Polityka bezpieczeństwa

Spis treści

1. Wstęp

Kontakt:

- za pomocą e-mail: **szpitalpck@bialystok.home.pl**
- telefonicznie pod numerem: **85-66-48-519**

Kontakt z Inspektorem Ochrony Danych Osobowych:

- **Krzysztof Stasiak**
- za pomocą e-mail: **iod@szpitalpck.pl**
- telefonicznie pod numerem: **730 946 566**

1.1 Słowniczek

Administrator danych / Administrator / ADO – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielne lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

W rozumieniu Polityki bezpieczeństwa w Samodzielnym Szpitalu Miejskim im. PCK w Białymstoku,

ul. Sienkiewicza 79, 15-003 Białystok

Administrator systemów informatycznych / ASI – osoba fizyczna lub prawna, wspierająca ADO w zapewnieniu zgodności działania infrastruktury informatycznej z zasadami ochrony danych osobowych,

Inspektor ochrony danych / IOD *– osoba fizyczna, wspierająca ADO w realizacji obowiązków,* wynikających z Przepisów,

Kontakt z Inspektorem Ochrony Danych Osobowych:

- Krzysztof Stasiak
- za pomocą e-mail**: iod@szpitalpck.pl**
- telefonicznie pod numerem: **730 946 566**

obszar przetwarzania danych osobowych – teren, na którym ADO dokonuje przetwarzania danych osobowych w formie papierowej lub elektronicznej,

organ nadzorczy – podmiot odpowiedzialny za nadzór nad przestrzeganiem przepisów RODO. W Polsce jest nim Prezes UODO,

podmiot przetwarzający / procesor - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu i na rzecz administratora danych,

Polityka bezpieczeństwa – ten dokument,

Prezes Urzędu Ochrony Danych Osobowych / Prezes UODO – organ właściwy do spraw ochrony danych osobowych w Polsce; organ nadzorczy w rozumieniu RODO,

Przepisy – przepisy polskie i unijne, dotyczące ochrony danych osobowych i bezpieczeństwa informacji, w szczególności RODO i Ustawa,

RODO - rozporządzenie 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 uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

Ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

1.2 Polityka bezpieczeństwa i cel jej stosowania

1. Polityka bezpieczeństwa:
    1) jest polityką ochrony danych w rozumieniu art. 24 ust. 2 RODO,
    2) została opracowana z uwzględnieniem Przepisów, wytycznych Prezesa UODO oraz dobrych praktyk, wytycznych lub standardów branży, którą reprezentuje ADO,
    3) służy zapewnieniu takiego poziomu bezpieczeństwa przetwarzanych przez ADO danych osobowych, których uchroni je przed dostępem osób nieupoważnionych lub nieuprawnionymi operacjami na danych bądź zmniejszy ryzyko takich działań,
    4) jest poddawana okresowym przeglądom; w razie potrzeby ADO aktualizuje jej treść, uwzględniając aktualne Przepisy, stan wiedzy technicznej oraz swoje możliwości logistyczne, kadrowe i finansowe,
    5) jest dokumentem wewnętrznym ADO; jej treść może być udostępniana jedynie osobom lub podmiotom uprawnionym.
2. Integralną część Polityki bezpieczeństwa stanowią załączniki, wymienione na końcu dokumentu. ADO może ponadto wprowadzać lub dopuszczać do stosowania dodatkowe wytyczne, regulaminy lub instrukcje, mające na celu realizację zasad ochrony danych osobowych, wskazanych w Polityce bezpieczeństwa lub przepisach.

1.3 Podstawowe zasady ochrony danych osobowych

1. ADO zapewnia realizację następujących zasad wykorzystania danych osobowych:
    1) zgodność z prawem, rzetelność i przejrzystość,
    2) ograniczenie celu,
    3) minimalizacja danych,
    4) prawidłowość,
    5) ograniczenie przechowywania,
    6) integralność i poufność,

- w rozumieniu przepisów o ochronie danych osobowych.

2. ADO wykazuje przestrzeganie zasad ochrony danych osobowych w szczególności poprzez:
    1) Politykę bezpieczeństwa,
    2) dodatkowe wytyczne, regulaminy i instrukcje,
    3) papierowe lub elektroniczne wykazy, ewidencje, notatki służbowe lub korespondencję.

2. Podmioty zaangażowane w ochronę danych osobowych i ich obowiązki

2.1 ADO

1. ADO:
    1) decyduje o celach i środkach przetwarzania danych osobowych,
    2) podejmuje działania, mające na celu zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych i zapewnienie przestrzegania zasad ochrony danych osobowych,

3) prowadzi rejestr czynności przetwarzania, zgodnie z art. 30 ust. 1 RODO; wzór rejestru stanowi załącznik nr 9 do Polityki bezpieczeństwa,
4) dokonuje analizy ryzyka czynności przetwarzania danych osobowych (zgodnie z art. 32 ust. 2 RODO) oraz oceny skutków w zakresie i na warunkach opisanych w art. 35 ust. 1 RODO; analiza ryzyka i ocena skutków są dokonywane zgodnie z procedurą, stanowiącą **załącznik nr 1 do Polityki bezpieczeństwa**,
5) wyznacza IOD

2. Działania ADO, o których mowa w ust. 1 p. 2 powyżej, obejmują w szczególności:
   1) wdrażanie odpowiednich rozwiązań organizacyjnych, informatycznych i fizycznych (opisanych w **rozdziale 5 poniżej** oraz w **załącznikach do Polityki bezpieczeństwa**),
   2) nadawanie upoważnień osobom, które w celach służbowych potrzebują dostępu do danych osobowych,
   3) zapewnianie, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy, dotyczące ochrony danych osobowych.

2.2 IOD

1. Do zadań IOD należy wspieranie ADO oraz innych osób i podmiotów zaangażowanych w przetwarzanie danych osobowych, w szczególności poprzez:
   1) informowanie o obowiązkach związanych z przetwarzaniem danych osobowych i doradzanie w tych sprawach,
   2) monitorowanie przestrzegania Przepisów oraz polityk w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu i związanych z tym audytów,
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
   4) współpraca z organem nadzorczym,
   5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz – w stosownych przypadkach – prowadzenie konsultacji we wszystkich innych sprawach,
   6) wspieranie ADO w realizacji obowiązków wskazanych w Polityce bezpieczeństwa oraz innych dokumentach, wskazanych w **rozdziale 1.3 powyżej**.
2. Szczegółowe zasady funkcjonowania IOD w strukturach ADO opisuje **załącznik nr 16 do Polityki bezpieczeństwa**.

2.3 ASI

1. ADO wyznacza na ASI osobę współpracującą z ADO lub powierza zadania ASI podmiotowi zewnętrznemu.
2. Do zadań ASI należy zapewnienie przestrzegania zasad ochrony danych osobowych, przetwarzanych za pomocą aplikacji, programów, systemów lub sprzętów wykorzystywanych przez ADO, w szczególności przez realizację zasad i działań wskazanych w **załączniku nr 11 do Polityki bezpieczeństwa**.
3. ASI podlega bezpośrednio najwyższemu kierownictwu ADO.
4. Jeżeli ADO nie wyznaczył ASI, za realizację obowiązków wskazanych w ust. 2 powyżej odpowiada ADO lub osoba wskazana przez ADO. Wprowadzone u ADO uregulowania, odnoszące się do ASI, stosuje się wówczas odpowiednio do ADO lub osoby wskazanej przez ADO.

2.4 Osoby upoważnione do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych dopuszczone są jedynie osoby upoważnione przez ADO.
2. Upoważnienie do przetwarzania danych osobowych jest nadawane zgodnie ze wzorem, stanowiącym **załącznik nr 13 do Polityki bezpieczeństwa** oraz procedurą, stanowiącą **załącznik nr 12 do Polityki bezpieczeństwa**. ADO może dopuścić – po konsultacji z IOD – nadawanie upoważnienia w inny sposób, np. przez zawarcie treści upoważnienia w treści umowy, będącej podstawą współpracy z daną osobą.
3. Po nadaniu upoważnienia do przetwarzania danych osobowych osoba, która je otrzymała:
    1) otrzymuje dostęp do aplikacji, sprzętów, dokumentów lub informacji niezbędnych do wykonywania jej obowiązków służbowych, w zakresie wynikających z zajmowanego stanowiska, zakresu obowiązków lub decyzji przełożonego,
    2) jest zobowiązana do przestrzegania Polityki bezpieczeństwa oraz innych dokumentów, o których mowa w rozdziale 1.3 powyżej,
    3) jest zobowiązana do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia zarówno w toku współpracy z ADO, jak i po jej zakończeniu.
4. Naruszenie przez osobę upoważnioną obowiązków, o których mowa w ust. 3 p. 2-3 powyżej może powodować dla takiej osoby konsekwencje dyscyplinarne lub karne.
5. Po zakończeniu współpracy z ADO:
    1) upoważnienie do przetwarzania danych osobowych automatycznie wygasa,
    2) dostęp osoby upoważnionej do aplikacji, sprzętów, dokumentów lub informacji jest odbierany lub blokowany.

2.5 Osoby przebywające w obszarze przetwarzania danych osobowych

1. Osoby współpracujące z ADO, które w związku z realizacją obowiązków służbowych przebywają na obszarze przetwarzania danych osobowych, ale do obowiązków, których nie należy przetwarzanie danych osobowych, podpisują oświadczenie o poufności, którego wzór stanowi załącznik nr 4 do Polityki bezpieczeństwa.
2. Osoby, o których mowa w ust. 1 powyżej:
    1) w przypadku wejścia w posiadanie danych osobowych lub informacji o sposobach ich zabezpieczeń, są zobowiązane do zachowania ich w tajemnicy, zarówno w toku współpracy z ADO, jak i po jej zakończeniu,
    2) w razie powzięcia informacji o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych, są zobowiązane do zawiadomienia o tym IOD lub bezpośredniego przełożonego.
3. Jeżeli osoby, o których mowa w ust. 1 powyżej, realizują swoje obowiązki w imieniu i na rzecz kontrahenta, którego łączy z ADO współpraca w zakresie świadczenia usług, obowiązek wskazany w ust. 1 powyżej może być zastąpiony odpowiednim zobowiązaniem umownym lub innym rozwiązaniem, zaakceptowanym przez IOD.
4. Pozostałe osoby, przebywające w obszarze przetwarzania danych osobowych (np. goście, interesanci, kurierzy itd.) powinny poruszać się po obszarze przetwarzania danych osobowych wyłącznie w towarzystwie osoby upoważnionej do przetwarzania danych osobowych.

3. Zasady przetwarzania danych osobowych

1. Przetwarzanie danych osobowych przez ADO jest dopuszczalne w razie istnienia przynajmniej jednej z podstaw, wskazanych w
2. W zakresie przetwarzania danych ADO wykorzystuje wzory zgód, oświadczeń itp. treści oraz procedury, zatwierdzone do stosowania przez IOD.

3. W razie wątpliwości, dotyczących podstaw prawnych przetwarzania danych osobowych, ADO dokonuje konsultacji z IOD. Jeżeli:
4. Wobec osób, których dane osobowe przetwarza ADO, realizowany jest – zgodnie z art. 13-14 RODO – obowiązek informacyjny. W tym zakresie ADO wykorzystuje wzory obowiązków oraz związane z nimi procedury, zatwierdzone do stosowania przez IOD.
5. ADO przyjmuje wnioski związane z prawami osób, których dane dotyczą, opisane w art. 15-22 RODO, na zasadach opisanych w **załączniku nr 8 do Polityki bezpieczeństwa**.
6. Udostępnianie informacji lub dokumentacji medycznej odbywa się zgodnie z procedurą, stanowiącą **załącznik nr 17 do Polityki bezpieczeństwa**.
7. Weryfikacja tożsamości pacjentów i innych osób odbywa się zgodnie z procedurą, stanowiącą **załącznik nr 18 do Polityki bezpieczeństwa**.

4. Przekazywanie danych osobowych w ramach współpracy z podmiotami zewnętrznymi

W sytuacji, w której:

1) ADO przetwarza dane osobowe w imieniu i na rzecz podmiotu zewnętrznego – ADO stosuje wytyczne z **rozdziału 4.1.1 poniżej**,
2) podmiot zewnętrzny przetwarza dane osobowe w imieniu i na rzecz ADO – ADO stosuje wytyczne z **rozdziału 4.1.2 poniżej**,
3) ADO przekazuje dane osobowe podmiotowi zewnętrznemu, gdzie każda ze stron realizuje własne cele wykorzystania danych osobowych - ADO stosuje wytyczne z **rozdziału 4.2poniżej**,
4) podmiot zewnętrzny przekazuje dane osobowe ADO, gdzie każda ze stron realizuje własne cele wykorzystania danych osobowych - ADO stosuje wytyczne z **rozdziału 4.2poniżej**,
5) ADO wspólnie z podmiotem zewnętrznym lub podmiotami zewnętrznymi wspólnie decydują o celach wykorzystania danych osobowych - ADO stosuje wytyczne z **rozdziału 4.3poniżej**.

4.1 Powierzenie

4.1.1 ADO jako administrator danych

W sytuacji, gdy ADO powierza przetwarzanie danych osobowych podmiotowi zewnętrznemu jako procesorowi, stosuje się następujące wytyczne:

1) przed rozpoczęciem współpracy ADO weryfikuje, czy podmiot zewnętrzny zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Weryfikacja może nastąpić w szczególności poprzez zobowiązanie podmiotu zewnętrznego do wypełnienia **ankiety, stanowiącej załącznik nr 5 do Polityki bezpieczeństwa**,
2) powierzenie przetwarzania danych osobowych następuje w drodze podpisania umowy powierzenia, aneksu do umowy głównej lub dodania odpowiedniej treści fragmentu do umowy głównej. **Wzór umowy powierzenia stanowi załącznik nr 6 do Polityki bezpieczeństwa** (w porozumieniu z IOD możliwe jest wykorzystanie innego wzoru umowy powierzenia, w szczególności przekazanego przez drugą stronę umowy).

4.1.2 ADO jako procesor

W sytuacji, gdy podmiot zewnętrzny powierza przetwarzanie danych osobowych ADO jako podmiotowi przetwarzającemu, stosuje się następujące wytyczne:

1) powierzenie przetwarzania danych osobowych następuje w drodze podpisania umowy powierzenia, aneksu do umowy głównej lub dodania odpowiedniej treści fragmentu do

umowy głównej. Wzór umowy powierzenia stanowi **załącznik nr 6** do Polityki bezpieczeństwa (w porozumieniu z IOD możliwe jest wykorzystanie innego wzoru umowy powierzenia, w szczególności przekazanego przez drugą stronę umowy),

2) ADO umieszcza informację o fakcie powierzenia przetwarzania w rejestrze kategorii czynności przetwarzania. Wzór rejestru stanowi **załącznik nr 10 do Polityki bezpieczeństwa**.

4.2 Udostępnienie

W sytuacji, w której ADO lub podmiot zewnętrzny udostępniają sobie dane osobowe, udostępnienie danych osobowych wymaga podpisania umowy udostępnienia, aneksu do umowy głównej lub dodania odpowiedniej treści fragmentu do umowy głównej. Treść umowy oraz inne obowiązki ADO związane z udostępnieniem są wcześniej konsultowane przez ADO z IOD.

4.3 Współadministracja

W sytuacji, gdy ADO staje się współadministratorem danych osobowych, określenie zasad wykorzystania danych osobowych wymaga zawarcia umowy o współadministrowaniu, aneksu do umowy głównej lub dodania odpowiedniej treści fragmentu do umowy głównej. Treść umowy oraz inne obowiązki ADO związane ze współadministrowaniem są wcześniej konsultowane przez ADO z IOD.

5. Środki stosowane w celu zapewnienia bezpieczeństwa danych osobowych

5.1 Organizacyjne

ADO stosuje w szczególności następujące środki organizacyjne:

1) wdrożenie i stosowanie Polityki bezpieczeństwa,
2) wdrożenie i stosowanie innych wytycznych, regulaminów i instrukcji, mających na celu realizację zasad ochrony danych osobowych i bezpieczeństwa informacji,
3) zobowiązanie osób zatrudnionych do zachowania w tajemnicy zarówno danych osobowych, jak i sposobów ich zabezpieczenia.
4) zapewnienie kontroli nad działaniem osób upoważnionych do przetwarzania danych osobowych i osób przebywających w obszarze przetwarzania danych osobowych,
5) zapewnienie kontroli nad działaniami osób postronnych, tymczasowo przebywających w obszarze przetwarzania danych osobowych.

5.2 Fizyczne

1. ADO stosuje w szczególności następujące zabezpieczenia fizyczne:
    1) możliwość zamykania pomieszczeń, w których przetwarzane są dane osobowe,
    2) zapewnienie osobom zatrudnionym dostępu do szafek, szuflad lub szaf zamykanych na klucz,
    3) dostęp do niszczarek dokumentów papierowych.
2. W przypadku niszczenia przez ADO większej liczby papierowych lub elektronicznych nośników potwierdzeniem dokonania zniszczenia zgodnie z procedurami bezpieczeństwa jest protokół, którego wzór stanowi **załącznik nr 14 do Polityki bezpieczeństwa**.
3. Bardziej szczegółowe informacje na temat stosowanych u ADO zabezpieczeń fizycznych znajdują się w **załączniku nr 15 do Polityki bezpieczeństwa**.

5.3 Informatyczne

1. ADO stosuje w szczególności następujące rozwiązania informatyczne:

1) uwierzytelnianie osób pracujących w aplikacjach, programach lub systemach informatycznych (w szczególności z wykorzystaniem loginów i haseł),
2) aplikacje, programy lub systemy chroniące przed złośliwym oprogramowaniem,
3) środki gwarantujące ciągłą pracę systemów informatycznych,
4) środki gwarantujące możliwość odtworzenia danych w razie wystąpienia zdarzenia niepożądanego,

2. Bardziej szczegółowe informacje na temat stosowanych u ADO rozwiązań informatycznych znajdują się w **załączniku nr 11 do Polityki bezpieczeństwa**.

6. Naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych jest odpowiedzialna za ich bezpieczeństwo.
2. Każda osoba współpracująca z ADO, podejrzewająca lub stwierdzająca naruszenie ochrony danych osobowych, zobowiązana jest do niezwłocznego zgłoszenia takiego naruszenia. Zgłoszenia dokonuje się na formularzu, którego wzór stanowi **załącznik nr 2 do Polityki bezpieczeństwa** lub w inny, uzgodniony z IOD sposób.
3. Zasady postępowania w przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych opisuje **załącznik nr 3 do Polityki bezpieczeństwa**.

7. Postanowienia końcowe

1. Polityka bezpieczeństwa obowiązuje od dnia jej wprowadzenia w sposób przyjęty u ADO. Wszelkie zmiany Polityki bezpieczeństwa obowiązują od dnia ich wprowadzenia w sposób przyjęty u ADO.
2. Z dniem wprowadzenia Polityki bezpieczeństwa traci ważność wcześniej obowiązująca u ADO dokumentacja ochrony danych osobowych.
3. W sprawach nieuregulowanych w Polityce bezpieczeństwa mają zastosowanie Przepisy.

8. Załączniki

Załączniki dostępne w dokumentacji wewnętrznej Samodzielnego Szpitala Miejskiego im. PCK w Białymstoku, ul. Sienkiewicza 79, 15-003 Białystok.