**ZARZĄDZENIE Nr ...39.../15**
**DYREKTORA GENERALNEGO SŁUŻBY WIĘZIENNEJ**
z dnia ..03...09... 2015 r.

**w sprawie zabezpieczenia danych osobowych w Centralnym Zarządzie Służby Więziennej**

Na podstawie art. 11 ust. 1 pkt 11 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. z 2014 r. poz. 1415 i 1822 oraz z 2015 r. poz. 529 i 928) oraz w związku z art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) i § 3 ust. 1 i 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) zarządza się, co następuje:

**§ 1.** 1. Wprowadza się do stosowania w Centralnym Zarządzie Służby Więziennej, zwanym dalej „CZSW", Politykę Bezpieczeństwa Danych Osobowych, zwaną dalej „PBDO".

2. Użyte w zarządzeniu określenia oznaczają:

1) ADO - Administratora Danych Osobowych w CZSW, którym jest Dyrektor Generalny Służby Więziennej;
2) ASI - Administratora Systemu Informatycznego w CZSW, odpowiedzialnego za realizację zabezpieczeń i odpowiednie funkcjonowanie systemu informatycznego, o którym mowa w zarządzeniu Nr 26/2014 Dyrektora Generalnego Służby Więziennej z dnia 11 lipca 2014 r. w sprawie ustanowienia systemu zarządzania bezpieczeństwem informacji w Centralnym Zarządzie Służby Więziennej i wprowadzenia polityki bezpieczeństwa informacji;
3) dane osobowe – wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) GIODO – Generalnego Inspektora Ochrony Danych Osobowych;

5) KI – komórkę organizacyjną CZSW odpowiedzialną za opracowywanie, wdrażanie i eksploatację systemów informatycznych oraz nadzór nad ich funkcjonowaniem;
6) KKI – kierownika KI;
7) KKO - kierownika komórki organizacyjnej w CZSW lub osobę zatrudnioną na jednoosobowym stanowisku pracy;
8) komórka organizacyjna – odpowiednio biuro, wydział, zespół lub jednoosobowe stanowisko pracy w CZSW;
9) naruszenie bezpieczeństwa danych osobowych – jakiekolwiek naruszenie poufności, integralności lub dostępności danych osobowych powstałe samoistnie, lub w wyniku działania osób;
10) PBI – zarządzenie Nr 26/2014 Dyrektora Generalnego Służby Więziennej z dnia 11 lipca 2014 r. w sprawie ustanowienia systemu zarządzania bezpieczeństwem informacji w Centralnym Zarządzie Służby Więziennej i wprowadzenia polityki bezpieczeństwa informacji;
11) pełnomocnik – wyznaczonego przez Dyrektora Generalnego Służby Więziennej pełnomocnika ds. ochrony danych osobowych;
12) przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie (archiwizowanie), opracowywanie, zmienianie, udostępnianie i usuwanie;
13) SW – Służbę Więzienną;
14) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych osobowych;
15) u.o.d.o. - ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
16) u.s.w. – ustawę z dnia 9 kwietnia 2010 r. o Służbie Więziennej;
17) użytkownik – osobę uprawnioną do przetwarzania danych osobowych w systemie informatycznym, która posiada ustalony indywidualny identyfikator oraz hasło.

**§ 2.** 1. PBDO określa zasady zarządzania procesami przetwarzania danych osobowych oraz ich bezpieczeństwem w CZSW i stanowi element składowy systemu zarządzania bezpieczeństwem informacji określonego w PBI.

2. PBDO ma zastosowanie do wszystkich danych osobowych, bez względu na formę ich przetwarzania.

3. Zasady przetwarzania danych w systemach informatycznych określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiąca załącznik nr 1 do niniejszego zarządzenia.

§ 3.1. Obszarem przetwarzania danych osobowych przez CZSW są budynki i pomieszczenia, w których są przetwarzane dane osobowe w formie papierowej lub w systemie informatycznym.

2. Obszar przetwarzania danych osobowych stanowią:

1) wszystkie pomieszczenia budynku CZSW za wyjątkiem:
   a) pomieszczeń Niepublicznego Zakładu Opieki Zdrowotnej funkcjonującego przy CZSW,
   b) pomieszczeń socjalnych znajdujących się w budynku CZSW (w szczególności: toalety, bar znajdujący się na parterze budynku, palarnia),
   c) pomieszczenia siłowni na poziomie -1 budynku CZSW,
   d) pomieszczeń warsztatowych na poziomie -1 budynku CZSW,
   e) korytarzy budynku CZSW,
   f) sali konferencyjnej CZSW,
   g) pomieszczeń Biura Emerytalnego przy CZSW;
   h) pomieszczeń magazynowych znajdujących się na poziomie -1 budynku CZSW, oraz magazynki gospodarcze środków czystości (znajdujące się na piętrze 1 i 3 budynku CZSW);
2) pomieszczenia centralnej serwerowni SW i pomieszczenia biurowe kierowców, znajdujące się na terenie Aresztu Śledczego Warszawa-Mokotów przy ul. Rakowieckiej 37;
3) pomieszczenia hotelu, przy CZSW wykorzystywane, jako pomieszczenia biurowe;
4) pomieszczenia użytkowane przez CZSW znajdujące się w budynku Okręgowego Inspektoratu Służby Więziennej w Warszawie, przy ulicy Wiśniowej 50;
5) pomieszczenia Biura Dozoru Elektronicznego znajdujące się w budynku przy ul. Zwycięzców 34.

3. Przebywanie wewnątrz obszaru, o którym mowa w ust. 2, osób nieupoważnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą ADO.

4. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania ustalonych w CZSW zasad dotyczących wprowadzania osób trzecich do obszaru, o którym mowa w ust 2.

5. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, są zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.

6. Ochrona pomieszczeń i budynków użytkowanych przez CZSW jest realizowana zgodnie z PBI.

§ 4.1. W CZSW przetwarza się następujące zbiory danych osobowych:

1) dane funkcjonariuszy SW i pracowników pełniących służbę lub zatrudnionych w CZSW oraz poza CZSW;
2) dane osób współpracujących z CZSW na podstawie umów cywilnoprawnych (zlecenia lub umowy o dzieło);
3) dane osób, wobec których jest lub było wykonywane pozbawienie wolności w jednostkach organizacyjnych SW, oraz osób, wobec których sąd skierował orzeczenie oczekujące na wykonanie;
4) dane osób zarejestrowanych w systemie komunikacyjno-monitorującym systemu dozoru elektronicznego – zbiór powierzony do przetwarzania przez Ministerstwo Sprawiedliwości;
5) dane osób prenumerujących czasopisma wydawane przez CZSW;
6) rejestr korespondencji – dane osobowe adresatów i nadawców pism.

2. Szczegółowy opis zbiorów danych osobowych jest prowadzony zgodnie ze wzorem wykazu zbiorów danych osobowych określonym w załączniku nr 2 do niniejszego zarządzenia.

§ 5. W CZSW obowiązują zabezpieczenia systemów informatycznych na poziomie wysokim, określonym w § 6 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 6.1. ADO jest odpowiedzialny za przetwarzanie i ochronę danych osobowych w CZSW.

2. Dyrektor Generalny Służby Więziennej wyznacza pełnomocnika, który wykonuje zadania w imieniu administratora danych, o których mowa w art. 36b u.o.d.o., w szczególności w zakresie:

1) nadzoru nad przestrzeganiem zasad ochrony danych osobowych w CZSW;
2) nadzoru nad aktualnością niniejszego dokumentu;
3) prowadzenia i aktualizowania dokumentacji, o której mowa w § 4 ust. 2;
4) prowadzenia aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych zgodnie ze wzorem określonym w załączniku nr 3 do niniejszego zarządzenia;
5) przygotowywania zgłoszeń zbiorów danych osobowych CZSW do rejestracji GIODO oraz aktualizacji tych zgłoszeń;
6) organizowania szkoleń, mających na celu pogłębienie wiedzy i podnoszenie świadomości w zakresie ochrony danych osobowych;
7) wydawania zaleceń dla KKO w zakresie podwyższenia standardów zabezpieczeń danych osobowych;
8) udziału w czynnościach kontrolnych dokonywanych w CZSW przez uprawnione w zakresie ochrony danych osobowych organy państwowe.

3. Pełnomocnik może mieć powierzone wykonywanie innych zadań, o ile nie naruszają prawidłowego wykonywania jego obowiązków związanych z nadzorem nad ochroną danych osobowych.

4. Za zarządzanie procesami przetwarzania danych osobowych w poszczególnych komórkach organizacyjnych odpowiadają KKO. Do obowiązków KKO należy, w szczególności:

1) zarządzanie zbiorami i zasobami danych osobowych wykorzystywanych w ramach zadań realizowanych przez komórkę organizacyjną;
2) przygotowanie upoważnień osób do dostępu do danych osobowych;
3) występowanie z wnioskiem do KKI o nadanie, modyfikację lub odebranie uprawnień dostępu osób do określonego systemu informatycznego, zgodnie z zakresem upoważnienia osoby do przetwarzania danych osobowych oraz z obowiązującymi w CZSW procedurami;
4) zapoznanie podległych osób ze szczegółowymi zasadami przetwarzania danych osobowych wykorzystywanych w komórce organizacyjnej;
5) nadzorowanie zabezpieczenia wykorzystywanych pomieszczeń, w których przetwarzane są dane osobowe;

6) uzyskanie akceptacji ADO na utworzenie nowego zbioru danych osobowych lub zmiany w przetwarzaniu już istniejącego, w szczególności: zmiana celu przetwarzania, zakresu przetwarzania, usunięcie zbioru lub zasobu;
7) ustalanie, w porozumieniu z ASI i z pełnomocnikiem, zasad tworzenia kopii zapasowych zbiorów i zasobów danych osobowych, przetwarzanych lokalnie na komputerach osób pracujących w podległej komórce organizacyjnej i nadzór nad ich wykonywaniem;
8) realizacja procesu udostępniania danych osobowych odbiorcom danych, o których mowa w art. 7 pkt 6 u.o.d.o oraz rejestrowanie tych czynności w rejestrze udostępnień danych osobowych odbiorcom danych prowadzonym zgodnie ze wzorem określonym w załączniku nr 4 do niniejszego zarządzenia;
9) przygotowanie procesu powierzania innym podmiotom przetwarzania danych osobowych w porozumieniu z pełnomocnikiem.

5. Za zabezpieczenie danych osobowych przetwarzanych w systemach informatycznych CZSW odpowiada KKI, do obowiązków którego w szczególności należy:
1) wdrożenie odpowiednich zabezpieczeń technicznych w systemach informatycznych służących do przetwarzania danych osobowych;
2) nadzór nad zgodnością systemów informatycznych z postanowieniami regulacji wewnętrznych dotyczących przetwarzania danych osobowych;
3) nadzór nad właściwym funkcjonowaniem systemów informatycznych, w których przetwarzane są dane osobowe;
4) nadzór nad rozwiązywaniem sytuacji kryzysowych, pojawiających się w systemach informatycznych;
5) kontrola działań podejmowanych przez ASI w zakresie ochrony danych osobowych.

6. ASI poza zadaniami określonymi w innych regulacjach wewnętrznych:
1) informuje pełnomocnika o nowych aplikacjach, serwerach i innych zmianach systemu informatycznego, istotnych ze względu na przetwarzanie danych osobowych;
2) zgłasza pełnomocnikowi informacje niezbędne do aktualizacji dokumentacji ochrony danych osobowych w zakresie bezpieczeństwa systemów informatycznych;
3) wykonuje inne zadania, zgodnie z procedurami zawartymi w Instrukcji, o której mowa w § 2 ust. 3.

7. W przypadku braku obowiązku powołania ASI dla systemu informatycznego wynikającego z PBI, KKI wyznacza ASI również dla tego systemu.

§ 7.1. Każda osoba przetwarzająca dane osobowe ma obowiązek zachować w tajemnicy przetwarzane dane osobowe i sposób ich zabezpieczenia.

2. Osoba przetwarzająca dane osobowe ma obowiązek zabezpieczenia danych osobowych, a w szczególności:

1) przetwarzać dane osobowe zgodnie z przepisami prawa oraz aktami prawa wewnętrznego CZSW, w szczególności z PBI;
2) stosować się do wskazówek ADO, pełnomocnika, KKO i ASI w zakresie prawidłowego przetwarzania danych osobowych i ich zabezpieczenia;
3) chronić dane osobowe przed osobami nieupoważnionymi do ich przetwarzania;
4) zabezpieczać dane osobowe przetwarzane w formie papierowej, w szczególności:
   a) przed wyjściem z pomieszczenia zabezpieczać dokumenty zawierające dane osobowe umieszczając je w zamykanej na klucz szafie, biurku lub innym przeznaczonym do tego celu bezpiecznym miejscu,
   b) po opuszczeniu pomieszczenia, jeżeli pozostaje ono puste, zamknąć drzwi na klucz,
   c) po zakończeniu pracy na dokumencie zawierającym dane osobowe umieścić go w przeznaczonym do tego bezpiecznym miejscu,
   d) przeznaczone do zniszczenia dokumenty zawierające dane osobowe, niszczyć w sposób uniemożliwiający odczytanie zawartych w nich danych, w szczególności w niszczarkach dokumentów,
   e) pracować na dokumentach zawierających dane osobowe w sposób uniemożliwiający ich nieumyślne zniszczenie, uszkodzenie, zabrudzenie albo zagubienie,
   f) nie wynosić dokumentów zawierających dane osobowe poza obszar przetwarzania danych osobowych CZSW bez zgody ADO lub KKO,
   g) w przypadku wytwarzania lub zbierania danych osobowych poza obszarem przetwarzania danych osobowych, zadbać o ich bezpieczne przetransportowanie do obszaru przetwarzania danych osobowych,
   h) umożliwiać dostęp do dokumentów zawierających dane osobowe jedynie osobom upoważnionym do ich przetwarzania, a w przypadku udostępniania

dokumentów osobom nieupoważnionym postępować zgodnie z zasadami określonymi w § 14;

5) zabezpieczać dane osobowe przetwarzane w systemie informatycznym, a w szczególności:
   a) zachować w tajemnicy hasło dostępu do systemu informatycznego i dokonywać zmiany hasła zgodnie z możliwościami systemu informatycznego i obowiązującymi w CZSW procedurami, nie rzadziej niż raz na 30 dni, chyba, że system informatyczny jest chroniony zabezpieczeniami o wyższym poziomie złożoności niż uwierzytelnianie za pomocą konta i hasła, takimi jak indywidualne karty kryptograficzne,
   b) uniemożliwiać odczytanie danych osobowych zawartych w systemie informatycznym osobom przebywającym w pomieszczeniu i nieupoważnionym do ich przetwarzania poprzez zamykanie dokumentów i aplikacji zawierających dane osobowe lub ustawienie monitora w sposób uniemożliwiający ich odczytanie,
   c) zabezpieczać system informatyczny na czas nieobecności w pomieszczeniu poprzez wyłączenie, zablokowanie komputera lub wylogowanie się z systemu, a po zakończeniu pracy każdorazowe wyłączenie komputera zgodnie z obowiązującymi w CZSW procedurami,
   d) zabezpieczać dane osobowe poprzez odpowiednio częste zapisywanie zmian w aplikacjach i przetwarzanych dokumentach elektronicznych,
   e) w przypadku przetwarzania danych osobowych w formie elektronicznej poza przeznaczonymi do tego celu sieciowymi aplikacjami bazodanowymi, po zakończeniu pracy na pliku z danymi osobowymi, zabezpieczyć go poprzez stworzenie kopii bezpieczeństwa w uzgodniony z KKO sposób,
   f) umożliwiać dostęp do dokumentów elektronicznych zawierających dane osobowe jedynie osobom upoważnionym do ich przetwarzania, a w przypadku udostępniania dokumentów osobom nieupoważnionym postępować zgodnie z zasadami określonymi w § 14,
   g) nie kopiować danych osobowych na nośniki zewnętrzne, bez uprzedniego skonsultowania z KKO zasadności wykonania takiej kopii,
   h) nie tworzyć wydruków z danymi osobowymi bez uzasadnionego celu, a po wykonaniu takiego wydruku, chronić go zgodnie z zabezpieczeniami opisanymi w pkt 4,

i) zabezpieczać nośniki zewnętrzne zawierające dane osobowe przed dostępem osób nieupoważnionych i zniszczeniem poprzez odpowiednie ich przechowywanie w wyznaczonym do tego celu bezpiecznym miejscu, zabezpieczenie nośników hasłem lub ich odpowiednie szyfrowanie,

j) nie wynosić danych osobowych znajdujących się na komputerach przenośnych lub nośnikach zewnętrznych poza obszar przetwarzania danych osobowych, bez zgody ADO lub KKO,

k) zabezpieczać dane osobowe wynoszone poza obszar przetwarzania danych osobowych, znajdujące się na komputerach przenośnych i nośnikach zewnętrznych, przed dostępem osób nieupoważnionych, poprzez stosowanie odpowiednich mechanizmów zabezpieczeń, w szczególności: zabezpieczanie komputerów przenośnych hasłami dostępu na poziomie BIOS i systemu operacyjnego, szyfrowanie i zabezpieczanie hasłem plików z danymi osobowymi; urządzenia przenośne i zewnętrzne nośniki zawierające dane osobowe wynoszone poza obszar przetwarzania nie mogą być pozostawione bez nadzoru osoby odpowiedzialnej za te dane,

l) w przypadku przesyłania danych osobowych za pomocą poczty elektronicznej, umieszczać dane osobowe w plikach chronionych hasłem dostępu, oraz korzystać wyłącznie ze służbowej, szyfrowanej skrzynki pocztowej,

m) przed użyciem w systemie informatycznym zewnętrznego nośnika danych, każdorazowo sprawdzić go programem antywirusowym,

n) nie używać zewnętrznych nośników danych, nie będących nośnikami służbowymi.

3. Osoba, która otrzymała sprzeciw na przetwarzanie danych osobowych od osoby, której dane dotyczą, jest zobowiązana przekazać informację o tym zdarzeniu do KKO i pełnomocnika.

4. W przypadku otrzymania wniosku o dostęp do danych osobowych od osoby, której dane dotyczą, osoba, która otrzymała wniosek jest zobowiązana poinformować o zaistniałej sytuacji KKO.

5. W przypadku otrzymania wniosku o poprawienie danych osobowych od osoby, której dane dotyczą, osoba, która otrzymała wniosek jest zobowiązana poinformować o zaistniałej sytuacji KKO i zgodnie z jego wytycznymi dokonać aktualizacji danych.

6. W przypadku potrzeby stworzenia nowego zbioru lub zasobu danych osobowych lub zmiany istniejącego, każda osoba zainteresowana wykonaniem powyższych czynności jest zobowiązana poinformować o tym pełnomocnika i KKO.

§ 8.1. ADO upoważnia do przetwarzania danych osobowych osoby zatrudnione w CZSW w zakresie niezbędnym do wykonania zadań na zajmowanym stanowisku lub wykonania zleconej pracy. Wzór upoważnienia do przetwarzania danych osobowych określa załącznik nr 5 do niniejszego zarządzenia.

2. ADO może upoważnić inną osobę do nadawania upoważnień do przetwarzania danych osobowych w jego imieniu.

3. KKO przygotowuje upoważnienia do przetwarzania danych osobowych dla podległych funkcjonariuszy i pracowników. Podpisane upoważnienie zostaje przekazane do komórki organizacyjnej CZSW właściwej w sprawach kadrowych w celu merytorycznego sprawdzenia jego poprawności i adekwatności przyznawanego zakresu dostępu, w stosunku do obowiązków służbowych funkcjonariusza SW albo pracownika. Sprawdzone i zaakceptowane upoważnienie zostaje podpisane przez ADO lub osobę przez niego upoważnioną i dołączone do akt osobowych upoważnianego funkcjonariusza lub pracownika.

4. Upoważnienia dla KKO do przetwarzania danych osobowych przygotowuje komórka organizacyjna CZSW właściwa w sprawach kadrowych.

5. Komórka organizacyjna CZSW właściwa w sprawach kadrowych każdorazowo przekazuje do pełnomocnika informację o nadaniu, odebraniu bądź zmianie zakresu upoważnienia do dostępu do danych osobowych.

6. Każda osoba przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostaje przeszkolona z zasad ochrony danych osobowych obowiązujących w CZSW. Za organizację szkoleń z zasad ochrony danych osobowych odpowiedzialny jest pełnomocnik, który jest informowany przez komórkę organizacyjną CZSW właściwą w sprawach kadrowych o potrzebie przeprowadzenia szkolenia.

7. KKO przed dopuszczeniem osoby do pracy przy przetwarzaniu danych osobowych:

1) sprawdza u pełnomocnika czy ta osoba otrzymała stosowne upoważnienie do przetwarzania danych osobowych;
2) zapoznaje tą osobę ze szczegółowymi zasadami przetwarzania i ochrony danych w zbiorach, do których przetwarzania została upoważniona;
3) występuje z wnioskiem do KKI o nadanie lub zmianę uprawnień dostępu do systemu informatycznego, zgodnie z obowiązującymi w CZSW procedurami.

8. ASI informuje pełnomocnika o nadanych, zmodyfikowanych i odebranych uprawnieniach i identyfikatorach informatycznych osób dopuszczonych do przetwarzania danych w systemie informatycznym w CZSW.

9. Upoważnienie do przetwarzania danych osobowych może zostać wycofane przez Dyrektora Generalnego Służby Więziennej lub osobę przez niego upoważnioną w formie pisemnej ze skutkiem natychmiastowym.

10. Upoważnienie wygasa wraz z ustaniem stosunku służbowego, stosunku pracy lub zakończeniem wykonywania prac, określonych umową zlecenia, umową o dzieło, umową o staż lub praktykę. Informacja o wygaśnięciu upoważnienia zostaje zgłoszona pełnomocnikowi przez komórkę organizacyjną CZSW właściwą w sprawach kadrowych.

**§ 9.**1. Dane osobowe w utworzonych zbiorach muszą być zbierane dla oznaczonych, zgodnych z prawem celów i nie mogą być poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

2. Zbierane dane osobowe muszą być merytorycznie poprawne i adekwatne w stosunku do celów, dla których są przetwarzane.

3. Rodzaj i treść danych nie może wykraczać poza potrzeby wynikające z celu ich zbierania.

4. Zabronione jest przetwarzanie danych osobowych, które są nieistotne lub mają większy stopień szczegółowości, niż wynika to z określonego celu przetwarzania.

5. Zabronione jest przetwarzanie danych osobowych, których zakres i cel przetwarzania nie został zatwierdzony przez Dyrektora Generalnego Służby Więziennej lub nie jest zgodny z tym zakresem.

6. Dane osobowe mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Ich dalsze przetwarzanie jest dopuszczalne wyłącznie w przypadku istnienia innych celów przetwarzania.

**§ 10.**1. W przypadku zbierania danych osobowych na formularzach, umowach, kwestionariuszach, drukach, zarówno papierowych, jak i elektronicznych, należy umieszczać na nich klauzulę informacyjną, o której mowa w art. 24 ust. 1 i art. 25 ust. 1 u.o.d.o. Przepisu nie stosuje się w przypadkach określonych w art. 24 ust. 2 i art. 25 ust. 2 u.o.d.o.

2. W przypadku braku innej podstawy prawnej na przetwarzanie danych osobowych w danym celu lub zakresie, należy pod klauzulą informacyjną umieścić klauzulę zgody wraz z odrębnym miejscem na podpis.

3. Klauzule informacyjne oraz klauzule zgody zatwierdza pełnomocnik, na podstawie propozycji przedłożonej przez KKO.

4. KKO sprawuje nadzór nad stosowaniem klauzul informacyjnych w swojej komórce organizacyjnej.

**§ 11.**1. Tworzenie nowych zbiorów danych osobowych lub dokonywanie zmian w zbiorach już istniejących odbywa się za akceptacją ADO i wiedzą pełnomocnika.

2. W przypadku, gdy tworzony zbiór podlega obowiązkowi rejestracji w rejestrze GIODO, pełnomocnik przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji.

3. Pełnomocnik, w porozumieniu z ASI, określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym niezbędne do wypełnienia wniosku zgłoszenia zbioru danych osobowych do rejestracji GIODO. W przypadku stwierdzenia braku wymaganych zabezpieczeń, pełnomocnik występuje z wnioskiem do właściwego KKO o podniesienie poziomu zabezpieczeń.

4. Przygotowany projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, pełnomocnik przekazuje do podpisu Dyrektorowi Generalnemu Służby Więziennej lub osobie przez niego upoważnionej.

5. Wniosek rejestracyjny jest przekazywany do GIODO, zgodnie z trybem wysyłania korespondencji urzędowej.

6. W przypadku dokonania zmiany w zbiorze danych osobowych, która wymaga złożenia wniosku rejestracyjnego do GIODO, pełnomocnik przygotowuje wniosek rejestracyjny w terminie 30 dni od dnia dokonania zmiany w zbiorze.

**§ 12.**1. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź musi nastąpić w terminie do 30 dni od daty jego otrzymania.

2. KKO, który otrzymał wniosek ustala w porozumieniu z pełnomocnikiem treść i zakres informacji, których dotyczy żądanie i sporządza odpowiedź oraz przedkłada do podpisu Dyrektorowi Generalnemu Służby Więziennej lub osobie przez niego upoważnionej.

3. Odpowiedź jest przekazywana osobie listem poleconym za potwierdzeniem odbioru.

**§ 13.**1. W przypadku wniesienia żądania lub sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 7 i 8 u.o.d.o., zwanego dalej „sprzeciwem", informacja o wniesieniu sprzeciwu przekazywana jest niezwłocznie do pełnomocnika, który ocenia zasadność otrzymanego wniosku.

2. W przypadku, gdy sprzeciw zostanie uznany za bezzasadny, pełnomocnik przygotowuje wniosek do GIODO o wydanie stosownej decyzji i przedkłada ADO do podpisu.

3. W przypadku, gdy sprzeciw jest zasadny, pełnomocnik informuje odpowiednich KKO o konieczności zaprzestania przetwarzania danych osobowych wskazanej osoby w określonym celu i zakresie, którzy niezwłocznie usuwają dane tej osoby ze zbiorów danych osobowych.

4. W celu uniknięcia ponownego wykorzystania danych osoby, która złożyła uzasadniony sprzeciw na przetwarzanie jej danych osobowych, KKO mogą pozostawić w zbiorze danych osobowych niezbędne informacje identyfikacyjne tej osoby.

5. Pełnomocnik prowadzi „Rejestr sprzeciwów", zgodnie ze wzorem zawartym w załączniku nr 6 do niniejszego zarządzenia.

**§ 14.**1. Dane osobowe mogą być udostępniane wyłącznie w sytuacjach określonych w art. 24 u.s.w. lub za uprzednią pisemną zgodą osoby, której dane dotyczą.

2. Zgoda na udostępnienie danych osoby, której dane dotyczą jest dobrowolna i potwierdzona podpisem tej osoby pod dokumentem zawierającym klauzulę informacyjną i klauzulę zgody, o których mowa w § 10.

3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

4. Za przygotowanie danych osobowych do udostępnienia w odpowiednim zakresie odpowiedzialny jest KKO.

5. Odpowiedzi na wniosek o udostępnienie danych osobowych udziela Dyrektor Generalny Służby Więziennej lub osoba przez niego upoważniona.

6. Informacje zawierające dane osobowe, przekazywane są uprawnionym podmiotom lub osobom, w sposób gwarantujący ich bezpieczeństwo, w szczególności: listem poleconym, przekazane osobiście, właściwie zabezpieczona wiadomość elektroniczna.

§ **15.**1. Zlecanie podmiotom zewnętrznym jakichkolwiek czynności związanych z przetwarzaniem danych osobowych w imieniu CZSW, jest formą powierzenia przetwarzania danych osobowych.

2. Decyzję o powierzeniu przetwarzania danych osobowych podejmuje Dyrektor Generalny Służby Więziennej, jako ADO, lub osoba przez niego upoważniona do zawierania umów.

3. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 31 u.o.d.o., na podstawie umowy zawartej na piśmie pomiędzy CZSW a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

4. W przypadku zlecenia czynności przetwarzania danych osobowych jednostce organizacyjnej Służby Więziennej, umowę powierzenia przetwarzania zastępuje pismo lub akt prawa wewnętrznego zatwierdzony przez Dyrektora Generalnego Służby Więziennej.

5. KKO przygotowuje projekt umowy, pisma lub aktu, o którym mowa w ust. 4, zamieszczając właściwe zapisy o powierzeniu przetwarzania danych osobowych i przedstawia pełnomocnikowi do akceptacji.

6. W zapisie powierzenia przetwarzania danych osobowych należy wyspecyfikować cel, zakres wykonywanych czynności związanych z przetwarzaniem powierzonych danych, zakres danych oraz wymagania dotyczące ochrony danych.

7. W przypadku powierzenia czynności, które nie polegają na gromadzeniu danych, w zapisach powierzenia przetwarzania danych osobowych nie określa się zakresu powierzonych danych osobowych.

§ **16.**1. Dane osobowe mogą być przetwarzane wyłącznie w systemach informatycznych, które spełniają wymogi u.o.d.o. i przepisy wykonawcze do tej ustawy.

2. Użytkownikami systemu informatycznego mogą być tylko osoby, które zostały upoważnione do przetwarzania tych danych i tylko w zakresie określonym w upoważnieniu.

3. Zasady zarządzania systemem informatycznym określa Instrukcja, o której mowa w § 2 ust. 3.

§ **17.**1. Sposób, częstotliwość tworzenia, przechowywania oraz likwidacji kopii zapasowych baz danych osobowych przetwarzanych w systemie informatycznym określa Instrukcja, o której mowa w § 2 ust. 3.

2. Zasady przechowywania, sposób archiwizowania i likwidacji dokumentów papierowych, określają właściwe przepisy archiwizacyjne. W zakresie nieuregulowanym tymi przepisami, odpowiednie zasady określa KKO po konsultacji z pełnomocnikiem.

**§ 18.**1. Sytuacją naruszenia zasad zabezpieczeń danych osobowych jest wystąpienie zagrożenia bezpieczeństwa danych, a w szczególności nieautoryzowanego dostępu, powielenia, ujawnienia, nieuprawnionej modyfikacji, nieprawidłowego wykorzystania, zniszczenia, utraty lub kradzieży.

2. Osoba, która podejrzewa lub stwierdzi naruszenie bezpieczeństwa danych osobowych postępuje zgodnie z procedurą zarządzania incydentami określoną w PBI.

**§ 19.** Traci moc zarządzenie Nr 17/09 Dyrektora Generalnego Służby Więziennej z dnia 9 lipca 2009 r. w sprawie zabezpieczenia danych osobowych w Centralnym Zarządzie Służby Więziennej i zarządzenie Nr 18/2009 Dyrektora Generalnego Służby Więziennej z dnia 15 lipca 2009 r. w sprawie wyznaczenia w Centralnym Zarządzie Służby Więziennej administratora bezpieczeństwa informacji.

**§ 20.** Zarządzenie wchodzi w życie po upływie 14 dni od dnia podpisania.

CENTRALNY ZARZĄD SŁUŻBY WIĘZIENNEJ

**Dyrektor Generalny**
**Służby Więziennej**

**gen. Jacek Kitliński**

Załączniki do zarządzenia
Dyrektora Generalnego Służby Więziennej
nr ..39...../15 z dnia 3 września 2015 r.

Załącznik nr 1

**Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

§ 1.1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowi wykonanie obowiązku, o którym mowa w § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

2. Zasady określone w niniejszej instrukcji, o ile jest to możliwe, mają zastosowanie również do urządzeń mobilnych.

§ 2.1. Dostęp do systemu informatycznego jest nadawany osobie na wniosek KKO, zgodnie z zakresem jej upoważnienia do przetwarzania danych osobowych i pełnionych obowiązków służbowych.

2. Procedura nadania, modyfikacji lub odebrania uprawnień dostępu do systemu informatycznego przebiega w następujący sposób:

1) KKO występuje z wnioskiem do KKI o nadanie, modyfikację lub odebranie uprawnień dostępu do określonego systemu informatycznego;
2) KKI rozpatruje wniosek i przekazuje go ASI do realizacji;
3) na podstawie zatwierdzonego przez KKI wniosku, ASI odbiera, modyfikuje lub nadaje użytkownikowi minimalne uprawnienia dostępu do systemu informatycznego, niezbędne do realizacji określonych przez KKO zadań; w przypadku uprawniania do dostępu nowego użytkownika, tworzone jest nowe konto użytkownika o odpowiednim identyfikatorze i zabezpieczone hasłem tymczasowym; w przypadku odebrania uprawnień konto użytkownika jest blokowane;

4) ASI przekazuje użytkownikowi informacje o nazwie użytkownika i haśle tymczasowym do założonego nowego konta.

3. Po nadaniu, zmodyfikowaniu bądź odebraniu uprawnień użytkownika systemu informatycznego, ASI informuje pełnomocnika o dokonanych zmianach.

4. ASI odbiera uprawnienia dostępu do systemu informatycznego z pominięciem procedury opisanej w ust. 2 w przypadku:

1) otrzymania polecenia odebrania uprawnień od ADO lub KKI;
2) uzyskania informacji z Biura Kadr i Szkolenia CZSW o zmianie stanowiska pracy osoby, która powoduje zmianę jego zakresu obowiązków i ustanie potrzeby dostępu do określonego systemu informatycznego lub o zakończeniu pracy w CZSW;
3) naruszenia przez osobę zasad użytkowania systemu informatycznego lub zagrożenia bezpieczeństwa informacji; uprawnienie odbiera się do czasu wyjaśnienia nieprawidłowości, informując KKI, pełnomocnika i odpowiedniego KKO.

5. Prace związane z nadawaniem, odbieraniem i modyfikacją uprawnień mogą być wykonywane przez osobę wyznaczoną przez KKI, którą nie jest ASI.

6. Procedury określonej w ust. 2, nie stosuje się w przypadku systemów informatycznych, dla których zasady nadawania, modyfikacji i odbierania uprawnień zostały określone w innych aktach prawa wewnętrznego obowiązującego w CZSW.

**§ 3.**1. Uwierzytelnienie użytkownika w systemie informatycznym następuje za pomocą identyfikatora i hasła.

2. Użytkownik zmienia hasło tymczasowe przy pierwszym logowaniu.

3. Użytkownik wpisuje osobiście hasło uprawniające do korzystania z systemu informatycznego. Hasło nie wyświetla się na ekranie monitora.

4. Użytkownik zobowiązany jest do zachowania hasła w tajemnicy.

5. Każde hasło użytkownika składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

6. Hasła użytkowników muszą być zmieniane nie rzadziej niż co 30 dni.

7. Hasła, w stosunku do których zaistniało podejrzenie o ich ujawnieniu, podlegają bezzwłocznej zmianie.

8. W celu zabezpieczenia awaryjnego dostępu do systemu aktualne hasło administratora systemu informatycznego jest deponowane w sejfie KKI.

9. Zasady określone w ust. 1-6 nie mają zastosowania w przypadku stosowania zabezpieczeń o wyższym poziomie złożoności, takich jak karty kryptograficzne.

§ 4.1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu zasilacza awaryjnego UPS i komputera, a następnie wprowadzeniu identyfikatora indywidualnego oraz hasła identyfikatora znanego tylko użytkownikowi.

2. W przypadku zawieszenia pracy przy stacji roboczej użytkownik ma obowiązek zapisać zmiany wprowadzanych danych i wyłączyć aplikacje oraz zablokować dostęp do systemu operacyjnego, wylogować się lub wyłączyć stację roboczą zgodnie z ust. 3.

3. Zakończenie pracy na stacji roboczej następuje po zapisaniu wprowadzanych danych, a następnie prawidłowym zamknięciu uruchomionych aplikacji oraz wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym UPS.

§ 5.1. W CZSW wykonuje się kopie zapasowe systemów informatycznych, które w przypadku awarii są wykorzystywane do odtworzenia systemu operacyjnego, aplikacji i danych systemu informatycznego.

2. Kopie zapasowe, o których mowa w ust. 1, wykonuje ASI lub inna osoba wyznaczona przez KKI w uzgodniony z KKI i pełnomocnikiem sposób.

3. Kopie zapasowe mogą być wykonywane automatycznie przy wykorzystaniu posiadanych narzędzi i systemów zgodnie z procedurami określonymi w szczegółowych aktach prawa wewnętrznego.

4. Użytkownik ma obowiązek wykonywać kopie zapasowe dokumentów z danymi osobowymi przechowywanych lokalnie na komputerze w uzgodniony z KKO i pełnomocnikiem sposób. Na wniosek KKO kopie te mogą być wykonywane przez KI.

5. Kopie bezpieczeństwa są przechowywane w obszarze przetwarzania danych osobowych, w ustalonym, bezpiecznym miejscu, innym niż miejsce, w którym znajdują się dane produkcyjne. Kopie przechowywane na nośnikach zewnętrznych muszą być zabezpieczone w sposób zapewniający dostęp wyłącznie osób upoważnionych oraz ochronę przed ich uszkodzeniem lub zniszczeniem, w szczególności: w zamykanych szafach lub sejfach.

6. W przypadku przechowywania kopii zapasowych na nośnikach zewnętrznych, nośniki te należy dwa razy do roku sprawdzać pod kątem ich dalszej przydatności.

7. Kopie zapasowe przechowuje się nie dłużej niż dane oryginalne, do czasu osiągnięcia celu ich przetwarzania, chyba, że przepisy rangi ustawowej dopuszczają ich dalsze przetwarzanie.

§ 6.1. Wynoszenie nośników zewnętrznych zawierających dane osobowe poza obszar przetwarzania danych osobowych jest dopuszczalne wyłącznie za zgodą KKO lub ADO.

2. Likwidacja uszkodzonych lub niepotrzebnych nośników zawierających dane osobowe odbywa się przez fizyczne zniszczenie nośnika.

3. Nie używane nośniki informacji mogą być przekazane innemu podmiotowi wyłącznie w sytuacji zapewnienia trwałego usunięcia znajdujących się na nich uprzednio danych.

4. Nośniki i urządzenia zawierające dane osobowe wynoszone poza obszar przetwarzania danych osobowych zabezpiecza się w sposób zapewniający poufność i integralność danych. Sposób zabezpieczenia określa KKO w porozumieniu z KI.

5. Dostęp do nośników, zawierających kopie bezpieczeństwa i kopie archiwalne systemów informatycznych posiadają wyłącznie osoby upoważnione do przetwarzania znajdujących się na nich danych osobowych.

6. Nieuzasadnione kopiowanie danych osobowych na nośniki zewnętrzne jest zabronione.

§ 7.1. W celu minimalizowania możliwości przedostania się szkodliwego oprogramowania do systemu informatycznego:

1) stosuje się zabezpieczenia organizacyjne określone w PBI;
2) każdy komputer wyposaża się w ochronę antywirusową i zaporę firewall;
3) systemy operacyjne komputerów, programy (w szczególności: programy antywirusowe i inne programy nadzorujące bezpieczeństwo) są na bieżąco aktualizowane o wymagane poprawki bezpieczeństwa;
4) komputery przenośne nie są dopuszczone do pracy w lokalnej sieci komputerowej CZSW.

2. W celu ochrony systemu informatycznego przed skutkami szkodliwego działania oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, zakłada się możliwość stosowania następujących zabezpieczeń:

1) stosowanie bezpiecznych konfiguracji komputerów:
   a) wyłączenie nieużywanych usług systemu operacyjnego,
   b) instalowanie aktualnych poprawek bezpieczeństwa,

c) stosowanie indywidualnych identyfikatorów i haseł w celu uwierzytelniania użytkowników, bądź w uzasadnionych przypadkach stosowanie dalej idącej ochrony (w szczególności stosowanie kart kryptograficznych),
d) ograniczenie uprawnień użytkowników do niezbędnego minimum,
e) uaktywnienie logów systemowych w zależności od możliwości systemu operacyjnego;

2) zabezpieczenia sieci informatycznej:
a) stosowanie przełączników (switch),
b) stosowanie podziału na podsieci,
c) stosowanie szyfrowanych kanałów dostępu z sieci zewnętrznych do sieci wewnętrznej,
d) stosowanie firewalli,
e) stosowanie sieciowych systemów wykrywania naruszeń bezpieczeństwa,
f) filtracja połączeń sieciowych;

3) ochrona antywirusowa:
a) stosowanie oprogramowania antywirusowego i antyspamowego na serwerach poczty elektronicznej,
b) stosowanie oprogramowania antywirusowego na serwerach, stacjach roboczych użytkowników w sieci wewnętrznej i komputerach przenośnych,
c) ochrona styku sieci wewnętrznej CZSW z sieciami zewnętrznymi;

4) ochrona przed złośliwym oprogramowaniem:
a) stosowanie oprogramowania antyspyware'owego na serwerach,
b) stosowanie oprogramowania antyspyware'owego na stacjach roboczych i komputerach przenośnych,
c) ochrona styku sieci wewnętrznej CZSW z sieciami zewnętrznymi;

5) zabezpieczenia komputerów przenośnych:
a) stosowanie haseł na BIOS,
b) stosowanie indywidualnych systemów firewall,
c) stosowanie oprogramowania do kryptograficznego zabezpieczenia plików lub dysków z danymi;

6) zabezpieczenia organizacyjne:
a) regulacje wewnętrzne dotyczące korzystania z systemu informatycznego dla użytkowników,

b) dokonywanie przeglądów i weryfikacja zabezpieczeń systemu informatycznego.

3. Sposób ochrony systemu informatycznego przed działaniem oprogramowania, o którym mowa w ust. 1, ustala ASI w porozumieniu z pełnomocnikiem i podlega akceptacji KKI.

**§ 8.**1. ASI na bieżąco monitoruje bezpieczeństwo systemu informatycznego, w tym pojawiające się informacje o nowych zagrożeniach dla systemu informatycznego.

2. W przypadku potrzeby aktualizacji systemu informatycznego, wynikającej z wykrytego zagrożenia, ASI wprowadza lub nadzoruje wprowadzenie koniecznych zmian informując KKI i pełnomocnika.

**§ 9.**1. W każdym systemie informatycznym odnotowuje się:

1) datę pierwszego wprowadzenia danych osobowych;
2) identyfikator użytkownika wprowadzającego dane.

2. W uzasadnionych przypadkach dotyczących przetwarzania danych osobowych odnotowuje się:

1) źródła pochodzenia danych, w przypadku zbierania danych nie od osoby, której one dotyczą;
2) informację o odbiorcach danych oraz o dacie i zakresie udostępnienia danych;
3) sprzeciw wobec dalszego przetwarzania danych osobowych, określony w art. 32 ust. 1 pkt 8 u.o.d.o.

**§ 10.**1. ASI dokonuje okresowego przeglądu i konserwacji systemu informatycznego oraz jego zabezpieczeń i kopii bezpieczeństwa, nie rzadziej niż raz do roku.

2. Procedura wykonania przeglądu systemu informatycznego obejmuje:

1) dokonanie analizy zużycia zasobów systemu informatycznego wraz z kontrolą obciążenia, w szczególności przestrzeni dyskowych, pamięci operacyjnej, ruchu sieciowego;
2) dokonanie analizy poprawności funkcjonowania systemu informatycznego, w szczególności analizy logów systemowych;
3) skontrolowanie logów aplikacji oraz poprawności wykorzystania zasobów przez użytkowników, w szczególności odpowiedniego wykorzystania przestrzeni dysków sieciowych i aplikacji;

4) weryfikację zabezpieczeń systemu informatycznego;

5) zainstalowanie brakujących poprawek bezpieczeństwa systemu operacyjnego i aplikacji.

3. Po zakończeniu przeglądu systemu informatycznego i przeglądu jego zabezpieczeń ASI składa sprawozdanie KKI.

4. W przypadku wystąpienia nieprawidłowości bądź stwierdzenia istotnych zagrożeń, ASI składa KKI sprawozdanie z dokonanego przeglądu w formie pisemnej, wskazując stwierdzone problemy. Kopia sprawozdania jest przekazywana do pełnomocnika.

5. Przegląd nośników informacji zawierających kopie bezpieczeństwa danych jest prowadzony doraźnie przez ASI, lub osobę je przechowującą.

6. Przeglądy i konserwacje systemów informatycznych mogą być prowadzone przez osobę wyznaczoną przez KKI nie będącą ASI.

7. Przeglądy określone w ust. 1 mogą być prowadzone w ramach przeglądów bezpieczeństwa określonych w PBI.

**§ 11.**1. Przeglądów, napraw i konserwacji systemu bądź jego poszczególnych elementów składowych dokonuje się zgodnie z zaleceniami producenta urządzeń. Przeglądy mogą być wykonywane przez firmę zewnętrzną.

2. Z firmą wykonującą prace określone w ust. 1, podpisuje się umowę powierzenia przetwarzania danych osobowych.

3. Pracownicy podmiotów zewnętrznych mający dostęp do systemu informatycznego bądź jego składowych elementów, podpisują oświadczenie o zachowaniu w tajemnicy informacji pozyskanych w trakcie wykonywania prac i sposobów zabezpieczeń stosowanych w CZSW.

4. Przed udzieleniem dostępu serwisantom, ASI wykonuje lub nadzoruje wykonanie kopii bezpieczeństwa danych osobowych lub kopii bezpieczeństwa systemu informatycznego, z wyłączeniem sytuacji, w której powstałe uszkodzenie w systemie informatycznym uniemożliwia wykonanie takiej kopii.

5. Prace serwisantów odbywają się pod nadzorem ASI lub osoby przez niego upoważnionej.

6. W przypadku przekazania elektronicznych nośników informacji do naprawy bez nadzoru ASI lub osoby przez niego upoważnionej, ASI pozbawia je zapisu danych osobowych w sposób uniemożliwiający ich odzyskanie lub nadzoruje ten proces.

Załącznik nr 2

Wzór wykazu zbiorów danych osobowych

| L.p. | Nazwa zbioru | System informatyczny w którym przetwarzane są dane | Opis struktury zbioru wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi | Sposób przepływu danych pomiędzy poszczególnymi zbiorami i systemami informatycznymi |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |
| 4. | | | | |
| 5. | | | | |
| 6. | | | | |

Załącznik nr 3

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

| Lp. | Imię i nazwisko | Stanowisko/ komórka organizacyjna | Data nadania upoważnienia | Data ustania upoważnienia | Zakres upoważnienia | Identyfikator w danym systemie informatycznym |
|---|---|---|---|---|---|---|
| 1. | | | | | | |
| 2. | | | | | | |
| 3. | | | | | | |
| 4. | | | | | | |
| 5. | | | | | | |
| 6. | | | | | | |

Załącznik nr 4

Wzór Rejestru udostępnień danych osobowych odbiorcom danych

| Imię i nazwisko udostępniającego | Data udostępnienia | Nazwa podmiotu, któremu udostępniono dane | Cel udostępnienia (podstawa prawna) | Zakres udostępnionych danych | Nazwa zbioru |
|---|---|---|---|---|---|
| | | | | | |

Załącznik nr 5

Wzór upoważnienia do przetwarzania danych osobowych

**Data nadania upoważnienia:** .....

**Upoważnienie do przetwarzania danych osobowych**

**Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662) upoważniam Pana/Panią:**

.....

*(imię i nazwisko upoważnianego)*

**zatrudnioną/-ego na stanowisku:**

.....

*(nazwa jednostki i komórki organizacyjnej)*

**do dostępu do danych osobowych:**

1) .....
2) .....
3) .....

*(należy sprecyzować zakres upoważnienia; można go określić poprzez wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba lub rodzaj czynności lub operacji, jakich może ona dokonywać na danych osobowych)*

**Okres trwania upoważnienia:**.....

*(należy sprecyzować okres obowiązywania upoważnienia, np. od dnia wystawienia do chwili ustania stosunku pracy)*

**Wystawił:** .....

*(podpis administratora danych*

*osobowych lub osoby reprezentującej)*

**Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy**, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

**Data i podpis osoby upoważnionej:** .....

Załącznik nr 6

Wzór rejestru sprzeciwów

| Informacje o osobie, której sprzeciw dotyczy | Data otrzymania sprzeciwu | Przedmiot sprzeciwu | Zbiór danych, którego sprzeciw dotyczy | Podjęte działania |
|---|---|---|---|---|
| | | | | |