przedsiębiorcy jest ta osoba; za kierownika przedsiębiorcy uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu upadłościowym; kierownik przedsiębiorcy jest kierownikiem jednostki organizacyjnej w rozumieniu przepisów ustawy;

15) ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

16) szacowaniem ryzyka – jest całościowy proces analizy i oceny ryzyka;

17) zarządzaniem ryzykiem – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;

18) zatrudnieniem – jest również odpowiednio powołanie, mianowanie lub wyznaczenie;

19)[2] rozwiązaniem informatycznym – jest urządzenie lub zespół urządzeń, oprogramowanie, narzędzie lub usługa informatyczna umożliwiająca przetwarzanie informacji niejawnych w postaci elektronicznej, eksploatowana lub planowana do wdrożenia wyłącznie w jednostkach organizacyjnych wskazanych w art. 10 ust. 2.

Spis treści

1 1. **Słowniczek.** W komentowanym przepisie zawarty został tzw. słowniczek pojęć stosowanych w ustawie. Jego celem – podobnie jak w przypadku ana-

[2] Art. 2 pkt 19 dodany ustawą z dnia 11.03.2022 r. (Dz.U. z 2022 r. poz. 655), która wchodzi w życie 23.04.2022 r.

logicznych regulacji zawartych w wielu innych ustawach – jest odkodowanie znaczenia nadanego tym pojęciom przez ustawodawcę, a w konsekwencji – ułatwienie ich zrozumienia i prawidłowego stosowania.

2. **Jednostka organizacyjna.** Pojęciu jednostki organizacyjnej ustawo- **2**
dawca nadał specyficzne znaczenie. Dotyczy ono bowiem każdego z podmiotów wymienionych w art. 1 ust. 2 OchrInfU, będącego dysponentem informacji niejawnych. Nie ma przy tym znaczenia jego forma własnościowa czy organizacyjna. Bez znaczenia pozostaje również fakt, czy dany podmiot dysponuje informacją niejawną z mocy prawa czy na skutek działań podjętych na zasadach określonych w art. 1 ust. 2 OchrInfU. Należy w tym zakresie zgodzić się z poglądem, zgodnie z którym zarówno struktura organizacyjna, jak i kadrowa każdej jednostki organizacyjnej, o której mowa w art. 1 ust. 2 OchrInfU, powinna zapewnić ochronę informacji niejawnych zgodnie z wymogami tej ustawy (*I. Stankowska*, Ustawa o ochronie informacji, s. 11).

3. **Rękojmia zachowania tajemnicy.** Pod pojęciem rękojmi zachowania **3**
tajemnicy należy rozumieć sytuację, w której dany podmiot spełnia określone w ustawie wymogi nakierowane na zapewnienie ochrony informacji niejawnych przed nieuprawnionym ich ujawnieniem. Prawną gwarancją rękojmi jest przeprowadzenie z wynikiem pozytywnym postępowania sprawdzającego, o którym mowa w art. 24 OchrInfU, którego celem jest ustalenie, czy osoba poddana procedurze sprawdzającej w istocie daje rękojmię zachowania tajemnicy, czy może istnieją wobec niej wątpliwości w tym zakresie. Wyeliminowanie ustawowego braku pewności co do osoby sprawdzanej następuje z momentem wydania poświadczenia bezpieczeństwa. Zastosowane przez ustawodawcę w przypadku komentowanego terminu sformułowanie dotyczące „ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem" nie zostało w żaden sposób dookreślone poprzez wskazanie jego desygnatów. Stąd może powstać słuszna konstatacja, że trudne (może nawet niemożliwe) jest spełnienie wymogów, które nie zostały w żaden sposób zdefiniowane ani dookreślone. Niemniej rękojmi zachowania tajemnicy nie można upatrywać we wskazaniu cech danej jednostki poddanej postępowaniu sprawdzającemu, świadczących o jej zdolności do właściwego postępowania z informacjami niejawnymi. Przeciwnie, o dawaniu wspomnianej rękojmi świadczyć będzie brak negatywnych przesłanek mogących stwarzać wątpliwości co do jej istnienia. Należy więc przyjąć, że jeśli wobec obywatela nie zostanie udokumentowana w postępowaniu sprawdzającym przynajmniej jedna wspomniana okoliczność