

ZARZĄDZENIE Nr 5 /2019  
DYREKTORA GENERALNEGO SŁUŻBY WIĘZIENNEJ

z dnia 19 lutego 2019 r.

**w sprawie wdrożenia w Centralnym Zarządzie Służby Więziennej  
polityki ochrony danych osobowych przetwarzanych w związku z zapobieganiem  
i zwalczaniem przestępczości**

Na podstawie art. 31 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125) oraz art. 11 ust. 1 pkt 11 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. z 2018 r. poz. 1542, 1669, 2245 i 2399 oraz z 2019 r. poz. 125) zarządza się, co następuje:

**§ 1.** Zarządzenie określa politykę ochrony danych osobowych przetwarzanych w Centralnym Zarządzie Służby Więziennej, zwanym dalej „Centralnym Zarządem”, w celach określonych w ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

**§ 2.** Użyte w zarządzeniu określenia oznaczają:

- 1) ustawa – ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);
- 2) ustawa o Służbie Więziennej – ustawę z dnia 9 kwietnia 2010 r. o Służbie Więziennej;
- 3) dane osobowe – dane osobowe, o których mowa w art. 4 pkt 5 ustawy;
- 4) przetwarzanie – przetwarzanie, o którym mowa w art. 4 pkt 14 ustawy;
- 5) Dyrektor Generalny – Dyrektora Generalnego Służby Więziennej, jako administratora, o którym mowa w art. 4 pkt 1 ustawy;
- 6) Inspektor Ochrony Danych – osobę wyznaczoną przez Dyrektora Generalnego, o której mowa w art. 46 ust. 1 – 3 ustawy, pełniącą obowiązki w Centralnym Zarządzie;
- 7) Administrator Systemów Informatycznych – Dyrektora Biura Informatyki i łączności Centralnego Zarządu;
- 8) osoba upoważniona – funkcjonariusza lub pracownika Centralnego Zarządu albo inną osobę, której niezbędnym jest udostępnienie danych osobowych, posiadającą imienne upoważnienie do przetwarzania danych osobowych;
- 9) naruszenie ochrony danych osobowych – naruszenie, o którym mowa w art. 4 pkt 6 ustawy.


§ 3. Wdraża się w Centralnym Zarządzie politykę ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, w skład której wchodzi:

- 1) procedura zarządzania ochroną danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, stanowiąca załącznik nr 1 do zarządzenia;
- 2) procedura ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przetwarzanych w postaci papierowej, stanowiąca załącznik nr 2 do zarządzenia;
- 3) procedura ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przetwarzanych w postaci elektronicznej, stanowiąca załącznik nr 3 do zarządzenia;
- 4) procedura prowadzenia wykazów kategorii czynności przetwarzania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, stanowiąca załącznik nr 4 do zarządzenia;
- 5) procedura przeprowadzania analiz ryzyka ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, stanowiąca załącznik nr 5 do zarządzenia;
- 6) procedura dokonywania oceny skutków dla ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, stanowiąca załącznik nr 6 do zarządzenia;
- 7) procedura nadawania, zmieniania i cofania upoważnień do przetwarzania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz prowadzenia ich ewidencji, stanowiąca załącznik nr 7 do zarządzenia;
- 8) procedura przeprowadzania szkoleń w zakresie ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, stanowiąca załącznik nr 8 do zarządzenia;
- 9) procedura powierzania przetwarzania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, stanowiąca załącznik nr 9 do zarządzenia;
- 10) procedura udostępniania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, stanowiąca załącznik nr 10 do zarządzenia;
- 11) procedura wypełniania obowiązków informacyjnych wobec osób, których dane dotyczą, w zakresie dotyczącym ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, stanowiąca załącznik nr 11 do zarządzenia;

12) procedura postępowania w sytuacji naruszenia przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz naruszeń ochrony tych danych, stanowiąca załącznik nr 12 do zarządzenia.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązywania od dnia 6 lutego 2019 r.

**DYREKTOR GENERALNY  
SŁUŻBY WIĘZIENNEJ**  
*gen. Jacek Kitliński*





## Uzasadnienie

Zarządzenie w sprawie wdrożenia w Centralnym Zarządzie Służby Więziennej polityki ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości stanowi wykonanie obowiązku, o którym mowa w art. 31 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), zwanej dalej „ustawą”, oraz art. 11 ust. 1 pkt 11 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. z 2018 r. poz. 1542, 1669, 2245 i 2399 oraz z 2019 r. poz. 125).

Niniejszy akt dotyczący ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości w Centralnym Zarządzie Służby Więziennej wdraża stosowną politykę ich ochrony, do wprowadzenia której zobowiązany jest administrator danych, w przypadku Centralnego Zarządu Służby Więziennej – Dyrektor Generalny Służby Więziennej, zgodnie z przepisami wchodzącej w życie z dniem 6 lutego 2019 r. ustawy, implementującej do krajowego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającą decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89).

Projekt zarządzenia określa politykę ochrony danych osobowych jako akt, na który składa się 12 wyodrębnionych procedur dotyczących poszczególnych obszarów ich ochrony, tj.:

- 1) procedura zarządzania ochroną danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 2) procedura ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przetwarzanych w formie papierowej;
- 3) procedura ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przetwarzanych w formie elektronicznej;
- 4) procedura prowadzenia wykazów kategorii czynności przetwarzania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 5) procedura przeprowadzania analiz ryzyka ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 6) procedura dokonywania oceny skutków dla ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 7) procedura nadawania, zmieniania i cofania upoważnień do przetwarzania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz prowadzenia ich ewidencji;

- 8) procedura przeprowadzania szkoleń w zakresie ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 9) procedura powierzania przetwarzania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 10) procedura udostępniania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 11) procedura wypełniania obowiązków informacyjnych wobec osób, których danych dotyczą, w zakresie dotyczącym ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- 12) procedura postępowania w sytuacji naruszenia przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz naruszeń ochrony tych danych.

Zastosowanie powyższego sposobu redakcji, z wykorzystaniem modelu wyraźnego podziału obowiązków, w zależności od specyfiki regulowanego obszaru ochrony danych osobowych, ułatwi korzystanie z niniejszego aktu w praktyce, zwłaszcza w przypadku konieczności działania pod presją czasu. Już sam tytuł wyodrębnionej procedury wskazuje bowiem, w którym miejscu zarządzenia winniśmy znaleźć interesującą nas normę, której adresatami jesteśmy wprost, lub na podstawie której możemy ustalić podmiot właściwy do realizacji danego zadania.

Zgodnie z projektem, największy zakres obowiązków został przypisany Inspektorowi Ochrony Danych, gdyż tak naprawdę to ten podmiot, jako posiadający odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, o których mowa w art. 46 ust. 2 pkt 2 ustawy, winien na co dzień sprawnie i właściwie pod względem merytorycznym je realizować. Założenie to potwierdza wieloletnia praktyka w obszarze funkcjonowania poprzedników inspektorów ochrony danych, tj. administratorów bezpieczeństwa informacji, ale nie tylko. Potwierdza je także dotychczasowe doświadczenie nabyte od 25 maja 2018 r., czyli w toku realizacji obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchyłającego dyrektywę 95/46/WE (Dz. Urz. UE. L Nr 119, str. 1 oraz Nr 8088/18, str. 258), zwłaszcza w obszarze związanym z reakcją na zaistniałe sytuacje problematyczne, w tym incydenty. Jednocześnie w tym miejscu szczególnego podkreślenia wymaga, iż Inspektorowi Ochrony Danych nie można powierzyć jedynie tych obowiązków, które naruszyłyby prawidłowe wykonywanie jego zadań ustawowych, oraz zadań powodujących konflikt interesów (art. 47 ust. 3 ustawy).

Kolejnymi podmiotami, którym zaprojektowano rozszerzone kompetencje i obowiązki, są kierownicy poszczególnych komórek organizacyjnych Centralnego Zarządu Służby Więziennej. W przypadku bowiem administratora danych, będącego podmiotem jednoosobowym, jak to ma

miejsce w zakresie dotyczącym Dyrektora Generalnego Służby Więziennej, nie jest możliwym zrealizowanie bezpośrednio przez ten organ licznych zadań nakładanych ustawą. To właśnie ci funkcjonariusze i pracownicy, którzy na co dzień kierują poszczególnymi komórkami Centralnego Zarządu Służby Więziennej, jako aparatu wykonawczego Dyrektora Generalnego Służby Więziennej, powinni realizować, w jego imieniu, także zadania związane z ochroną danych osobowych, w obszarach adekwatnych do nadzorowanych przez nich pionów służby. Stąd też projekt zakłada w szczególności, że to właśnie kierownicy komórek organizacyjnych będą zobowiązani do upoważniania do dostępu do danych osobowych podległych im funkcjonariuszy i pracowników w ramach danej kategorii czynności przetwarzania, gdyż to właśnie oni są właściwi do określania zakresów ich czynności, immanentnie związanych przecież z zakresem upoważnienia, które z kolei winno zostać skonstruowane zgodnie z zasadami adekwatności, stosowności i nienadmierności przetwarzania danych, o których mowa w art. 31 ust. 1 pkt 3 ustawy.

Wejście w życie niniejszego zarządzenia nie pociągnie za sobą dodatkowych skutków finansowych.

