Załącznik nr 1
do Zarządzenia nr 12/2019
Dyrektora Ośrodka Leczenia Uzależnień
SP ZOZ w Lublinie
z dnia 27.12.2019
w sprawie organizacji
systemu bezpieczeństwa informacji

POLITYKA BEZPIECZEŃSTWA

OŚRODEK LECZENIA UZALEŻNIEŃ SP ZOZ W LUBLINIE

UL. M. KARŁOWICZA 1, 20-027 LUBLIN

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH - ZAGADNIENIA OGÓLNE

Polityka Bezpieczeństwa przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie określa zbiór zasad bezpieczeństwa regulujących sposób zarządzania danymi, ich ochroną i wymianą wewnątrz Ośrodka jak i na zewnątrz w kontaktach z instytucjami państwowymi oraz indywidualnymi pacjentami i pracownikami.

Dokument ten został opracowany na podstawie § 3 pkt. 1 i § 4 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) w związku z realizacją obowiązków ciążących na administratorze danych wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

ROZDZIAŁ I

DOKUMENTACJA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Na pełną dokumentację bezpieczeństwa danych osobowych składają się następujące dokumenty:

1. Polityka bezpieczeństwa zawierająca:

1. opis struktury organizacyjnej odpowiedzialnej za bezpieczeństwo danych osobowych,
2. wykaz budynków i pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
3. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
4. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi,
5. sposób przepływu danych pomiędzy poszczególnymi systemami,
6. określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,

7. zasady powierzania przetwarzania danych osobowych oraz sposoby spełnienia obowiązku informacyjnego,
8. zasady prowadzenia audytów wewnętrznych – sprawdzeń systemu bezpieczeństwa,
9. określenie incydentów mających wpływ na bezpieczeństwo danych osobowych oraz postępowanie w sytuacji naruszenia ochrony danych osobowych,

2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zawierająca:

1. określenie kompetencji, obowiązków i zakresu odpowiedzialności osób przetwarzających dane osobowe w systemach informatycznych i w sposób tradycyjny – w dokumentach papierowych oraz osób odpowiedzialnych za bezpieczeństwo danych osobowych,
2. procedury postępowania podczas przebywania i pracy w obszarach przetwarzania danych osobowych oraz stosowanie mechanizmów ochrony fizycznej,
3. procedury dostępu do systemów informatycznych służących do przetwarzania danych osobowych,
4. procedury nadawania i cofania uprawnień użytkownikom,
5. procedury stosowane podczas przetwarzania danych osobowych w systemach informatycznych w tym ochrona kryptograficzna,
6. procedury udostępniania i przesyłania danych osobowych,
7. procedury tworzenia kopii bezpieczeństwa i postępowania z dokumentacją tradycyjną (papierową),
8. procedury zarządzania infrastrukturą teleinformatyczną oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego w tym zapewnienie ciągłości działania,
9. procedury postępowania w sytuacji wystąpienia incydentu ochrony danych i naruszenia ochrony danych osobowych,
10. procedury postępowania przy powierzaniu przetwarzania danych osobowych i wypełnianie obowiązku informacyjnego.

3. Dokument szacowania ryzyka i oceny skutków zawierający:

1. określenie kontekstu definiującego elementy związane ze środowiskiem prawnym, geograficznym, politycznym oraz społecznym funkcjonowania Ośrodka i przetwarzania danych osobowych,
2. inwentaryzację aktywów Ośrodka. Przez „aktywa" należy przez rozumieć wszystko to, co ma wartość dla Ośrodka jako administratora danych osobowych przetwarzanych w Ośrodku. **Aktywa podstawowe** to procesy, działania biznesowe oraz informacje związane z funkcjonowaniem Ośrodka (w tym dane osobowe i inne informacje prawnie chronione). **Aktywa wspierające –** są to środki umożliwiające korzystanie z aktywów podstawowych jak sprzęt, oprogramowanie, sieć, pracownicy, infrastruktura
3. identyfikację zasobów oraz inwentaryzację elementów środowiska związanego z przetwarzaniem danych osobowych,
4. opisanie procesów oraz wykazy osób biorących udział w procesie przetwarzania, źródła pozyskiwania danych (zewnętrzne i wewnętrzne), kategorie osób i podmiotów od których dane są pozyskiwane, systemy IT służące do przetwarzania danych, monitoring wizyjny, środki elektronicznej transmisji danych, wykaz zbiorów papierowych, budynków, pomieszczeń, przypadki powierzania lub przekazywania danych wewnątrz lub na zewnątrz Ośrodka,
5. identyfikację zagrożeń dla naruszenia praw do wolności i prywatności osób oraz dla ryzyk związanych z poufnością, integralnością oraz dostępnością przetwarzanych danych niezależnie od tego czy przetwarzane są w postaci elektronicznej, papierowe czy przekazywane ustnie – zgodnie z normą PN-EN ISO/IEC 27001,
6. ocenę poziomu ryzyka,
7. postępowanie z ryzykiem.

4. Rejestr czynności i rejestr kategorii przetwarzania danych osobowych zawierający:

1. dane kontaktowe administratora i inspektora ochrony danych,
2. cele przetwarzania,
3. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
4. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym

odbiorców w państwach trzecich lub w organizacjach międzynarodowych,

5. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń,

6. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

7. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

ROZDZIAŁ II

WPROWADZENIE

§ 1

Cel polityki bezpieczeństwa

Administrator danych administruje danymi osobowymi w rozumieniu przepisów Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (D. U. z 2018, poz. 1000) oraz Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/2017 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), realizując czynności w sprawach z zakresu ochrony danych osobowych oraz nadzorując również ich wykonywanie.

Dane osobowe zgodnie z art. 4 pkt 1 RODO oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, 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.

Administrator danych osobowych biorąc pod uwagę wagę problemów związanych z ochroną danych osób fizycznych powierzających im swoje dane osobowe do właściwej i skutecznej ochrony, deklarują doskonalić i rozwijać nowoczesne metody przetwarzania danych. Ponieważ poprzez „przetwarzanie danych” rozumie się operację lub zestaw operacji na danych lub

zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie - celem niniejszej Polityki bezpieczeństwa jest wskazanie działań i określenie zasad przetwarzania danych osobowych oraz ich bezpieczeństwa poprzez ustalenie praw, reguł, procedur i praktycznych doświadczeń regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz struktury Administratora danych, jak i w kontaktach z otoczeniem.

Polityka bezpieczeństwa reguluje ogólne zasady przetwarzania określone w art. 5 RODO w zakresie:

a) zapewnienia, aby dane przetwarzane były zgodnie z prawem – art. 6 – 11 RODO,

b) zapewnienia, aby przestrzegane były prawa osób, których dane są przetwarzane – art. 12-23 RODO,

c) zapewnienia wypełniania ogólnych obowiązków w zakresie przetwarzania danych ciążących na administratorze i podmiocie przetwarzającym – art. 24 – 31 RODO,

d) zapewnienia bezpieczeństwa przetwarzania danych uwzględniając charakter zakres, kontekst i cele przetwarzania danych – art. 32- 36 RODO,

e) zapewnienia kontroli nad przetwarzaniem danych w postaci monitorowanie przestrzegania przepisów i przyjętych procedur przetwarzania przez Inspektora Ochrony Danych lub podmioty certyfikujące, czy monitorujące przestrzeganie przyjętych kodeksów postępowania – art. 27- 43,

f) stosowania się do wymagań w zakresie przekazywania danych do państw trzecich i instytucji międzynarodowych – art. 44 – 49 RODO.

Należy zaznaczyć, że zgodnie z art. 24 oraz art. 32 RODO przy wykonywaniu wyżej wymienionych obowiązków w zakresie zapewniania zgodności, uwzględnia się stan wiedzy technicznej, koszty, charakter, zakres, kontekst, cele przetwarzania a także ryzyka na jakie są narażone przetwarzane dane.

§ 2

Definicje

Administrator danych osobowych - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,

Podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

Osoba, której dane dotyczą - osoba fizyczna, możliwa do zidentyfikowania na podstawie określonych danych osobowych;

Dane osobowe: „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, 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;

Dane wrażliwe - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne lub dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej.

ROZDZIAŁ III

ZAKRES DANYCH, PRZETWARZANIE DANYCH

§ 1

Zakres danych osobowych

Polityką bezpieczeństwa objęte są dane osobowe, którymi zgodnie z Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz RODO są wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfika-

cyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Wśród informacji o osobie zwanych „danymi osobowymi" wyróżnia się ich szczególną kategorię - „wrażliwe dane osobowe":

a) ujawniające pochodzenie rasowe lub etniczne,

b) ujawniające poglądy polityczne,

c) ujawniające przekonania religijne lub światopoglądowe,

d) ujawniające przynależność do związków zawodowych,

e) genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,

f) dotyczące zdrowia lub seksualności i orientacji seksualnej tej osoby.

§ 2

Pojęcie przetwarzania danych osobowych

Czynność przetwarzania danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany, a w szczególności:

a) zbieranie danych – uzyskiwanie ich w jakikolwiek sposób, bez względu na to, czy ostatecznie zostaną one zapisane czy usunięte,

b) utrwalanie danych – zapisanie ich na jakimkolwiek materialnym nośniku,

c) organizowanie danych – łączenie i dopasowywanie danych,

d) porządkowanie danych – układanie nośników danych według określonego kryterium,

e) przechowywanie danych – sam akt posiadania i przechowywania danych, choćby bez dostępu do ich treści, stanowi jedną z form przetwarzania danych. Dotyczy to nawet sytuacji, w której podmiot przechowujący dane nie będzie miał w danym momencie środków technicznych do zapoznania się z ich treścią. Więc np. w sytuacji,

w której przechowywane są dane zaszyfrowane, zaś podmiot przechowujący nie będzie miał możliwości ich odczytania, wciąż będzie on przetwarzał dane,

f) adaptowanie lub modyfikowanie danych – każde zmienianie formatu i metody, w jakiej dane są zapisane, oraz ingerowanie w ich treść,

g) pobieranie danych – pozyskiwanie i zapisywanie danych ze źródeł ogólnodostępnych,

h) przeglądanie danych – zapoznawanie się z treścią i zawartością zestawów danych osobowych,

i) wykorzystywanie danych – dokonywanie każdej czynności, dla której potrzebne jest wykorzystanie danych osobowych,

j) ujawnianie danych poprzez przesłanie – przekazanie danych do pojedynczego, konkretnego odbiorcy,

k) rozpowszechnianie lub innego rodzaju udostępnianie danych – umożliwienie dostępu do danych dla otwartej grupy odbiorców, np. poprzez umieszczenie danych w publicznie dostępnym miejscu,

l) dopasowywanie lub łączenie danych – tworzenie powiązań pomiędzy różnymi zestawami danych osobowych,

m) ograniczanie danych – częściowe usunięcie danych, pozbawienie ich pewnych połączeń i powiązań z innymi danymi,

n) usuwanie danych – pozbawienie danych własności pozwalających na uznanie ich za dane osobowe,

o) niszczenie danych – trwałe wykasowanie danych, poprzez całkowite usunięcie ich z nośnika, na którym zostały utrwalone.

Ze względu na szczególny zakres działania Ośrodka Leczenia Uzależnień przetwarzane są w Ośrodku również dane wrażliwe - pacjentów.

ROZDZIAŁ IV

ZESPÓŁ DS. ZARZĄDZANIA BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

W celu zarządzania bezpieczeństwem danych osobowych została określona następująca struktura organizacyjna, wraz z zakresami odpowiedzialności poszczególnych osób:

1. Administrator danych – Ośrodek Leczenia Uzależnień w Lublinie w imieniu którego działa Dyrektor Ośrodka Leczenia Uzależnień SP ZOZ w Lublinie, decydujący o celach i środkach przetwarzania danych osobowych,
2. Inspektor Ochrony Danych – osoba, która określa i nadzoruje realizację polityki bezpieczeństwa danych osobowych w jednostce, ustanowiony zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych w OLU SP ZOZ,
3. Administrator Systemu Informatycznego (ASI) – osoba, która dba o bezpieczeństwo danych osobowych w systemach teleinformatycznych, ustanowiony zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych w OLU SP ZOZ.
4. użytkownik systemu – osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym OLU.

ROZDZIAŁ V

ZASADY OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Zgodnie z art. 5 RODO przy przetwarzaniu danych osobowych stosowane są następujące zasady przetwarzania:

1. zgodność z prawem, rzetelność i przejrzystość - przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
2. ograniczanie celu przetwarzania – dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami,
3. minimalizacja danych – zbierane są dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

4. prawidłowość przetwarzania – dane są prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,
5. ograniczanie przechowywania – dane są przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą,
6. integralność i poufność – dane są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,
7. rozliczalność i niezaprzeczalność - Administrator danych odpowiedzialny za przestrzeganie zasad 1-5 musi być w stanie wykazać ich przestrzeganie.

ROZDZIAŁ VI

ZARZĄDZANIE PRZETWARZANIEM DANYCH OSOBOWYCH

§ 1

Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Komórki organizacyjne Ośrodka Leczenia Uzależnień SP ZOZ w Lublinie zlokalizowane są w Lublinie w budynkach przy ul. Karłowicza 1 i Al. Tysiąclecia 5.

Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe oraz rodzaj i zakres przetwarzania danych przedstawia poniższa tabela:

Tabela nr 1

Wykaz budynków i pomieszczeń OLU SP ZOZ w Lublinie, tworzących obszar, w którym przetwarzane są dane osobowe

Lp.	**Budynek**	**Pomieszczenie**	**Komórka organizacyjna**	**Rodzaj przetwarzanych danych**	**Sposób przetwarzania**
1.	Karłowicza 1 w Lublinie	Rejestracja	Administracja	Dane osobowe pacjentów	1,2,3,4,5,6
		Pokój nr 2	PTUodSPdD/ PLU	Dane osobowe pacjentów	1,2,4,5
		Pokój nr 6	PLU	Dane osobowe pacjentów	1,2,4,5
		Pokój nr 7	PLU	Dane osobowe pacjentów	1,2,4,5,
		Pokój nr 8	PLU	Dane osobowe pacjentów	1,2,4,5
		Pokój nr 10	Z-ca dyrektora	Dane osobowe pacjentów	1,2,4,5
		Pokój nr 11	Dyrektor	Dane osobowe pacjentów i pracowników	1,2,4,5
		Pokój nr 12	PLU	Dane osobowe pracowników	1,2,3,4,5,6,
		Pokój nr 102	PTUAiW	Dane osobowe pacjentów	1,2,3,4,5,6,
		Pokój nr 106	Administracja	Dane osobowe pracowników	1,2,3,4,5,6,
				Dane pacjentów	2,6
		Pokój nr 107	Administracja	Dane osobowe pracowników	1,2,3,4,5,6,
		Pokój nr 108	PTUAiW	Dane osobowe pacjentów	1,4,5,
		Pokój nr 110	PTUAiW	Dane osobowe pacjentów	1,4,5,

		Pokój nr 111	PTUAiW	Dane osobowe pacjentów	1,4,5,
		Pokój nr 112	PTUAiW	Dane osobowe pacjentów	1,4,5,
		Pokój nr 113	PTUAiW/ DOTUA	Dane osobowe pacjentów	1,4,5,
		Pokój nr 114	DOTUA	Dane osobowe pacjentów	1,4,5,
		Pokój nr 115	DOTUA	Dane osobowe pacjentów	1,4,5,
2.	Tysiąclecia 5	Rejestracja	Program Terapii Substytucyjnej	Dane osobowe pacjentów	1,3,
		Pokój Terapeutów	Program Terapii Substytucyjnej	Dane osobowe pacjentów	1,2,3,4,5
		Pokój lekarski	Program Terapii Substytucyjnej	Dane osobowe pacjentów	2,4,6

LEGENDA: 1. zbieranie, 2. utrwalanie, 3. przechowywanie, 4. opracowywanie, 5. zmienianie, 6. udostępnianie, 7. usuwanie

§ 2

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Wykaz zbiorów danych osobowych opracowano w oparciu o Jednolity Rzeczowy Wykaz Akt OLU SP ZOZ w Lublinie, stanowiący załącznik do Instrukcji Kancelaryjnej dla Ośrodka.
2. Nazwy zbiorom nadano zgodnie z hasłem klasyfikacyjnym pierwszej, drugiej i trzeciej klasy.
3. Ośrodek Leczenia Uzależnień SP ZOZ w Lublinie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych tworzonych na jego obszarze.

Wykaz zbiorów danych osobowych wraz ze wskazaniem sposobu gromadzenia danych i nazwy programu, w którym są przetwarzane:

Tabela nr 2

Lp.	Nazwa zbioru danych osobowych (hasło klasyfikacyjne)	Sposób gromadzenia	Nazwa programu
1.	**ORGANIZACJA I ZARZĄDZANIE** 1. Akty normatywne. 2. Prognozowanie, Planowanie, Sprawozdawczość i Statystyka. 3. Informatyka. 4. Współdziałanie, Kontakty 5. Nadzór, Kontrole	Forma papierowa. Forma elektroniczna.	**System Informatyczny:** 1. Kadrowo-Płacowy - GRATYFIKANT 2. Księgowo-Rachunkowy - REWIZOR 3.Ubezpieczeniowy – PŁATNIK 4. SUBIEKT 5. System operacyjny Windows 6. Oprogramowanie biurowe
2.	**DZIAŁALNOŚĆ MERYTORYCZNA** Działalność merytoryczna - dokumentacja indywidualna pacjentów - PLU - PTUAiW - DOTUA - Programu Terapii Substytucynej - dokumentacja zbiorcza - księga główna - wydruki z rejestru komputerowego	Forma elektroniczna. Forma papierowa.	1. System KS-PPS – rozliczenia 2. System SZOI 3. System operacyjny Windows 4. Oprogramowanie biurowe)

	Dokumentacja dotycząca udzielanych w OLU SP ZOZ w Lublinie świadczeń zdrowotnych Dokumentacja związana z działalnością Programu Terapii Substytucyjnej		
3.	**KADRY.** Akta osobowe Ewidencja akt osobowych Zatrudnienie i wynagradzanie. Szkolenie pracowników. Dyscyplina pracy, urlopy, kary. Sprawy socjalno – bytowe. Ubezpieczenia osobowe. - Pomoc socjalno-bytowa - Dofinansowania i zapomogi - opieka zdrowotna - Ubezpieczenia społeczne - składki ubezpieczenia spolecznego Bezpieczeństwo i higiena pracy. - szkolenia Wypadki przy pracy, choroby Zawodowe - profilaktyka zapobiegawcza - badania okresowe	Forma papierowa. Forma elektroniczna.	1. GRATYFIKANT - system kadrowo- płacowy, 2. System SZOI 3. System operacyjny Windows 4. Oprogramowanie biuro we
4.	**BUDŻET, PODATKI, RACHNKOWOŚĆ**	Forma papierowa.	1. REWIZOR - system fi-

	Podatki i opłaty Rachunkowość, księgowość, obsługa kasowa · księgowość · płace - rozliczenia, diety, ubezpieczenia - dokumentacja wynagrodzeń za umowy zlecenia i o dzieło - deklaracje podatkowe PIT - ustalanie i odprowadzanie składek ubezpieczenia społecznego - naliczanie kapitału początkowego Zamówienia publiczne	Forma elektroniczna.	nansowo-księgowy, 2. PŁATNIK – program ubezpieczeniowy, 3. GRATYFIKANT- s. kadrowo-placowy, 4. System operacyjny Windows, 5. oprogramowanie biurowe

4. Ośrodek Leczenia Uzależnień SP ZOZ w Lublinie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia ochronę zbiorom danych osobowych sporządzanym doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką prowadzenia zajęć z pacjentami realizowanymi w Ośrodku, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji.
5. Ośrodek Leczenia Uzależnień SP ZOZ w Lublinie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zabrania tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne dla realizacji celów statutowych Ośrodka.

§ 3

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi.

1. Dane osobowe w Ośrodku Leczenia Uzależnień gromadzone są w systemach informatycznych, na zewnętrznych nośnikach danych oraz w zbiorach dokumentów papierowych.

2. Rozwiązania techniczne w systemach informatycznych pozwalają na uzupełnianie tych samych danych z innych posiadanych zasobów w ramach jednostki, co przekłada się na ich efektywniejsze wykorzystanie w załatwianiu spraw. Zakres gromadzonych danych osobowych jest zgodny z przepisami prawa.

Tabela nr 3

Struktura zbioru zawierającego informacje o pracownikach, zatrudnieniu i wynagrodzeniu.

KADRY	Ewidencja	Dane osobowe	Imię i nazwisko, PESEL, data i miejsce urodzenia, imię ojca i matki, stan cywilny, płeć, adres zamieszkania
		Pozostałe dane	Dokument tożsamości, dane ubezpieczeniowe, rozliczeniowe – nr konta w banku, badania okresowe, kursy bhp
	Zatrudnienie	Umowa o pracę	Pracownik – imię i nazwisko, adres zamieszkania, umowa nr na czas, aneksy
		Umowa cywilnoprawna	Pracownik – imię nazwisko, data umowy, nr dowodu tożsamości, adres zamieszkania, umowa- tytuł, rachunek na kwotę
PŁACE	Wypłaty	Umowy o pracę	Listy płac
		Umowy cywilnoprawne	Rachunki za świadczone usługi
INNE:	ZFŚS	Zapomogi, dofinansowanie – pracownik – imię i nazwisko, świadczenie	
SZOI	Rozliczenia	Rozliczenia z NFZ – dane osobowe pracowników i pacjentów	

Struktura zbioru zawierającego informacje o pacjentach, historia choroby i przeprowadzona terapia.

dane pacjenta:	[**pacjent -** imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), dane identyfikacyjne(Pesel,]
Udzielenie świadczenia zdrowotnego	[pacjent - imię i nazwisko, data udzielanego świadczenia, rozpoznanie

pacjentowi:	główne, rozpoznanie współistniejące i okres leczenia] Lekarz, terapeuta – imię i nazwisko , pesel, numer prawa wykonywania zawodu, data udzielonego świadczenia, rodzaj udzielonego świadczenia
Przeprowadzona terapia i zastosowane leki:	[historia choroby pacjenta]

§ 4

Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Gromadzenie danych następuje przez pozyskiwanie ich z danych źródłowych, a także z innych zasobów.
2. Gromadzone dane osobowe są udostępniane pracownikom w zakresie niezbędnym do ich pracy i wynikającym z przepisów prawa poprzez posiadane systemy informatyczne.
3. Dane udostępniane są poprzez oprogramowanie systemowe lub przy wykorzystaniu oprogramowania firm zewnętrznych.
4. Możliwość wglądu przez pracowników w dane osobowe pozwala na ich porównywanie i sprostowanie ewentualnych rozbieżności.
5. Udostępnianie danych upoważnionym pracownikom w OLU SP ZOZ w Lublinie możliwe jest za pośrednictwem serwera na którym zainstalowane jest oprogramowanie kadrowo – płacowe firmy INSERT (REWIZOR, GRATYFIKANT, SUBIEKT i program PŁATNIK. Do serwera podłączone są komputery w administracji i księgowości (stacje klienckie).
6. Dane do tych systemów wprowadzone zostały ręcznie przez obsługujących, upoważnionych pracowników OLU.
7. Pozostałe systemy i programy używane do przetwarzania danych osobowych w OLU SP ZOZ w Lublinie bazują na danych wprowadzonych przez pracowników i są to systemy zamknięte (dotyczą najczęściej komputerów znajdujących się w gabinetach terapeutów).
8. Systemy NFZ, tj. KS-PPS i SZOI, do których mają dostęp upoważnieni pracownicy Ośrodka współpracują ze sobą w przepływie danych osobowych w sieci informatycznej Narodowego Funduszu Zdrowia oraz sieci lokalnej.

Schematy przebiegu sieci lokalnej: w siedzibie ADO przy ul. Karłowicza 1 stanowi załącznik nr 1, w siedzibie przy Al. Tysiąclecia 5 stanowi załącznik nr 2.

ROZDZIAŁ VII

OKREŚLENIE ŚRODKÓW ORGANIZACYJNYCH I TECHNICZNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA ZGODNEGO Z PRAWEM PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

Środki organizacyjne

1. Osoby przetwarzające dane osobowe

W Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie w procesie zarządzania i przetwarzania danych osobowych biorą udział następujące osoby:

1. Administrator danych osobowych w OLU SP ZOZ w Lublinie, którym jest Dyrektor Ośrodka.
2. Inspektor Ochrony Danych który określa i nadzoruje realizację polityki bezpieczeństwa danych osobowych w jednostce - funkcję Inspektora Ochrony Danych (IOD) pełni osoba powołana przez ADO. W związku z wypełnianiem swoich obowiązków IOD podlega wyłącznie ADO. IOD wypełnia obowiązki nałożone przez niego **zgodnie art. 39 ust. 1 oraz 38 ust. 4 RODO** poprzez:
    a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
    d) współpracę z Prezesem Urzędu Ochrony Danych Osobowych;

e) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

f) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

IOD wypełnia **obowiązki nałożone przez niego przez ADO**, w szczególności określa i nadzoruje realizację polityki bezpieczeństwa danych osobowych w jednostce przez:

a) koordynowanie działań poszczególnych komórek organizacyjnych Ośrodka Leczenia Uzależnień w zakresie ochrony danych osobowych i innych informacji prawnie chronionych;

b) zapewnienie przestrzegania przepisów prawa o ochronie danych osobowych oraz zarządzeń Dyrektora Ośrodka dotyczących ochrony danych osobowych, przez sprawdzanie zgodności przetwarzania informacji prawnie chronionych w tym danych osobowych z przepisami o ochronie danych osobowych oraz opracowywania w tym zakresie sprawozdań dla administratora danych oraz na żądanie Urzędu Ochrony Danych, cyklicznych oraz doraźnych;

c) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania informacji prawnie chronionych, w tym danych osobowych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;

d) nadzorowanie przestrzegania zasad określonych w dokumentacji opisującej sposób przetwarzania informacji prawnie chronionych w tym danych osobowych oraz zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych informacji;

e) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

f) współdziałania z komórkami organizacyjnymi oraz stanowiskami pracy w zakresie realizowanych przez nie zadań związanych z przetwarzaniem informacji prawnie chronionych, w tym danych osobowych;

g) przeprowadzanie sprawdzeń systemu – audytów wewnętrznych.

3. Administrator systemu informatycznego (ASI) - jest to osoba wskazana przez ADO. W zakresie wypełniania swoich obowiązków ASI podlega wyłącznie ADO, zaś w przypadku realizacji zadań związanych z ochroną danych osobowych i innych informacji prawnie chronionych – podlega IOD. ASI dba o bezpieczeństwo danych osobowych w systemach teleinformatycznych, a w szczególności:

a) współpracuje z ADO przy określaniu standardów fizycznego zabezpieczenia pomieszczeń, w których są przetwarzane informacje prawnie chronione;

b) określa strategię zabezpieczania systemów informatycznych (procedury bezpieczeństwa i standardy zabezpieczeń);

c) sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania informacji;

d) sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są informacje chronione prawem, w tym dane osobowe;

e) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie informacji prawnie chronionych, w tym danych osobowych w systemach informatycznych;

f) określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są informacje podlegające ochronie;

g) odpowiada za instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;

h) sprawuje nadzór nad bezpieczeństwem informacji zawartych w komputerach przenośnych, dyskach wymiennych, pamięciach przenośnych i

innych nośnikach, w których przetwarzane są informacje prawnie chronione w tym dane osobowe;

i) monitoruje działanie zabezpieczeń teleinformatycznych wdrożonych w celu ochrony informacji i danych osobowych w systemach informatycznych;

j) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników;

w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych;

k) przyznaje danemu użytkownikowi identyfikatora oraz prawa dostępu do informacji chronionych w danym systemie teleinformatycznym;

l) prowadzi profilaktykę antywirusową;

m) monitoruje i zapewnia ciągłość działania systemu informatycznego oraz baz danych;

n) optymalizuje wydajność systemu informatycznego baz danych;

o) zarządza kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie;

p) przeciwdziała próbom naruszenia bezpieczeństwa informacji w systemach teleinformatycznych,

q) przyznaje ściśle określone prawa dostępu do informacji w danym systemie.

4. Osoby upoważnione (użytkownicy) - pracownicy OLU posiadający upoważnienie wydane przez Administratora danych lub osobę przez niego wyznaczoną i dopuszczone w zakresie wskazanym w tym upoważnieniu do przetwarzania danych osobowych w sposób tradycyjny i w systemie informatycznym danej komórki organizacyjnej,
5. Osoby upoważnione do dostępu do danych osobowych przetwarzanych w OLU na podstawie odrębnych umów powierzenia przetwarzania danych osobowych.

2. Procedury nadawania uprawnień do przetwarzania danych osobowych

1. Do przetwarzania danych, zgodnie z art. 29 RODO mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych. Ewidencję osób upoważ-

nionych do przetwarzania danych osobowych prowadzi pracownik kadr wskazany przez Administratora danych, ewidencja, której wzór stanowi załącznik nr 3 do niniejszej Polityki bezpieczeństwa ta zawiera:

a) imię i nazwisko osoby upoważnionej,

b) nazwę komórki organizacyjnej,

c) nazwę zbioru danych osobowych,

d) formę zatrudnienia lub współpracy,

e) datę nadania i ustania upoważnienia,

f) zakres upoważnienia do przetwarzania danych osobowych,

g) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

1. Ewidencja prowadzona jest w formie elektronicznej, w przypadku potrzeby przedstawienia jej w formie dokumentu – jest drukowana i podpisywana przez Dyrektora OLU - Administratora danych.
2. Upoważnienia do przetwarzania danych osobowych wydawane są na podstawie „Zakresu obowiązków, praw i odpowiedzialności" pracownika zatrudnianego w OLU SP ZOZ w Lublinie, w którym zawierają się czynności, które wymagają przetwarzania danych osobowych pracownika bądź pacjenta.
3. Dopuszcza się możliwość upoważniania do przetwarzania danych osobowych osób będących pracownikami firm zewnętrznych, które wykonują zadania na rzecz OLU w Lublinie, w obszarze gdzie przetwarza się dane osobowe, wynikające z zawartej umowy. Inspektor Ochrony Danych kieruje wniosek o wydanie upoważnienia do Administratora danych osobowych.

3. Zasady przestrzegane przy przetwarzaniu danych osobowych

W pomieszczeniach Ośrodka, w których przetwarzane są dane osobowe należy przestrzegać następujących zasad:

1. Do przetwarzania danych osobowych mogą być wykorzystywane wyłącznie urządzenia, sprzęt komputerowy i oprogramowanie będące własnością Ośrodka.

2. W pomieszczeniach Ośrodka, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych.
3. Osoby nie upoważnione do przetwarzania danych osobowych mogą przebywać w pomieszczeniach OLU SP ZOZ w którym przetwarzane są dane osobowe - wyłącznie w obecności upoważnionego pracownika Ośrodka.
4. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, wiąże się z zastosowaniem wszelkich środków zabezpieczających dane osobowe oraz to pomieszczenie przed wejściem osób niepowołanych.
5. Chwilowe opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiającym dostęp do danych osobowych osobom niepowołanym.
6. Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne, i jako takie traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

4. Zasady postępowania w przypadku naruszenia ochrony danych osobowych

Każda osoba biorąca udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialna za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogące spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Inspektora Ochrony Danych, Administratora Systemu Informatycznego lub Administratora danych.

§ 2

Środki techniczne

1. Kontrola dostępu – ochrona fizyczna pomieszczeń

Dostęp do pomieszczeń Ośrodka Leczenia Uzależnień SP ZOZ w Lublinie, w których przetwarzane są dane osobowe podlega kontroli, tj.:

1. Kontrola dostępu polega w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia oraz godzinę pobrania i zdania klucza.
2. Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane są wyłącznie pracownikom posiadającym upoważnienie do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych pomieszczeń na odrębnych zasadach.
3. Ośrodek Leczenia Uzależnień realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.

2. Postępowanie w zakresie komunikacji w sieci komputerowej

1. Podłączenie sprzętu komputerowego do sieci teleinformatycznej wykonuje wyłącznie Administrator Systemu Informatycznego na polecenie Dyrektora OLU, za wiedzą IOD.
2. Zasoby informatyczne mogą być wykorzystywane wyłącznie do wykonywania obowiązków służbowych.
3. OLU SP ZOZ nie korzysta z sieci bezprzewodowej.
4. Komunikacja pomiędzy pracownikami następuje poprzez foldery udostępnione w sieci, na serwerze NAS.
5. W celu wykonywania obowiązków służbowych ASI wykorzystuje zdalny dostęp do zasobów sieci lokalnej poprzez serwer VPN oraz FDP (pulpit zdalny) w obu lokalizacjach OLU (ul. Karłowicza, Al. Tysiąclecia).

6. Serwisant oprogramowania KS PPS (w lokalizacji Karłowicza) – firma SO-Med – wykorzystuje do zdalnego łączenia się z zasobami bazy danych KS-PPS oraz dwóch komputerów rejestracji poprzez program LogMeIn. Ma również dostęp do kopii bazy danych na serwerze NAS (udział sieciowy).
7. Serwisant oprogramowania Molteni (w lokalizacji przy ul. Tysiąclecia) wykorzystuje do zdalnego łączenia się z zasobami bazy danych SERT (komputer dzierżawiony od firmy Molteni) program TeamViewer. Ma również dostęp do kopii bazy danych na serwerze NAS (udział sieciowy) w lokalizacji Tysiąclecia.
8. Skonfigurowano możliwość współdzielenia zasobów informatycznych lokalizacji Karłowicza i Tysiąclecia.

Środki techniczne i organizacyjne zostały określone w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie" wprowadzonej zarządzeniem Dyrektora.

3. Ochrona danych osobowych przetwarzanych w formie elektronicznej

Uwzględniając kategorie przetwarzanych danych wprowadza się w OLU wysoki poziom bezpieczeństwa ochrony danych osobowych. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego połączone jest z siecią publiczną.

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną, oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.
3. Stosuje się mechanizmy kontroli dostępu do danych osobowych, wprowadzając w tym systemie, rejestrowany dla każdego użytkownika odrębny identyfikator.
4. Dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia przez wprowadzenie hasła.

5. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.
6. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed utratą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej przez zastosowanie UPS`ów oraz wykonywanie kopii bezpieczeństwa zbiorów danych.
7. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji pozbawia się wcześniej zapisów tych danych.
8. W razie konieczności naprawy sprzętu komputerowego zachowuje się szczególną ostrożność, aby nie doszło do ujawnienia danych osobowych. Nie dopuszcza się samowolnego naprawiania lub ingerencji w sprzęt osób nieuprawnionych.
9. Nie dopuszcza się przetwarzania danych osobowych na komputerach przenośnych lub stacjonarnych, jeśli wynoszone są poza obszar przetwarzania danych.
10. Każda osoba, jeżeli została dopuszczona do przetwarzania danych osobowych poprzez wydanie dla niej upoważnienia do przetwarzania danych osobowych, jest zobowiązana do poznania działania powierzonych mu do eksploatacji narzędzi informatycznych (sprzęt i oprogramowanie) w sposób, który umożliwi jej prawidłowe wykonywanie obowiązków służbowych. W przypadkach szczególnych, dotyczących szczególnie istotnych lub skomplikowanych niezbędnych do wykonania czynności dotyczących sprzętu lub oprogramowania, osoba taka może wystąpić do Administratora danych z wnioskiem o skierowanie jej na szkolenie specjalistyczne.
11. Szkolenie nie może dotyczyć podstaw posługiwania się sprzętem komputerowym (jak włączanie, wyłączanie sprzętu, drukowanie, logowanie do systemu i aplikacji użytkowych, zmiana haseł itp.), posługiwania się pakietem oprogramowania biurowego oraz innych czynności podstawowych.

UWAGA: Szczegółowe zasady, procedury postępowania i środki bezpieczeństwa podczas przetwarzania i gromadzenia danych osobowych w formie elektronicznej zawarte są w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w OLU SP ZOZ w Lublinie

4. Środki ochrony w zakresie zabezpieczenia sprzętowego

1. serwer wyposażony w pamięć operacyjną z detekcją błędów,
2. równoległy zapis na dyskach,
3. zasilanie awaryjne serwerów i stacji roboczych (UPS).

5. Środki ochrony w ramach oprogramowania systemu

1. Zbiory danych osobowych oraz programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem poprzez wykonywanie kopii bezpieczeństwa.
2. W celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych.
3. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
4. W celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu informatycznego, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło.
5. Ograniczone zostało logowanie do systemu na koncie użytkownika uprzywilejowanego.
6. Rejestracja nieudanych prób logowania do systemu.
7. Logowanie wszystkich wykonywanych czynności.
8. W celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją.
9. Oprogramowanie antywirusowe jest stale aktywne

6. Konfiguracja systemu do przetwarzania danych osobowych

Konfiguracja systemu do przetwarzania danych osobowych należy do wyłącznej kompetencji Administratora Systemu Informatycznego. Sprawuje on bieżący nadzór nad systemami informatycznymi, niedopuszczalne jest ingerowanie w konfigurację osób nieupoważnionych.

Konfiguracja obejmuje:

1. stacje robocze,

3. urządzenia wielofunkcyjne,

4. drukarki,

5. skanery,

6. urządzenia sieciowe – routery, switch`e

7. Acces Point`y

Konfiguracja systemu:

- ustawienia BIOS`u

- zasady konta,

- zasady haseł,

- zasady blokady konta,

- zasady lokalne: zasady inspekcji,

- logowanie na kontach,

- zarządzanie kontami,

- śledzenie,

- usługi katalogowe,

- logowanie/wylogowywanie,

- dostęp do obiektów,

- zmiana zasad,

- wykorzystanie uprawnień,

- system,

- globalny dostęp do obiektów,

- zasady lokalne: przypisywanie praw użytkownika,

- opcje zabezpieczeń: inspekcje

- dzienniki zdarzeń (logi systemowe): instalator, system, zabezpieczenia

- składniki systemu Windows: instalator Windows, interfejs użytkownika do obsługi poświadczeń, Internet Explorer, kopia zapasowa, NetMeeting, pomoc online, Windows defender, Windows Update

- usługi pulpitu zdalnego: host sesji pulpitu zdalnego: połączenia, przekierowywanie urządzeń i zasobów, zabezpieczenia, klient usługi podłączanie pulpitu zdalnego, Windows Anytime Upgrade, Windows media Center, Windows Messanger, zarządzanie prawami cyfrowymi w pakiecie Windows Media, zasady autoodtwarzania

- system: dostęp do magazynu wymiennego, logowanie, pomoc zdalna, zarządzanie komunikacją internetową, zasady grupy, zdalne wywoływanie procedury

- konfiguracja konta użytkownika: Menu Start i pasek zadań, panel sterowania - personalizacja, Eksplorator Windows

- ustawienia sieciowe.

7. Kopie bezpieczeństwa

1. Za tworzenie kopii bezpieczeństwa odpowiadają:

a) Firma So-MED. Magdalena Wdowicz z siedzibą w Lublinie, ul. Zana 13/4 w przypadku oprogramowania KAMSOFT – Podstawowy Program Świadczeniobiorcy KS-PPS na podstawie zawartych umów.

b) Maciej Łabno – serwisant Molteni dla bazy SERT na podstawie zawartych umów,

c) Administrator Systemu Informatycznego administrujący również oprogramowaniem INSERT na podstawie zawartej umowy tj. m.in. instalujący oprogramowanie, podłączający klientów do bazy danych, wykonujący aktualizacje i reset haseł.

d) Administrator Systemu Informatycznego w przypadku oprogramowania KMASOFT, SERT, INSERT wykonuje kopie bazy danych na podstawie sporządzonych przez So-MED oraz M. Łabno kopii baz.

2. Procedury dotyczące kopii baz danych

a) Kopie baz danych wykonywane są codziennie przy użyciu modułów zawartych w oprogramowaniu, jak również przy użyciu oprogramowania Cobian Backup i serwerów NAS.

b) Co trzydziesta kopia jest sprawdzana pod kątem użyteczności i umieszczana w Archiwum. Sprawdzenia kopii dokonują podmioty je wykonujące.

c) Dostęp do kopii mają ASI oraz formy odpowiednio wykonujące kopie.

d) Kopie bezpieczeństwa są przechowywane na będącym własnością OLU SP ZOZ w Lublinie serwerze bazodanowym oraz NAS.

8. Postępowanie z kluczami kryptograficznymi, służącymi do kontaktowania się z podmiotami zewnętrznymi

1. Klucze kryptograficzne, wykorzystywane w OLU SP ZOZ służą do zabezpieczania kontaktów z podmiotami zewnętrznymi, tj. bankami, ZUS i funduszami.
2. Osoby dysponujące kluczami kryptograficznymi zobowiązane są do ich nieudostępniania osobom postronnym oraz do przechowywania ich w zamykanych na klucz, niedostępnych osobom postronnym meblach biurowych.
3. Wykaz osób, dysponujących kluczami kryptograficznymi zawarty jest w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w OLU SP ZOZ w Lublinie.

9. Narzędzia kryptograficzne

1. Należy tworzyć trudne do złamania hasła oraz przestrzegać elementarnych zasad ich ochrony
2. **Nigdy nie należy podawać hasła w wiadomościach e–mail, bądź też w odpowiedzi na żądanie, które zostało przesłane pocztą e-mail.**
3. Nie wolno używać publicznie dostępnych komputerów (np. w hotelach, kafejkach internetowych) do logowania się do takich usług jak bank, konto pocztowe. Komputery takie są pod słabym nadzorem i często są zainfekowane oprogramowaniem szpiegującym.
4. Nie wolno używać programów pochodzących z nielegalnego źródła, podejrzanych stron, klikania w linki, które rzekomo przenoszą użytkownika do szokującego lub niedostępnego w inny sposób materiału.
5. Szczególną ostrożność należy zachować przy wykorzystywania wszelkich urządzeń mobilnych, gdyż z reguły są one słabiej zabezpieczone i cieszą się rosnącym zainteresowaniem wśród cyberprzestępców.
6. W celu podniesienia poziomu zabezpieczeń wprowadza się obowiązek zabezpieczania przekazywanego dokumentu przed odczytaniem przez osobę nieuprawnioną oraz przed

naniesieniem nieautoryzowanych zmian w jego treści.

10. Ochrona danych osobowych przetwarzanych w formie papierowej.

1. Dane osobowe przetwarzane i gromadzone przy użyciu tradycyjnych środków gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach.
2. Dane te należy przechowywać w szafach zamykanych na zamek patentowy oraz w sejfach i kasetkach przeznaczonych do tego celu.
3. Obszar przetwarzania i gromadzenia danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych. Przebywanie osób nieupoważnionych w obszarze przetwarzania danych jest dopuszczalne za zgodą administratora danych w obecności osób upoważnionych do przetwarzania danych osobowych.
4. Sposób postępowania z kluczami do pomieszczeń i szaf określają Procedury postępowania z kluczami mechanicznymi i elektronicznymi, stanowiącymi załącznik do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych .

11. Udostępnianie danych osobowych.

1. Udostępnienie danych osobowych pacjentów i pracowników może nastąpić jedynie w formie pisemnej.
2. Dane osobowe pracowników i pacjentów mogą być udostępniane jedynie osobom i podmiotom do tego upoważnionym.
3. Zasady udostępniania danych osobowych w bieżącej działalności ADO określa Instrukcja zarządzania system informatycznym służącym do przetwarzania danych osobowych.
4. Zasady udostępniania danych osobowych innym administratorom danych określone jest w Rozdziale VI – Powierzenie przetwarzania danych osobowych oraz Rozdziale VII – Udostępnianie danych osobowych niniejszej Polityki bezpieczeństwa.

Udostępnienie danych pacjenta określa Instrukcja postępowania w sprawie udostępniania dokumentacji medycznej.

10. PRZYPORZĄDKOWANIE OKREŚLONYCH TECHNICZNYCH I ORGANIZACYJNYCH ŚRODKÓW OCHRONY DO CHRONIONYCH ATRYBUTÓW INFORMACJI

Zgodnie z przedmiotem działalności OLU SP ZOZ w Lublinie przyjęto, że przez zachowanie bezpieczeństwa danych osobowych należy rozumieć zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności i niezaprzeczalności informacji zawierających te dane.

Poufność danych - właściwość danych wskazująca obszar, w którym te dane nie powinny być dostępne lub ujawnione osobom niepowołanym, procesom lub innych podmiotom.

Środki realizujące to:

1. dostęp osób do serwerowni (pok. 4) ograniczony i kontrolowany, w pok. 102, 114, 116 i Zakładowej Składnicy Akt są także przechowywane dane w formie tradycyjnej (papierowe) – do pomieszczeń tych dostęp jest również ograniczony;

2. zastosowanie odpowiednich szaf z odpowiednimi zamkami do przechowywania dokumentów i elektronicznych nośników danych zawierających dane osobowe, opracowanie i stosowanie regulaminu Zakładowej Składnicy Akt regulującego i ograniczającego dostęp do dokumentacji medycznej pacjentów;

3. konstrukcja budynku i drzwi, zabezpieczenia okien na parterze, stosowanie rolet wewnętrznych;

4. utworzono indywidualne konta użytkowników chronione hasłami.

Integralność danych - właściwość polegająca na tym, że dane nie zostały wcześniej zmienione lub zniszczone w nieautoryzowany sposób.

Środki realizujące to:

1. indywidualne konta użytkowników chronione hasłami,

2. kopie bezpieczeństwa,

3. ograniczony, kontrolowany dostęp do obszarów przetwarzania danych osobowych odpowiednich kategorii.

Rozliczalność i niezprzeczalność danych - zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Środki realizujące to:

1. opracowanie, wdrożenie i przestrzeganie w OLU dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ich ochronę tj. Polityki bezpieczeństwa w zakresie przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie, opracowanie dokumentacji Szacowania ryzyka związanego z bezpieczeństwem danych osobowych oraz Instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie,

2. powołanie Inspektora Ochrony Danych (IOD), który określa i nadzoruje realizację polityki bezpieczeństwa danych osobowych oraz Administratora Systemów Informatycznych (ASI), który dba o bezpieczeństwo danych osobowych w systemach teleinformatycznych i realizuje zalecenia IOD.

Dostępność danych - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.

Środki realizujące to:

1. dedykowane i odpowiednio opisane szafy do przechowywania dokumentacji,

2. odpowiednio skonfigurowany system operacyjny (szybkość, niezawodność),

3. zapewnienie dostępu do danych z innej stacji klienckiej (w razie awarii),

4. prosty układ katalogów użytkowników,

5. zapewnienie zasilania awaryjnego (UPS),

6. kopie bezpieczeństwa.

ROZDZIAŁ III

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

Każdy podmiot biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogące spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania o tym fakcie IOD i/lub ADO, i/lub ASI.

1. Definicja naruszenia ochrony danych osobowych

Za naruszenie ochrony danych osobowych uważa się naruszenie bezpieczeństwa danych osobowych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych tj. każde naruszenie poufności, dostępności, integralności, rozliczalności, autentyczności, niezaprzeczalności danych osobowych, w szczególności gdy:

1. przetwarzanie danych odbywa się bezprawnie tj. bez posiadania podstawy prawnej do przetwarzania lub jest prowadzone przez osoby/podmioty nieuprawnione. Podmiotem nieuprawnionym do przetwarzania jest podmiot, któremu nie wydano stosownego upoważnienia do przetwarzania danych osobowych w konkretnym zbiorze danych lub nie zawarto z takim podmiotem umowy powierzenia przetwarzania danych osobowych w imieniu administratora danych;
2. stwierdzono przebywanie w obszarach przetwarzania danych osobowych osób nieuprawnionych;
3. stwierdzono uszkodzenie zabezpieczeń fizycznych pomieszczeń, tworzących obszar przetwarzania danych osobowych;
4. stwierdzono ujawnienie danych osobowych podmiotom nieuprawnionym (utrata atrybutu poufności danych);
5. stwierdzono ingerencję osób nieuprawnionych w architekturę systemu przetwarzającego dane osobowe;
6. stwierdzono niezgodne z niniejszą Polityką bezpieczeństwa i/lub Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych postępowanie osób uprawnionych;
7. stwierdzono utratę danych osobowych utrwalonych w sposób tradycyjny (papierowy),
8. zgubione zostało utrwalone (zapisane) hasło;
9. podczas kontroli antywirusowej wykryto szkodliwe oprogramowanie na dysku wewnętrznym komputera;

2. Postępowanie w przypadku podejrzenia wystąpienia naruszenia ochrony danych osobowych

Przyjmuje się następującą procedurę informowania o pojawiającym się naruszeniu oraz sposób postępowania w przypadku naruszenia ochrony danych osobowych:

a) w przypadku stwierdzenia wystąpienia lub podejrzenia wystąpienia naruszenia ochrony danych osobowych użytkownicy standardowi i/lub ASI powiadamiają niezwłocznie ADO,

b) wszelkie czynności i ustalenia odnośnie naruszenia ochrony danych osobowych są dokumentowane na bieżąco w Protokole ustaleń naruszenia ochrony danych osobowych, stanowiącym załącznik nr 4 do niniejszej Polityki.

3. Postępowanie w przypadku naruszenia ochrony danych osobowych

IOD oraz ADO, po otrzymaniu zawiadomienia o naruszeniu ochrony danych osobowych, we współpracy z ASI – jeśli jest wymagana, niezwłocznie podejmuje następujące działania:

a) dokonuje oceny, czy i w jaki sposób naruszona została ochrona, w szczególności czy naruszono ochronę fizyczną i w jaki sposób, czy i w jaki sposób naruszono ochronę architektury systemu informatycznego,

b) dokonuje oceny istotności naruszenia dla poufności, dostępności, integralności, rozliczalności, autentyczności i niezaprzeczalności informacji,

c) gromadzi dokumentację dowodową naruszenia ochrony danych osobowych, w szczególności zabezpiecza i dokumentuje ślady naruszenia ochrony fizycznej, zabezpiecza logi systemowe i pliki elektroniczne, gromadzi dane z systemów monitorowania dostępu,

d) podejmuje decyzję o dalszej eksploatacji systemu służącego do przetwarzania danych osobowych lub o jej wstrzymaniu,

e) podejmuje działania niezbędne do usunięcia skutków naruszenia ochrony danych osobowych,

f) dokonuje ponownego oszacowania ryzyka wywołanego incydentem,

g) wydaje zalecenia dotyczące podniesienia poziomu jakości lub zmiany zabezpieczeń i nadzoruje ich wykonanie w odniesieniu do ochrony fizycznej,

h) wydaje zalecenia dotyczące podniesienia poziomu jakości zabezpieczeń i nadzoruje ich wykonanie w odniesieniu do architektury systemu służącego do przetwarzania danych osobowych,

i) dokonuje niezbędnych zmian w dokumentacji bezpieczeństwa,

j) wykonuje sprawdzenie systemu - audyt systemu służącego do przetwarzania danych osobowych zgodnie z Listą pytań audytu wewnętrznego, stanowiącą załącznik nr 5 do niniejszej Polityki bezpieczeństwa.

k) przeprowadza szkolenie użytkowników obejmujące dokonane w ochronie systemu służącego do przetwarzania danych osobowych zmiany wraz z informacją o zaistniałym incydencie.

Niezależnie od prowadzenia wewnętrznej procedury wyjaśniającej, ADO powiadamia Urząd Ochrony Danych jeżeli stwierdzi, że występuje ryzyko naruszenia praw lub wolności osób, które jest następstwem takiego przetwarzania danych osobowych, które może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych.

ROZDZIAŁ IV

SPRAWDZENIA SYSTEMU – AUDYTY WEWNĘTRZNE

1. Częstotliwość wykonywania sprawdzeń systemu – audytów wewnętrznych

Sprawdzenia systemu zabezpieczeń wykonuje się:

1.1. Pełne sprawdzenie

- po zatwierdzeniu dokumentacji bezpieczeństwa,
- cyklicznie raz na 12 miesięcy.

1.2. Sprawdzenia częściowe, w zakresie dokonanych w systemie zabezpieczeń zmian, koniecznych w związku z zaistniałymi zdarzeniami:

- po wystąpieniu naruszenia ochrony danych osobowych i usunięciu jego skutków,
- po każdej istotnej zmianie dokumentacji bezpieczeństwa.

Jeżeli w/w zaistniałe zdarzenia określone zostaną jako mające duży wpływ na poziom bezpieczeństwa danych osobowych - wykonuje się sprawdzenie pełne.

1.3. Zagadnienia sprawdzeń

Sprawdzeniu podlegają następujące zagadnienia:

- uprawnienia do dostępu do danych osobowych przetwarzanych w systemie,

- bezpieczeństwo fizyczne systemu,
- ciągłość działania, kopie zapasowe, zasilanie awaryjne,
- ustawienia konfiguracyjne systemu i urządzeń, zarządzanie konfiguracją,
- utrzymanie systemu, przeglądy diagnostyczne i naprawy,
- incydenty naruszenia ochrony danych osobowych, ochrona przed oprogramowaniem złośliwym,
- zasady wprowadzania poprawek, aktualizacja oprogramowania,
- ochrona informatycznych nośników danych,
- identyfikacja i uwierzytelniania użytkowników i urządzeń,
- kontrola dostępu do systemu,
- zarządzanie ryzykiem.

1.4. Dokumentacja sprawdzenia

Sprawdzenia dokumentowane są w postaci sporządzenia Sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, którego wzór stanowi załącznik nr 6.

Sprawozdanie obejmuje określenie co najmniej:

- administratora danych,
- podmiotu/podmiotów wykonujących sprawdzenia,
- wykaz czynności objętych sprawdzeniem oraz podanie osób i podmiotów uczestniczących w sprawdzeniu,
- datę rozpoczęcia i zakończenia sprawdzenia,
- określenie przedmiotu i zakresu sprawdzenia,
- opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wyszczególnienie załączników – w tym załącznika stanowiącego tabele audytu.

1.5. Podmioty wykonujące sprawdzenia

Osoby i podmioty odpowiedzialne za bezpieczeństwo danych osobowych, tj. za wdrożone i eksploatowane systemy i procedury zabezpieczeń tj. ADO wraz z ASI oraz – w miarę potrzeb – z przedstawicielami podmiotów świadczących na podstawie umów powierzenia przetwarzania danych osobowych i umów serwisowych usługi mające wpływ na ochronę danych osobowych.

1.6. Działania podejmowane na podstawie wyników sprawdzeń

Wyniki audytu analizuje ADO, który po zapoznaniu się z jego wynikami podejmuje decyzję o wstrzymaniu lub nie wstrzymywaniu przetwarzania danych osobowych.

1.7. Częstotliwości planowanych przeglądów dokumentacji bezpieczeństwa danych osobowych

- podczas wdrażania dokumentacji bezpieczeństwa,
- po wystąpieniu naruszenia ochrony danych osobowych i usunięciu jego skutków, jeśli zajdzie taka potrzeba,
- na wniosek Administratora Systemu Informatycznego lub użytkownika standardowego.

1.8. Zmiany w dokumentacji bezpieczeństwa danych osobowych

Zmian i aktualizacji w zapisach dokumentacji bezpieczeństwa danych osobowych dokonuje się gdy:

- nastąpiła zmiana zagrożeń występujących przy przetwarzaniu danych osobowych,
- wykryto nowe słabe miejsca w systemie środków ochrony, mających istotny wpływ na bezpieczeństwo danych osobowych,
- nastąpiła zmiana wymagań bezpieczeństwa będąca następstwem zmian przepisów prawa stanowiących o wymaganiach bezpieczeństwa systemu teleinformatycznego, służącego do przetwarzania danych osobowych,
- dokonano zmian w oprogramowaniu systemowym lub innym oprogramowaniu mającym związek z bezpieczeństwem systemu,

- dokonano zmiany klasy bezpieczeństwa zastosowanych urządzeń lub oprogramowania realizującego funkcje zabezpieczeń,
- dokonano zmian w konfiguracji sprzętowej, mających wpływ na bezpieczeństwo danych osobowych.

ROZDZIAŁ V

OBOWIĄZEK INFORMACYJNY

1. ZASADY STOSOWANE PRZY WYPEŁNIANIA OBOWIĄZKU INFORMACYJNEGO

Zgodnie z Motywem 60 preambuły RODO osoba, której dane dotyczą, musi być poinformowana o fakcie prowadzenia operacji przetwarzania jej danych osobowych i o celach takiego przetwarzania oraz uzyskać wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.

1.1 Obowiązek informacyjny wypełnia się:

1) gdy dane zbierane są bezpośrednio od osoby, której one dotyczą - najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą,

2) w przypadku gromadzenia danych ze źródeł pośrednich, tj. nie od osoby, której one dotyczą - w rozsądnym terminie, jednak nie później niż w ciągu miesiąca,

3) w przypadku planowania przez administratora ujawnienia danych osobowych innemu odbiorcy - w momencie pierwszego ujawnienia tych danych innemu odbiorcy,

4) w przypadku rozszerzenia katalogu danych, które administrator ma już w posiadaniu o nowe kategorie informacji o osobie, której dane dotyczą,

5) w przypadku zmiany celu przetwarzania danych osobowych na inny cel, niż dla którego dane osobowe zostały zebrane.

1.2. Obowiązku informacyjnego nie wypełnia się:

1) w przypadku, gdy w wyniku działań prowadzonych przez administratora lub osoby, której dane dotyczą, zebrane dane zostają jedynie zaktualizowane lub usunięte,

2) w przypadku, gdy osoba, której dane dotyczą, dysponuje już tymi informacjami, przy czym nie ma znaczenia z jakiego źródła dane te zostały zebrane (jedynie w sytuacji, gdy osoba, której dane dotyczą już posiada pełną informację o administratorze danych),

3) w przypadkach gdy okaże się to niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym o ile obowiązek informacyjny może uniemożliwić lub poważnie utrudnić realizację celów przetwarzania. Jeżeli spełnienie obowiązku informacyjnego jest niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, administrator danych podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osób, których dane dotyczą, przy czym może to zrealizować poprzez umieszczenie treści obowiązku informacyjnego w miejscu powszechnie dostępnym, czyli np. na swojej stronie internetowej,

4) w przypadku, gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,

5) w przypadku, gdy dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

2. ZAKRES OBOWIĄZKU INFORMACYJNEGO

ADO, przetwarzający dane osobowe jest zobowiązany do wypełnienia wobec tych osób obowiązku informacyjnego określonego w art. 13 i 14 RODO, tj poinformowania tych osób o:

1) nazwie oraz danych kontaktowych administratora danych,

2) danych kontaktowych Inspektora Ochrony Danych,

3) celu i podstawie przetwarzania danych,

4) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,

5) okresie przez jaki dane osobowe będą przechowywane,

6) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,

7) prawie do cofnięcia wyrażonej zgody na przetwarzanie danych w dowolnym momencie,

8) prawie do wniesienia skargi do organu nadzorczego,

9) ewentualnym profilowaniu danych.

3. REALIZACJA OBOWIĄZKU INFORMACYJNEGO PRZEZ ADO

Kategorie osób, których dane dotyczą wobec których ADO spełnia obowiązek informacyjny:

- pacjenci ADO,
- pracownicy ADO,
- kontrahenci ADO.

3.1. Obowiązek informacyjny wobec pacjentów

- obowiązek informacyjny wobec pacjentów realizuje się wobec:
- pacjentów pełnoletnich,
- pacjentów małoletnich, którzy ukończyli 16 lat,
- w przypadku pacjentów małoletnich poniżej 16 roku życia i pacjentów, którzy nie posiadają pełnej zdolności do czynności prawnych – wobec ich przedstawicieli ustawowych.

3.2. Obowiązek informacyjny wobec pracowników ADO

„Pracownikiem" określa się każdą osobę pozostającą w takim stosunku prawnym z ADO, że pozostaje on administratorem danych osobowych tej osoby, zgromadzonych do celu realizacji zawartej umowy tj.:

- pracowników zatrudnionych na umowę o pracę,

- osób z którymi zawarto umowę cywilnoprawną, jeśli osoby te stanowią personel ADO,

- wolontariuszy, stażystów itd.

Realizując obowiązek informacyjny wobec pracowników, ADO uwzględnia każdorazowo odrębny cel, do jakiego gromadzi i przetwarza dane osobowe, tj.

- cel - rekrutacja pracowników,

- cel – zawarcie i realizacja umowy z pracownikiem.

3. 3. Obowiązek informacyjny wobec kontrahentów

Realizując obowiązek informacyjny wobec kontrahentów ADO określa jako podstawowy cel przetwarzania danych osobowych - zawarcie i realizację umowy. Dane osobowe przetwarzane w celu zawarcia i realizacji umowy dotyczą danych osobowych osób fizycznych będących kontrahentami ADO oraz danych osobowych przedstawicieli firm i osób podanych do kontaktu.

3.4. Sposób wypełniania obowiązku informacyjnego przez ADO

ADO spełnia obowiązek informacyjny poprzez stosowanie pisemnych klauzul informacyjnych, odpowiednio skonstruowanych w każdym przypadku, gdy pozyskuje i przetwarza dane osobowe.

ROZDZIAŁ VI

POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Definicja powierzenia

Powierzenie przetwarzania danych osobowych polega na przekazaniu do przetwarzania danych innemu podmiotowi w celu i zakresie określonym przez podmiot, który dane powierza. Podmiot powierzający pozostaje administratorem tych danych i nadal decyduje o celach i środkach przetwarzania danych. Podmiot, któremu dane powierzono do przetwarzania, przetwarza dane na polecenie podmiotu powierzającego, nie może wykorzystywać ich do realizacji własnych celów. Dalsze udostępnianie, bądź sprzedawanie danych osobowych przez ten podmiot bez zezwolenia jest niezgodne z prawem – dane są własnością administratora. Odpowiedzialność za stosowanie się przez podmiot, któremu dane powierzano do przepisów o ochronie danych osobowych ponosi podmiot, który dane powierzył.

2. Umowa główna i umowa powierzenia

1) ADO jest uprawniony do zawierania z zewnętrznymi podmiotami specjalistycznymi umów na skorzystanie w określonym zakresie z wiedzy posiadanej przez te specjalistyczne podmioty (outsourcing IT, usług finansowo – księgowych, obsługi prawnej itp.). Umowa, którą zawrze ADO na świadczenie usług specjalistycznych stanowić będzie umowę główną.

2) Jeżeli do realizacji tej umowy konieczne jest przekazanie danych osobowych, których ADO jest administratorem, zaś przetwarzanie będzie dokonywane przez procesora na polecenie administratora w sposób przez niego (administratora) wskazany i nadal będzie on decydo-

wał o celach i środkach przetwarzania, administrator zobowiązany jest do zawarcia z tym podmiotem umowy powierzenia przetwarzania danych osobowych. Umowa powierzenia zostanie zawarta w związku z zawarciem umowy głównej.

3) W umowie powierzenia przetwarzania danych osobowych podmiotem powierzającym jest administrator tych danych (ADO), zaś podmiot, któremu powierzono przetwarzanie - procesorem, przetwarzającym dane osobowe przekazane przez administratora. Warunkiem konieczności zawarcia umowy powierzenia przetwarzania danych osobowych jest to, że procesor, któremu powierza się dane jest podmiotem odrębnym i funkcjonującym poza strukturą administratora danych.

3. Uregulowania zawarte w umowie powierzenia

3.1. Określenie zakresu oraz celu przetwarzania danych osobowych

3.1.1. Zakres danych

Przez zakres danych należy rozumieć zarówno kategorie danych osobowych (imię, nazwisko, adres, itp.) jak i operacje, jakie procesor może wykonywać na powierzonych mu danych (przechowywanie, zbieranie, usuwanie, itp.).

Zakres przetwarzania danych powinien zostać wskazany enumeratywnie lub, w przypadku gdy jest to niemożliwe ze względu na rodzaj współpracy, określić należy zbiory danych osobowych lub też wprowadzić zapis, iż powierzenie następuje *w zakresie niezbędnym do realizacji umowy głównej.*

3.1.2. Cel przetwarzania

Określenie celu wiąże się ze wskazaniem przeznaczenia danych osobowych, tj. realizacji przedmiotu umowy głównej.

3.1.3. Przedmiot i czas trwania przetwarzania

Należy wskazać czas, na jaki zostaje zawarta umowa powierzenia (np. na czas realizacji umowy głównej)

3.1.4. Charakter przetwarzania

Należy określić, czy powierzenie będzie działaniem jednorazowym, czy też będzie miało charakter ciągły. Należy również wskazać, czy dane będą przetwarzane w sposób tradycyjny (wyłącznie papierowy) czy też z wykorzystaniem narzędzi informatycznych.

Należy określić, jakie operacje na danych osobowych są dopuszczalne dla procesora (zbieranie, przechowywanie, modyfikowanie, usuwanie, niszczenie itp.).

3.1.5. Rodzaj danych osobowych

Należy określić, czy powierzane będą dane osobowe szczególnych kategorii tj. dane wrażliwe oraz dane osobowe dotyczące wyroków skazujących i naruszeń prawa, czy też dane „zwykłe" (tj. nie będące danymi wrażliwymi oraz dotyczącymi skazań i naruszeń prawa)

3.1.6. Kategorie osób, których dane dotyczą

Należy wskazać, czyje dane zostały przekazane procesorowi do przetwarzania – np. dane pracowników, kontrahentów itd.

3.2. Obowiązki i prawa administratora

Obowiązki:

Administrator danych jest zobowiązany do wyboru takiego procesora, który zapewnia gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Odpowiedzialność za powierzenie przetwarzania danych przez odpowiedni podmiot leży na administratorze.

Prawa:

- zastrzeżenie kar umownych w przypadku naruszenia przez procesora postanowień umowy,
- wprowadzenie szczegółowych zasad prowadzenia audytów lub inspekcji przez administratora,
- określenie skuteczności i mocy wiążącej zaleceń wydawanych w toku prowadzonych audytów lub inspekcji przez administratora,
- wspieraniem administratora w przypadku kontroli przestrzegania przepisów RODO,
- stosownymi obostrzeniami lub konkretnymi rozstrzygnięciami w zakresie obligatoryjnych środków technicznych i organizacyjnych, których zastosowania żąda administrator,

- zobowiązuje się do stosowania się do instrukcji i poleceń Administratora dotyczących przetwarzania należących do niego danych osobowych.

3.3. Obowiązki procesora

Obowiązki procesora należy określić w zawieranej umowie powierzenia zgodnie z art. 28 ust. 3 lit. a)-h) RODO tj:

- przetwarzanie danych osobowych wyłącznie na udokumentowane polecenie administratora,
- zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
- podejmowanie wymaganych środków zabezpieczających przetwarzane dane osobowe,
- pomoc administratorowi w wywiązywaniu się z obowiązków wobec osób, których dane dotyczą,
- po zakończeniu świadczenia usług związanych z przetwarzaniem, usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie ich istniejących kopii (zależnie od decyzji administratora).

Wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 7.

ROZDZIAŁ VII

UDOSTĘPNIANIE DANYCH OSOBOWYCH

Udostępnianie danych osobowych polega na przekazaniu danych osobowych innemu podmiotowi, który sam decyduje o celach i środkach przetwarzania danych tj. odrębnemu administratorowi danych osobowych. Za legalność udostępniania danych odpowiada administrator udostępniający dane. Dane udostępnia się wyłącznie na piśmie, na podstawie złożonego wniosku o udostępnienie danych.

Udostępnienie danych osobowych zachodzi, gdy:

- administrator nie ma kontroli nad przetwarzaniem tych danych, a więc nie decyduje o sposobie i celach przetwarzania przekazanych danych osobowych przez podmiot, który otrzymał dane,

- podstawami do udostępnienia danych jest zawarta umowa lub obowiązek wynikający z przepisów prawa,
- wykonywana jest procedura dostępu do danych (art. 15 ust. 1 RODO) osób, których dane dotyczą,
- wykonywana jest procedura uzyskania kopii danych (art. 15 ust. 3 RODO) osób, których dane dotyczą.

Rodzaje udostępniania:

RODO wyróżnia dwa rodzaje udostępniania danych:

- udostępnianie innemu administratorowi – jeden administrator udostępnia dane drugiemu i każdy z nich wykorzystuje je do realizacji własnych celów (w tym osobie, której dane dotyczą),
- współadministrowanie – współpraca w zakresie wspólnego zarządzania danymi osobowych poprzez stosowne porozumienia.

Rozdział VIII

ZARZĄDZANIE RYZYKIEM

Zarządzanie ryzykiem w odniesieniu do systemów informatycznych służących do przetwarzania danych osobowych ma na celu wykazanie, których ryzyk i jak można uniknąć, stosując przyjęte rozwiązania organizacyjne i techniczne w zakresie przetwarzania danych osobowych oraz jak zminimalizować ryzyka szczątkowe tak, aby stały się ryzykiem akceptowalnym. W tym celu prowadzone są przeglądy ryzyka i bieżące monitorowanie bezpieczeństwa oraz działania tych systemów.

1. Przeglądy ryzyk

Przeglądy ryzyk dokonywane są okresowo, zaś częstotliwość tych przeglądów i okresowe szacowania ryzyka dokonuje się nie rzadziej niż 1 raz na 12 miesięcy.

2. Dodatkowe szacowanie ryzyka

Przewiduje się także dokonywane dodatkowego szacowania ryzyka, które przeprowadzane jest obligatoryjnie, każdorazowo po wystąpieniu naruszenia ochrony danych osobowych oraz w przypadkach istotnych zmian zagadnień zawartych w Polityce bezpieczeństwa.

Dokument Szacowania ryzyka i oceny skutków jest dokumentem odrębnym, wykonanym w 1 egzemplarzu, nie wchodzi w skład Polityki bezpieczeństwa, nie może być publikowany w serwisach internetowych, dostęp do tego dokumentu mają wyłącznie: Administrator danych, Inspektor Ochrony Danych i osoby wskazane przez Administratora danych, przedstawiciele organów kontroli. Dostęp osób nieuprawnionych jest wykluczony.

Rozdział IX

AUDYTY SYSTEMU SŁUŻĄCEGO DO PRZETWARZANIA DANYCH OSOBOWYCH I ZASADY AKTUALIZACJI DOKUMENTACJI

1. Częstotliwości przeprowadzania audytów wewnętrznych

1. Audyt wewnętrzny całościowy przeprowadza się obligatoryjnie:

    a) przed rozpoczęciem eksploatacji systemu informatycznego służącego do przetwarzania danych osobowych,

    b) po wystąpieniu incydentu naruszenia ochrony danych osobowych i usunięciu jego skutków,

    c) po każdej istotnej zmianie dokumentacji bezpieczeństwa przetwarzania danych osobowych.

1. Częstotliwości przeprowadzania całościowych audytów wewnętrznych ustalono na 1 raz na 12 miesięcy podczas eksploatacji systemów informatycznych służących do przetwarzania danych osobowych.
2. Audyt wewnętrzny przeprowadza Inspektor Ochrony Danych we współpracy z Administratorem Systemu Informatycznego wg Zagadnień audytu dla systemów przetwarzających dane osobowe.
3. Wynik audytu jest zatwierdzany przez Administratora danych.
4. Na podstawie wyniku audytu Administrator danych podejmuje decyzję o wstrzymaniu przetwarzania danych osobowych lub dopuszczenia przetwarzania danych osobowych.
5. Audyty częściowe mogą być przeprowadzane przez Inspektora Ochrony Danych we współpracy z Administratorem Systemu Informatycznego wg Zagadnień audytu dla systemów przetwarzających dane osobowe w przypadkach, gdy wykonanie audytu

całościowego jest niekonieczne ze względu na ograniczony obszar funkcjonalny przedmiotu sprawdzenia.

Rozdział X

ODPOWIEDZIALNOŚĆ KARNA I DYSCYPLINARNA

1 **Odpowiedzialność porządkowa i dyscyplinarna**

Pracownicy mają obowiązek postępować zgodnie z RODO, Ustawą o ochronie danych osobowych oraz wewnętrznymi regulacjami (Polityką ochrony danych, Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych).

Przetwarzanie danych sposób sprzeczny z przepisami oraz w sytuacji przetwarzania danych osobowych w zakresie przekraczającym udzielone upoważnienie stanowi naruszenie podstawowych obowiązków pracowniczych i może skutkować karą upomnienia, **nagany lub rozwiązania stosunku prawnego w trybie dyscyplinarnym z winy pracownika.**

2. Odpowiedzialność odszkodowawcza

Jeżeli nieprawidłowe przetwarzanie danych przez pracownika narazi Ośrodek na szkodę – Ośrodek będzie zobowiązany do wypłaty odszkodowania na rzecz osoby fizycznej, której prawa i wolności zostały naruszone na skutek niezgodnego z prawem i procedurami działania pracownika. Jeśli wtedy bezprawność zachowania (wskutek niewykonania lub nienależytego wykonania obowiązków pracowniczych) i wina pracownika zostaną należycie wykazane, **pracownik może zostać pociągnięty do odpowiedzialności materialnej** (odszkodowawczej) – na zasadach ogólnych, w granicach rzeczywistej straty pracodawcy.

3. Odpowiedzialność karna

W przypadku, gdy naruszenie miałoby charakter **umyślnego przestępstwa**, wówczas zastosowanie powinny znaleźć **przepisy karne**, a konkretniej art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), zgodnie z którym: „1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, **podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch**". Natomiast jeśli przetwarzanie dotyczy tzw. danych „wrażliwych" (w tym danych dot. stanu zdrowia, seksualności, danych genetycznych, ujawniających pochodzenie rasowe lub etniczne czy przekonania religijne) **ustawodawca zaostrzył karę pozbawienia wolności do lat trzech** (art. 107 ust. 2).

Załączniki:

- załącznik nr 1 – Schemat przebiegu sieci lokalnej w siedzibie ADO przy ul. Karłowicza 1

- załącznik nr 2 – Schemat przebiegu sieci lokalnej w siedzibie ADO przy Al. Tysiąclecia 5

- załącznik nr 3 - Ewidencja osób upoważnionych do przetwarzania danych osobowych

- załącznik nr 4 - Protokół ustaleń naruszenia ochrony danych osobowych

- załącznik nr 5 - Lista pytań audytu wewnętrznego

- załącznik nr 6 – Wzór sprawozdania

- załącznik nr 7 – Wzór umowy powierzenia