DZIENNIK URZĘDOWY

CENTRALNEGO BIURA ANTYKORUPCYJNEGO

Warszawa, dnia 6 lutego 2019 r.

Poz. 6

ZARZĄDZENIE NR 6/19
SZEFA CENTRALNEGO BIURA ANTYKORUPCYJNEGO

z dnia 6 lutego 2019 r.

w sprawie systemu ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym

Na podstawie art. 10 ust. 3 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2018 r. poz. 2104 i 2399 oraz z 2019 r. poz. 53 i 125) zarządza się, co następuje:

§ 1. 1. Tworzy się w Centralnym Biurze Antykorupcyjnym, zwanym dalej „CBA", system ochrony danych osobowych.

2. System ochrony danych osobowych:

1) wskazuje podstawowe regulacje wewnętrzne wchodzące w skład tego systemu, jak również inne jego komponenty wynikające z dokumentacji przetwarzania danych osobowych oraz wzory dokumentów stosowanych w związku z przetwarzaniem danych osobowych w CBA

2) służy zgodnemu z przepisami ustawy o CBA przetwarzaniu danych osobowych, ich zabezpieczaniu oraz realizacji kontroli weryfikującej prawidłowość ich przetwarzania przez funkcjonariuszy i pracowników CBA w związku z realizacją ustawowych zadań.

3. Dane osobowe, o których mowa w ust. 2, stanowią informacje o zidentyfikowanej lub możliwej do bezpośredniego lub pośredniego zidentyfikowania osobie fizycznej, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

4. System ochrony danych osobowych, z zastrzeżeniem art. 6 pkt 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 i 1669) i art. 3 pkt 2 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), tworzą:

1) przepisy ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym oraz wydane na jego podstawie akty wykonawcze;

2) przepisy niniejszego zarządzenia;

3) decyzja nr 3/11 Szefa Centralnego Biura Antykorupcyjnego z dnia 3 stycznia 2011 r. w sprawie określenia zasad i trybu kontroli przetwarzania danych osobowych w Centralnym Biurze Antykorupcyjnym (Dz. Urz. CBA z 2011 r. Nr 1, poz. 24),

4) decyzja nr 88/11 Szefa Centralnego Biura Antykorupcyjnego z dnia 21 lutego 2011 r. w sprawie określenia trybu weryfikacji i usuwania danych osobowych przetwarzanych w Centralnym Biurze Antykorupcyjnym (Dz. Urz. CBA z 2011 r. Nr 1, poz. 32, z późn. zm).

5. Prawidłowość funkcjonowania systemu podlega kontroli pełnomocnika, o którym mowa w ustawie o CBA.

§ 2. Zarządzenie określa dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych w CBA odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, którą stanowią:

1) Polityka bezpieczeństwa ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym, określona w załączniku nr 1,

2) Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w Centralnym Biurze Antykorupcyjnym, określona w załączniku nr 2.

§ 3. 1. Dokumentacja stosowana w związku z przetwarzaniem danych osobowych w CBA obejmuje:

1) zgłoszenie zbiorów danych osobowych, którego wzór określa załącznik nr 3;

2) ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór określa załącznik nr 4;

3) zaświadczenie o ukończeniu szkolenia z zakresu ochrony danych osobowych, którego wzór określa załącznik nr 5.

§ 4. Kierownicy jednostek organizacyjnych są obowiązani do zapoznania podległych im funkcjonariuszy i pracowników z zarządzeniem w terminie 14 dni od dnia jego wejścia w życie.

§ 5. Obowiązek, o którym mowa § 6 ust. 1 pkt 6 załącznika nr 1, stanowiący zgłoszenie aktualizacyjne, zostanie zrealizowany po raz pierwszy w terminie 21 dni od wejścia w życie zarządzenia.

§ 6. Traci moc zarządzenie nr 18/16 Szefa Centralnego Biura Antykorupcyjnego z dnia 1 lipca 2016 r. w sprawie systemu ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym (Dz. Urz. CBA z 2016 r. poz. 18).

§ 7. Zarządzenie wchodzi w życie z dniem ogłoszenia.

Szef Centralnego Biura Antykorupcyjnego

Ernest Bejda

Załącznik Nr 1 do Zarządzenia Nr 6/19
Szefa Centralnego Biura Antykorupcyjnego
z dnia 6 lutego 2019 r.

Rozdział 1.
Organizacja systemu ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym

§ 1. 1. W systemie ochrony danych osobowych w CBA wyróżnia się:

1) administratora danych osobowych;

2) pełnomocnika do spraw kontroli przetwarzania przez Centralne Biuro Antykorupcyjne danych osobowych, o którym mowa w art. 22b ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2018 r. poz. 2104 i 2399 oraz z 2019 r. poz. 53 i 125, zwanego dalej „pełnomocnikiem”;

3) administratora bezpieczeństwa informacji;

4) lokalnych administratorów danych osobowych;

5) administratora systemu;

6) administratorów bezpieczeństwa zbiorów;

7) osoby upoważnione do przetwarzania danych osobowych w CBA.

2. Podmioty, o których mowa w ust. 1, każdy w zakresie swojego działania, odpowiadają za realizację obowiązku przestrzegania zasady legalności, celowości, merytorycznej poprawności, adekwatności oraz ograniczenia czasowego przetwarzania danych osobowych w CBA.

§ 2. Szef CBA, jako administrator danych osobowych, podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem konieczności właściwej realizacji zadań CBA oraz aktualnych technik zabezpieczenia tych danych.

§ 3. 1. Pełnomocnik wykonuje zadania administratora bezpieczeństwa informacji.

2. Pełnomocnik, niezależnie od zadań określonych w § 4, sprawuje nadzór nad zgodnością z prawem przetwarzania danych osobowych gromadzonych przez CBA, w szczególności przez:

1) kontrolę prawidłowości przetwarzania przez CBA danych osobowych;

2) wydawanie pisemnych poleceń usunięcia stwierdzonych uchybień w zakresie prawidłowości przetwarzania danych osobowych;

3) prowadzenie działań zmierzających do wyjaśnienia okoliczności naruszenia przepisów w zakresie przetwarzania danych osobowych w CBA;

4) wydawanie zaleceń dotyczących usprawnienia systemu ochrony danych osobowych w CBA;

5) inicjowanie zmian w polityce bezpieczeństwa ochrony danych osobowych w CBA w celu zapewnienia właściwego poziomu ochrony ich przetwarzania.

§ 4. 1. Administrator bezpieczeństwa informacji:

1) zapewnia przestrzeganie przepisów o ochronie danych osobowych w CBA;

2) sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania;

3) nadzoruje opracowanie i aktualizację dokumentacji przetwarzania danych osobowych, o której mowa w § 2 zarządzenia;

4) prowadzi wykaz zbiorów danych osobowych przetwarzanych w CBA;

5) prowadzi rejestr zbiorów danych;

6) prowadzi szkolenia z zakresu ochrony danych osobowych dla osób upoważnionych do przetwarzania danych osobowych.

2. Administrator bezpieczeństwa informacji wykonuje również powierzone mu zadania administratora danych osobowych polegające na:

1) nadzorze nad realizacją obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych;

2) dokonywaniu okresowej analizy zagrożeń dla bezpieczeństwa danych osobowych oraz zlecaniu jej przeprowadzenia dla zbiorów przetwarzanych danych osobowych;

3) realizowaniu procedur związanych ze zgłaszaniem Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych osobowych przetwarzanych w CBA podlegających rejestracji;

4) udzielaniu osobom uprawnionym informacji o zasadach i sposobach przetwarzania danych osobowych w CBA.

§ 5. Zadania lokalnych administratorów danych osobowych wykonują, w podległych im jednostkach organizacyjnych CBA, o których mowa w statucie CBA, kierownicy tych jednostek.

§ 6. 1. Lokalny administrator danych osobowych:

1) sprawuje bieżący, bezpośredni nadzór nad właściwym przetwarzaniem danych osobowych;

2) zgłasza administratorowi bezpieczeństwa informacji wszelkie nieprawidłowości dotyczące przetwarzania danych osobowych i podejmuje w tym zakresie działania zmierzające do ich wyjaśnienia;

3) wyznacza administratorów bezpieczeństwa zbiorów, w których przetwarzane są dane osobowe, chyba że sami wykonują ich zadania;

4) kieruje na szkolenie z zakresu ochrony danych osobowych osoby upoważnione do ich przetwarzania;

5) wykonuje zalecenia administratora bezpieczeństwa informacji w zakresie ochrony danych osobowych;

6) niezwłocznie przekazuje administratorowi bezpieczeństwa informacji aktualne dane do wykazu i rejestru, o których mowa odpowiednio w § 4 ust. 1 pkt 4 i 5, według wzoru zgłoszenia określonego w załączniku nr 3 do zarządzenia, z wyłączeniem informacji o zbiorach doraźnych;

7) zgłasza administratorowi bezpieczeństwa informacji zmiany w organizacji mające wpływ na ochronę danych osobowych w podległej jednostce organizacyjnej.

2. Lokalny administrator danych osobowych wykonuje zadania administratora danych osobowych polegające na:

1) nadawaniu i aktualizacji upoważnień do przetwarzania danych osobowych;

2) określaniu obowiązków i zakresu odpowiedzialności osób upoważnionych do przetwarzania danych osobowych oraz prowadzeniu ewidencji tych osób według wzoru określonego w załączniku nr 4 do zarządzenia;

3) opracowaniu i aktualizacji instrukcji zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w zbiorze prowadzonym w podległej jednostce organizacyjnej w przypadku, gdy system, z uwagi na specyfikę swojego działania, nie podlega regulacjom instrukcji, o której mowa w § 2 pkt 2 zarządzenia;

4) stosowaniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;

5) udostępnianiu danych osobowych ze zbiorów danych podmiotom uprawnionym do ich otrzymania w związku z realizacją zadań służbowych.

3. Zakres i formę upoważnienia, o którym mowa w ust. 2 pkt 1, określają przepisy dotyczące zakresów obowiązków i odpowiedzialności funkcjonariuszy i pracowników CBA.

4. Instrukcja, o której mowa w ust. 2 pkt 3, przed zatwierdzeniem przez lokalnego administratora danych osobowych podlega akceptacji administratora bezpieczeństwa informacji.

§ 7. 1. Administratorem systemu jest kierownik jednostki organizacyjnej, do której zadań należy zapewnienie ciągłości działania systemów i sieci teleinformatycznych służących do przetwarzania danych osobowych.

2. Szczegółowe zadania administratora systemu określa instrukcja.

§ 8. Administratorzy bezpieczeństwa zbiorów są obowiązani w zakresie podległych im zbiorów danych osobowych do:

1) wdrażania i nadzorowania przestrzegania dokumentacji przetwarzania danych osobowych, o której mowa w § 2 zarządzenia, z uwzględnieniem § 6 ust. 2 pkt 3.

2) wykonywania zaleceń administratora bezpieczeństwa informacji w zakresie ochrony danych osobowych.

Rozdział 2.
Cel i zakres stosowania Polityki bezpieczeństwa ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym

§ 9. Polityka bezpieczeństwa ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym, zwana dalej „polityką bezpieczeństwa", ma na celu zabezpieczenie przetwarzanych danych osobowych w CBA.

§ 10. 1. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w sposób tradycyjny oraz w systemach teleinformatycznych.

2. Dane osobowe mogą być przetwarzane w systemach teleinformatycznych CBA połączonych z siecią Internet wyłącznie za pośrednictwem połączenia udostępnionego i administrowanego przez administratora systemu i pod warunkiem wykorzystania dostarczonych przez administratora systemu urządzeń i technologii.

Rozdział 3.
Obowiązki osób upoważnionych do przetwarzania danych osobowych

§ 11. 1. Osoba upoważniona do przetwarzania danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków służbowych.

2. Zwolnienie ze służby, rozwiązanie stosunku pracy, odwołanie z zajmowanego stanowiska lub przeniesienie do dyspozycji Szefa CBA powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

§ 12. 1. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia.

2. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres pełnienia służby lub zatrudnienia w CBA, a także po ustaniu stosunku służby lub pracy.

§ 13. 1. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana zapoznać się i przestrzegać przepisów w zakresie ochrony danych osobowych, w szczególności postanowień polityki bezpieczeństwa i instrukcji.

2. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana do stosowania określonych przez administratora danych osobowych oraz administratora bezpieczeństwa informacji procedur oraz zaleceń mających na celu zgodne z prawem przetwarzanie danych.

§ 14. 1. Osoba upoważniona do przetwarzania danych osobowych korzysta z systemu teleinformatycznego CBA zgodnie z dokumentacją użytkową i zaleceniami administratora bezpieczeństwa informacji.

2. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana:

1) zabezpieczać dane przed ich udostępnianiem osobom nieupoważnionym;

2) przetwarzać dane w sposób uniemożliwiający dostęp osób nieupoważnionych.

Rozdział 4.
Obszary przetwarzania danych osobowych

§ 15. 1. Obszar przetwarzania danych osobowych w CBA stanowi obszar budynków pozostających w dyspozycji CBA, nad którymi nadzór sprawuje wyłącznie CBA.

2. Środki bezpieczeństwa, w tym środki ochrony fizycznej, stosowane w obszarach przetwarzania danych osobowych na podstawie odrębnych przepisów, stosuje się również do systemów teleinformatycznych, o których mowa w § 10 ust. 2.

3. Przetwarzanie danych osobowych poza obszarami, o których mowa w ust. 1, jest dopuszczalne, jeśli wynika to z upoważnienia, o którym mowa w § 6 ust. 2 pkt 1 i zgody lokalnego administratora danych osobowych.

Rozdział 5.
Szkolenia z zakresu ochrony danych osobowych

§ 16. 1. Administrator bezpieczeństwa informacji przeprowadza szkolenia dla osób upoważnionych do przetwarzania danych osobowych w CBA.

2. Szkolenie przeprowadza się obligatoryjnie także w przypadku istotnej zmiany zasad ochrony danych osobowych.

3. Tematyka szkoleń obejmuje:

1) przepisy dotyczące ochrony danych osobowych;

2) sposoby ochrony danych przed osobami postronnymi i zasady udostępniania danych osobom, których one dotyczą;

3) obowiązki osób upoważnionych do przetwarzania danych osobowych i innych;

4) zasady odpowiedzialności za naruszenie obowiązków z zakresu ochrony danych osobowych.

4. Osoba przeszkolona otrzymuje zaświadczenie o ukończeniu szkolenia, według wzoru określonego w załączniku nr 5 oraz składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie danych osobowych.

§ 17. Przeszkolenie w CBA w zakresie, o którym mowa w § 16, przed dniem wejścia w życie zarządzenia, zachowuje ważność bez konieczności wystawiania zaświadczeń.

Rozdział 6.
Zasady ochrony danych osobowych

§ 18. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana do:

1) przetwarzania ich wyłącznie w zakresie zgodnym z udzielonym upoważnieniem;

2) przetwarzania ich tylko w zakresie wynikającym z obowiązków służbowych;

3) przetwarzania ich zgodnie z celem ich gromadzenia i przetwarzania w CBA;

4) ciągłej weryfikacji adekwatności i niezbędności posiadanych oraz przetwarzanych danych osobowych.

§ 19. 1. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana do przestrzegania zasad bezpieczeństwa systemu teleinformatycznego, do którego posiadają dostęp, w szczególności poprzez:

1) zakaz samodzielnego instalowania oprogramowania na urządzeniach przetwarzających dane osobowe;

2) zakaz gromadzenia i przechowywania w urządzeniach przetwarzających dane osobowe, danych niezwiązanych z realizacją zadań służbowych, w szczególności plików multimedialnych;

3) zakaz celowego opracowywania, generowania, kompilowania, kopiowania, rozpowszechniania, uruchamiania lub usiłowania wprowadzania szkodliwych kodów komputerowych, określanych powszechnie jako „kody złośliwe”, w szczególności wirusów, trojanów, keyloggerów, na urządzeniach przetwarzających dane osobowe;

4) stosowanie zasad ochrony antywirusowej, w szczególności sprawdzanie nośników zewnętrznych przed ich użyciem programem antywirusowym zainstalowanym przez administratora systemu.

§ 20. Do podstawowych zasad bezpieczeństwa przetwarzania danych osobowych w CBA należy:

1) zakaz udostępniania identyfikatora i hasła uprawniającego do przetwarzania danych osobowych w systemie teleinformatycznym innym osobom;

2) obowiązek działania osób upoważnionych do przetwarzania danych osobowych wyłącznie w granicach swoich uprawnień do przetwarzania danych osobowych;

3) nakaz ewidencjonowania materiałów i nośników zawierających dane osobowe;

4) obowiązek stosowania się do zaleceń administratora bezpieczeństwa informacji;

5) niszczenie zbędnych materiałów zawierających dane osobowe;

6) kasowanie zbędnych plików zawierających dane osobowe w systemach teleinformatycznych;

7) obowiązek przechowywania w meblach biurowych zamykanych na klucz wszelkich dokumentów w formie papierowej po zakończeniu pracy z danymi osobowymi, z wyłączeniem przypadków, gdy odrębne przepisy nakładają wyższe rygory bezpieczeństwa ich przechowywania;

8) zakaz pozostawiania bez nadzoru urządzeń przenośnych oraz nośników zawierających dane osobowe poza obszarami przetwarzania danych;

9) zakaz pozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, w tym pracowników serwisu czy też osób sprzątających, bez obecności osoby upoważnionej do przetwarzania danych osobowych lub innej osoby upoważnionej do przebywania w tym pomieszczeniu;

10) zakaz przesyłania i wynoszenia poza obszar przetwarzania danych osobowych całych zbiorów danych oraz szerokich z nich wypisów, także w postaci zaszyfrowanej, bez upoważnienia lokalnego administratora danych osobowych;

11) przesyłanie danych osobowych internetową pocztą elektroniczną w postaci zaszyfrowanej, z zastrzeżeniem zakazu, o którym mowa w pkt 10.

§ 21. Lokalny administrator danych osobowych, uwzględniając zasady bezpieczeństwa przetwarzania danych osobowych, wskazuje stacje robocze, na których są przetwarzane dane osobowe, które będą posiadały połączenie z Internetem.

§ 22. Administrator bezpieczeństwa zbioru, w zakresie podległego mu zbioru danych osobowych, na podstawie wytycznych przekazanych przez administratora bezpieczeństwa informacji, określa:

1) strukturę zbioru danych, ze wskazaniem poszczególnych pól informacyjnych i powiązań między nimi;

2) programy zastosowane do przetwarzania danych osobowych;

3) sposób przekazywania danych między poszczególnymi systemami.

Załącznik Nr 2 do Zarządzenia Nr 6/19

Szefa Centralnego Biura Antykorupcyjnego

z dnia 6 lutego 2019 r.

Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w Centralnym Biurze Antykorupcyjnym

Rozdział 1.
Zagadnienia ogólne

§ 1. 1. Instrukcja określa sposób zarządzania i funkcjonowania systemu teleinformatycznego, wykorzystywanego do przetwarzania danych osobowych w CBA, zwanego dalej „systemem teleinformatycznym", w celu zabezpieczenia danych osobowych przed zagrożeniami, w szczególności przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Przepisów instrukcji nie stosuje się w przypadku, gdy system teleinformatyczny posiada odrębną dokumentację obowiązującą na podstawie wewnętrznych aktów prawnych Szefa CBA lub wydaną przez lokalnego administratora danych osobowych instrukcję zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w zbiorze prowadzonym w podległej jednostce organizacyjnej, o której mowa w § 6 ust. 2 pkt 3 Polityki bezpieczeństwa ochrony danych osobowych w CBA.

Rozdział 2.
Procedura nadawania uprawnień do przetwarzania danych osobowych i rejestrowanie lub wyrejestrowywanie uprawnień w systemie teleinformatycznym

§ 2. 1. Dostęp do systemu teleinformatycznego może uzyskać wyłącznie osoba upoważniona przez lokalnego administratora danych osobowych do przetwarzania danych osobowych i zarejestrowana w tym systemie przez administratora systemu jako użytkownik.

2. Rejestracja użytkownika, następuje na wniosek lokalnego administratora danych osobowych i polega na przyporządkowaniu mu: identyfikatora, przydzieleniu hasła i nadaniu określonych we wniosku uprawnień oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§ 3. 1. Wyrejestrowania użytkownika z systemu teleinformatycznego dokonuje administrator systemu na wniosek lokalnego administratora danych osobowych lub administratora bezpieczeństwa informacji.

2. Wyrejestrowanie może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje przez:

1) zablokowanie konta użytkownika lub odebranie uprawnień do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe);

2) usunięcie danych użytkownika z bazy użytkowników systemu lub odebranie uprawnień (wyrejestrowanie trwałe).

§ 4. Czasowe wyrejestrowanie użytkownika z systemu teleinformatycznego może nastąpić w razie:

1) nieobecności dłuższej niż 30 dni kalendarzowych;

2) zawieszenia w czynnościach służbowych;

3) wszczęcia postępowania dyscyplinarnego;

4) przeniesienia do dyspozycji Szefa CBA.

§ 5. Rozwiązanie lub wygaśnięcie stosunku służby, pracy lub innego stosunku prawnego, w ramach którego użytkownik wykonywał swoje obowiązki oraz odebranie uprawnień stanowi podstawę do trwałego wyrejestrowania użytkownika z systemu teleinformatycznego.

Rozdział 3.
Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 6. 1. Użytkownicy są uprawnieni do logowania się do systemu teleinformatycznego tylko na własne konto założone przez administratora systemu.

2. Dostęp jest indywidualnie zdefiniowany dla każdego użytkownika. Użytkownik ma dostęp jedynie do zasobów, które są mu niezbędne do wykonywania obowiązków służbowych.

3. Tożsamość użytkownika systemu jest jednoznacznie określona i sprawdzona przed rozpoczęciem pracy w systemie (uwierzytelnienie).

4. Uwierzytelnienie w systemie teleinformatycznym odbywa się z wykorzystaniem indywidualnych haseł oraz wymaga od użytkowników w szczególności:

1) nieujawniania haseł do kont w systemie teleinformatycznym;

2) natychmiastowej zmiany hasła w przypadku podejrzenia jego ujawnienia, o ile istnieje taka możliwość techniczna.

§ 7. 1. Aktualne hasła do kont administratora systemu przechowuje administrator systemu w zbiorze haseł awaryjnych.

2. Hasła, o których mowa w ust. 1, są przechowywane odrębnie dla każdego systemu i zabezpieczone przed dostępem osób nieuprawnionych.

3. Administrator systemu dokumentuje każdy dostęp i użycie hasła ze zbioru, o którym mowa w ust. 1.

§ 8. 1. Użytkownik jest odpowiedzialny za użycie zasobów teleinformatycznych przy wykorzystaniu jego identyfikatora i hasła, z zastrzeżeniem ust. 6.

2. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

3. Pierwsze hasło wymagane do uwierzytelnienia się w systemie teleinformatycznym przydzielane jest przez administratora systemu po pouczeniu osoby upoważnionej o obowiązku zachowania haseł w tajemnicy oraz po potwierdzeniu odbioru pierwszego hasła.

4. System teleinformatyczny automatycznie wymusza zmianę hasła przy pierwszym logowaniu oraz co 30 dni.

5. Administrator bezpieczeństwa informacji może, w uzasadnionych przypadkach, polecić użytkownikowi dokonanie zmiany hasła.

6. Administrator systemu jest uprawniony do dokonania zmiany hasła dostępu do konta na wniosek użytkownika lub jego przełożonego.

7. Zablokowanie konta użytkownika w systemie, o ile istnieje taka możliwość techniczna, następuje po trzech nieudanych próbach wprowadzenia hasła.

Rozdział 4.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemuteleinformatycznego

§ 9. 1. Rozpoczęcie pracy na stacji roboczej w systemie teleinformatycznym następuje po wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora (logowanie).

2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w obecności użytkownika lub innej osoby upoważnionej do przebywania w tym pomieszczeniu.

§ 10. 1. Na stacjach roboczych w systemie teleinformatycznym należy stosować wygaszacze ekranu.

2. W przypadku czasowego opuszczenia stanowiska pracy użytkownik jest obowiązany zablokować stację roboczą.

3. Zakończenie pracy na stacji roboczej następuje po prawidłowym wylogowaniu się użytkownika.

§ 11. 1. Użytkownik powiadamia administratora systemu o braku możliwości zalogowania się na konto przez użytkownika lub stwierdzenia innych nieprawidłowości w pracy systemu.

2. W przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane w tym celu narzędzia programowe lub sprzętowe, użytkownik niezwłocznie powiadamia o tym fakcie administratora systemu oraz lokalnego administratora danych osobowych.

Rozdział 5.
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania oraz zasady ich przechowywania

§ 12. 1. Użytkownicy nie są upoważnieni do kopiowania całych zbiorów danych osobowych.

2. Całe zbiory danych mogą być kopiowane tylko przez administratora systemu, administratora bezpieczeństwa zbioru lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.

3. Jednostkowe dane osobowe mogą być kopiowane na nośniki pod warunkiem, że po ustaniu przydatności tych kopii należy trwale skasować dane lub fizycznie zniszczyć nośniki, na których są przechowywane.

§ 13. 1. Tworzenie kopii zapasowych zbiorów danych jest obligatoryjne.

2. Częstotliwość tworzenia kopii zapasowych musi uwzględniać charakter zbioru, częstotliwość jego modyfikacji oraz zmiany liczby danych oraz zasady jego funkcjonowania.

§ 14. Nośniki zawierające kopie zapasowe należy oznaczać jako „kopia zapasowa” wraz z podaniem daty sporządzenia i nazwy systemu teleinformatycznego, o ile istnieje taka możliwość.

§ 15. Administrator bezpieczeństwa informacji w uzgodnieniu z administratorem systemu określa:

1) szczegółowe procedury tworzenia i niszczenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania;

2) zasady przechowywania i udostępniania kopii, o których mowa w pkt 1.

Rozdział 6.
Sposób i miejsce przechowywania elektronicznych nośników informacji zawierających dane osobowe

§ 16. 1. Elektroniczne nośniki informacji zawierające dane osobowe przechowuje się w sposób zapewniający ochronę przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem.

2. Dopuszcza się przechowywanie nośników, o których mowa w ust. 1, w zamykanych na klucz meblach biurowych, z wyłączeniem przypadków, gdy odrębne przepisy nakładają wyższe rygory bezpieczeństwa ich przechowywania.

3. Nośniki, o których mowa w ust. 1, podlegają obligatoryjnemu ewidencjonowaniu.

§ 17. Nośniki, o których mowa w § 16 ust. 1, nie mogą być pozostawiane bez nadzoru poza obszarem przetwarzania danych osobowych.

§ 18. Podstawowe zasady bezpieczeństwa przetwarzania danych osobowych w CBA, o których mowa w polityce bezpieczeństwa stosuje się również do danych osobowych zgromadzonych na nośnikach, o których mowa w § 16 ust. 1.

Rozdział 7.
Zabezpieczenie systemu teleinformatycznego przed oprogramowaniem szkodliwym oraz przeglądy i konserwacja systemów i nośników służących do przetwarzania danych osobowych

§ 19. 1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, uszkodzone lub nienadające się do dalszej eksploatacji niszczy się w sposób uniemożliwiający ich odczytanie.

2. Naprawa urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe, jest przeprowadzana wyłącznie na obszarze przetwarzania danych osobowych w CBA.

3. Naprawa urządzeń przetwarzających dane osobowe może zostać przeprowadzona poza siedzibą CBA po wymontowaniu z nich i pozostawieniu w siedzibie CBA dysków lub innych elektronicznych nośników informacji.

§ 20. Administrator systemu jest obowiązany do:

1) zainstalowania i aktualizowania oprogramowania antywirusowego oraz określenia częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie;

2) usuwania wszelkich nieprawidłowości w pracy systemu;

3) zapewnienia ciągłości pracy systemu i nadzoru nad jego prawidłowym funkcjonowaniem;

4) przeglądu i konserwacji systemu.

§ 21. 1. Administrator bezpieczeństwa informacji w uzgodnieniu z administratorem systemu określa sposób zabezpieczenia systemu teleinformatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu.

2. Administrator bezpieczeństwa informacji w uzgodnieniu z administratorem systemu określa procedury wykonywania przeglądów i konserwacji systemów oraz nośników służących do przetwarzania danych osobowych.

Rozdział 8.
Warunki eksploatacji systemu teleinformatycznego oraz realizacji wymagań rozliczalności przetwarzania danych osobowych w systemach

§ 22. 1. System teleinformatyczny posiadający połączenie z Internetem chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2. Administrator systemu, w uzgodnieniu z administratorem bezpieczeństwa informacji, określa sposób zabezpieczenia systemu teleinformatycznego posiadającego połączenie z Internetem.

§ 23. Administrator bezpieczeństwa informacji, w uzgodnieniu z administratorem systemu, określa rodzaj, zakres i czas przechowywania informacji o zdarzeniach w systemie teleinformatycznym, gromadzonych dla potrzeb kontroli.

§ 24. Do podstawowych zasad bezpiecznej eksploatacji systemów przeznaczonych do przetwarzania danych osobowych należy:

1) zakaz podłączania do gniazd dedykowanej sieci elektrycznej przeznaczonych dla sprzętu komputerowego innych urządzeń;

2) obowiązek dbania o prawidłową eksploatację sprzętu i oprogramowania zgodnie z instrukcjami, wytycznymi administratora systemu i administratora bezpieczeństwa informacji oraz zaleceniami producenta.

Załącznik Nr 3 do Zarządzenia Nr 6/19
Szefa Centralnego Biura Antykorupcyjnego
z dnia 6 lutego 2019 r.

WZÓR ZGŁOSZENIA
WYKAZ ZBIORÓW DANYCH OSOBOWYCH PROWADZONYCH W <NAZWA JEDNOSTKI ORGANIZACYJNEJ CBA>

Nazwa zbioru			**Nazwa podzbioru**			
Podstawa prawna utworzenia podzbioru			**Cel przetwarzania**			
Data utworzenia	**Opis kategorii osób, których dane są przetwarzane w podzbiorze**	**Zakres danych osobowych**	**Forma funkcjonowania podzbioru danych[1]**	**Miejsce przetwarzania danych osobowych[2]**	**Klauzula tajności podzbioru**	**Sposób zbierania danych do podzbioru[3]**
Imię i nazwisko administratora bezpieczeństwa zbioru	**Dokumentacja przetwarzania danych osobowych**	**Poziom bezpieczeństwa danych osobowych[4]**	**Podmiot, któremu powierzono przetwarzanie danych z podzbioru**	**Sposób udostępniania danych z podzbioru[5]**	**Odbiorca danych lub kategoria odbiorców, którym dane mogą być przekazywane**	**Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego**

.....
(podpis lokalnego administratora danych osobowych)

[1] Forma:
- papierowa/teleinformatyczna/dualna (papierowa i teleinformatyczna), w przypadku zbioru funkcjonującego w systemie teleinformatycznym należy dodatkowo wskazać program zastosowany do przetwarzania danych
- system scentralizowany/rozproszony – z uwagi na strukturę zbioru

[2] adres siedziby, piętro pokoju, w przypadku przetwarzania danych osobowych w środowisku rozproszonym należy wskazać nazwę sieci lub lokalizację stanowisk, na których są przetwarzane dane

[3] w szczególności należy podać informację, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą

[4] podstawowy (w systemie teleinformatycznym nie są przetwarzane dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, żadne z urządzeń systemu nie jest połączone z siecią publiczną); podwyższony (w systemie teleinformatycznym są przetwarzane dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, żadne z urządzeń systemu nie jest połączone z siecią publiczną); wysoki (co najmniej jedno urządzenie systemu teleinformatycznego połączone jest z siecią publiczną).

[5] w szczególności należy podać informację, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa

Załącznik Nr 4 do Zarządzenia Nr 6/19
Szefa Centralnego Biura Antykorupcyjnego
z dnia 6 lutego 2019 r.

WZÓR

Ewidencja osób upoważnionych do przetwarzania danych osobowych w ……
(nazwa jednostki organizacyjnej)

Lp.	Identyfikator upoważnionego	Imię i nazwisko	Nazwa zbioru/podzbioru/ systemu danych osobowych	Zakres upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Uwagi

……

(data i podpis lokalnego administrator danych osobowych)

Załącznik Nr 5 do Zarządzenia Nr 6/19
Szefa Centralnego Biura Antykorupcyjnego
z dnia 6 lutego 2019 r.

WZÓR

ZAŚWIADCZENIE NR …….

o ukończeniu szkolenia z zakresu ochrony danych osobowych

wydane przez administratora bezpieczeństwa informacji w Centralnym Biurze Antykorupcyjnym

***Pani/Panu*.....**

Identyfikator nr .....

Na podstawie zarządzenia nr .../19
Szefa Centralnego Biura Antykorupcyjnego
z dnia ..... 2019 r.
w sprawie systemu ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym

……, dnia ……. *……*
(pieczęć i podpis)