Warszawa, dnia 22 sierpnia 2016 r.

Poz. 34

**ZARZĄDZENIE NR 31**
**MINISTRA CYFRYZACJI**

z dnia 18 sierpnia 2016 r.

**w sprawie kancelarii tajnej**

Na podstawie art. 47 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167) zarządza się, co następuje:

**§ 1.** Zarządzenie określa:

1) szczególny sposób organizacji i funkcjonowania kancelarii tajnej;

2) sposób i tryb przetwarzania informacji niejawnych;

3) dobór i stosowanie środków bezpieczeństwa fizycznego.

**§ 2.** Ilekroć w zarządzeniu jest mowa o:

1) materiale – należy przez to rozumieć dokument lub przedmiot albo dowolną 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;

2) pełnomocniku ochrony – należy przez to rozumieć pełnomocnika ds. ochrony informacji niejawnych Ministerstwa Cyfryzacji;

3) pionie ochrony – należy przez to rozumieć pracowników Zespołu Ochrony Informacji Niejawnych Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji;

4) kierowniku jednostki organizacyjnej – należy przez to rozumieć Ministra Cyfryzacji.

**§ 3.** 1. Kancelaria tajna, zwana dalej „kancelarią”, przyjmuje, wydaje, rejestruje, przechowuje, przekazuje, udostępnia i wysyła materiały, a także je brakuje i przygotowuje do przekazania do archiwum.

2. W kancelarii prowadzi się dzienniki ewidencji, o których mowa w § 2 ust. 2 rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. poz. 1631 i z 2013 r. poz. 11).

**§ 4.** Kierownik kancelarii:

1) realizuje zadania, o których mowa w § 4 ust. 1 pkt 1–5 rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych;

2) ewidencjonuje materiały;

3) prowadzi kontrole w zakresie postępowania z materiałami przez pracowników Ministerstwa Cyfryzacji;

4) informuje pełnomocnika ochrony o zagrożeniach ujawnienia, utraty lub zagubienia materiałów;

5) sprawuje nadzór nad przygotowaniem materiałów do przekazania do archiwum;

6) bierze udział w niszczeniu materiałów niearchiwalnych;

7) prowadzi rejestr dzienników, książek ewidencyjnych i teczek dokumentów oraz innych urządzeń ewidencyjnych.

**§ 5.** W przypadku czasowej nieobecności kierownika kancelarii jego obowiązki przejmuje inny upoważniony pracownik pionu ochrony.

**§ 6.** 1. Materiały są przechowywane w szafach metalowych.

2. W kancelarii mogą być przechowywane materiały nie zawierające informacji niejawnych, jeżeli wchodzą w skład zbioru materiałów.

3. Kierownik jednostki organizacyjnej lub pełnomocnik ochrony może wyrazić pisemną zgodę na przechowywanie materiałów o klauzuli „poufne" poza kancelarią, na czas niezbędny do realizacji zadań związanych z dostępem do tych materiałów, gdy zapewnione są odpowiednie do klauzuli „poufne" warunki ochrony przed nieuprawnionym ujawnieniem.

**§ 7.** 1. Przyjęcie przesyłki może nastąpić po:

1) dokonaniu czynności, o których mowa w § 18 ust. 1 i 2 rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. poz. 1603);

2) sprawdzeniu zgodności numerów na przesyłce z numerami w wykazie przesyłek lub książce doręczeń.

2. W przypadku stwierdzenia rażących nieprawidłowości, o których mowa w § 18 ust. 3 rozporządzenia Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne lub w § 7 ust. 6 rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych, można odmówić przyjęcia przesyłki i dokonać zwrotu przesyłki do nadawcy.

**§ 8.** 1. Materiały przyjęte do kancelarii rejestruje się zgodnie z przepisami § 7 ust. 1-4 oraz § 8 i 9 rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych.

2. Rejestrowany materiał w postaci papierowej oznacza się pieczęcią wpływu na jego pierwszej stronie, w obrębie odcisku pieczęci wpływu wpisuje się datę oraz numer z dziennika ewidencji.

**§ 9.** 1. Nie rejestruje się korespondencji, która wpłynęła do kancelarii omyłkowo.

2. Korespondencję, o której mowa w ust. 1, przekazuje się, łącznie z pierwotnym opakowaniem, właściwemu adresatowi, za pokwitowaniem w książce doręczeń lub w wykazie przesyłek. W przypadku trudności z doręczeniem właściwemu adresatowi, przesyłkę zwraca się do nadawcy.

**§ 10.** 1. Przed przyjęciem materiału do wysłania pracownik kancelarii sprawdza, czy materiał:

1) posiada właściwą sygnaturę literowo-cyfrową;

2) posiada właściwy adres;

3) posiada rozdzielnik;

4) zawiera dane wykonawcy oraz liczbę wykonanych egzemplarzy;

5) wytworzono w takiej liczbie, jaką podano w rozdzielniku;

6) zawiera dane określające faktyczną liczbę załączników, stron lub innych jednostek miary załączników.

2. Materiały wysyła się zgodnie z rozdzielnikiem, pozostawiając jeden egzemplarz materiału w kancelarii.

3. Materiał wykonany w jednym egzemplarzu przekazuje się adresatowi.

**§ 11.** 1. Wykonanie kopii, odpisu, wyciągu lub tłumaczenia materiału następuje za zgodą wytwórcy dokumentu lub adresata, odnotowaną na pierwszej stronie dokumentu.

2. Czynności, o których mowa w ust. 1, mogą wykonywać wyłącznie pracownicy pionu ochrony w warunkach gwarantujących ochronę tych materiałów.

3. Zgodność kopii z oryginałem potwierdza podpisem, na ostatniej stronie materiału w postaci papierowej, kierownik kancelarii lub pracownik pionu ochrony wykonujący powyższe czynności.

**§ 12.** 1. Codziennie po zakończeniu pracy pracownik pionu ochrony sprawdza prawidłowość zamknięcia szaf, a następnie zamyka pomieszczenia kancelarii; klucze pomieszczeń kancelarii przekazuje w zaplombowanych workach lub kasetkach ochronie budynku Ministerstwa Cyfryzacji.

2. Klucze, o których mowa w ust. 1, zdaje i pobiera uprawniony pracownik pionu ochrony.

3. Przed otwarciem pomieszczeń kancelarii uprawniony pracownik pionu ochrony sprawdza, czy drzwi, zamki i plomby nie noszą śladów uszkodzeń.

4. Kierownik kancelarii, nie rzadziej niż raz na 12 miesięcy, określa obowiązujące hasła dostępu i szyfry, zamków szyfrowych i zabezpieczeń elektronicznych, stosowane w szafach metalowych służących do przechowywania materiałów.

5. Hasła dostępu i szyfry stosowane w systemie alarmowym kancelarii i szafach metalowych służących do przechowywania materiałów oraz duplikaty kluczy do pomieszczeń kancelarii przechowuje pełnomocnik ochrony lub pracownik Ministerstwa Cyfryzacji odpowiedzialny za ochronę Ministerstwa Cyfryzacji.

6. Nieprawidłowości związane z naruszeniem zasad, o których mowa w ust. 1–4, niezwłocznie zgłasza się pełnomocnikowi ochrony.

**§ 13.** 1. W przypadku nieobecności pracownika, będącego dysponentem materiałów pobranych z kancelarii, dopuszcza się komisyjne otwarcie szafy, w której przechowywane są materiały.

2. Decyzję o komisyjnym otwarciu szafy, podejmuje kierownik komórki organizacyjnej lub osoba przez niego upoważniona, w porozumieniu z pełnomocnikiem ochrony.

3. Z czynności, o której mowa w ust. 1, sporządza się protokół w dwóch egzemplarzach. Pierwszy egzemplarz protokołu przechowywany jest w kancelarii, a drugi w szafie u dysponenta dokumentu.

**§ 14.** 1. Materiały w postaci elektronicznej przetwarzane są wyłącznie na zaewidencjonowanych w kancelarii tajnej informatycznych nośnikach danych.

2. Informatyczne nośniki danych posiadają:

1) numer pod którym nośnik został zarejestrowany w rejestrze wydanych przedmiotów;

2) klauzulę tajności nośnika.

3. Informatyczne nośniki danych podlegają ochronie, stosownej do klauzuli tajności, jaką zostały oznaczone.

4. Kancelaria zakłada „Metrykę dokumentu elektronicznego”, zawierającą dane dotyczące informacji zapisanych na nośniku.

5. Fizyczne zniszczenie informatycznego nośnika danych odnotowuje się w rejestrze wydanych przedmiotów.

**§ 15.** Akta spraw zakończonych zawierających materiały o klauzuli „poufne” lub wyższej przechowuje się w kancelarii do momentu zniesienia klauzuli tajności. Po zniesieniu klauzuli tajności materiały przekazuje się do archiwum zakładowego, zgodnie z obowiązującymi w Ministerstwie Cyfryzacji przepisami.

**§ 16.** 1. Kancelarię lokalizuje się w strefie ochronnej.

2. Pomieszczenia kancelarii oddziela się od pozostałych pomieszczeń trwałymi ścianami i stropami, spełniającymi wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły pełnej o grubości 100 mm.

3. Drzwi do kancelarii posiadają certyfikat Instytutu Mechaniki Precyzyjnej, co najmniej klasy 2 według Polskiej Normy PN-EN 1627. Drzwi są wyposażone w zamek kluczowy co najmniej klasy 3 według Polskiej Normy PN-EN 12209.

4. Okna kancelarii zabezpiecza się przed włamaniem oraz obserwacją wnętrza kancelarii z zewnątrz.

5. Kancelarię wyposaża się w certyfikowane szafy metalowe:

1) spełniające co najmniej wymagania klasy odporności na włamanie S2, określone w Polskiej Normie PN-EN 14450 lub nowszej;

2) spełniające co najmniej wymagania klasy odporności na włamanie S1, określone w Polskiej Normie PN-EN 14450 lub nowszej;

3) przeznaczone do przechowywania materiałów o klauzuli „poufne”.

6. Pomieszczenia kancelarii wyposaża się w barierkę odgradzającą pracowników od interesantów oraz system kontroli dostępu.

7. W pomieszczeniach kancelarii instaluje się co najmniej:

1) system sygnalizacji włamania i napadu;

2) system nadzoru wizyjnego wraz z rejestracją obrazu, wyłącznie do obserwacji wejścia do pomieszczeń kancelarii.

8. W kancelarii wydziela się stanowisko lub pomieszczenie, w którym osoby upoważnione mogą zapoznawać się z materiałami – czytelnię, która powinna być zorganizowana w sposób umożliwiający stały nadzór nad materiałami ze strony pracowników kancelarii. W czytelni nie instaluje się systemu nadzoru wizyjnego.

**§ 17.** W Ministerstwie Cyfryzacji tworzy się strefy ochronne II i III na podstawie kryteriów określonych w § 5 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683).

**§ 18.** Zarządzenie wchodzi w życie z dniem 1 września 2016 r.

-Anna *STREŻYŃSKA*
MINISTER CYFRYZACJI