

	CENTRUM ODWYKOWE SP ZOZ	Strona 1 z 23
	Polityka ochrony danych osobowych obowiązująca w Centrum Odwykowym SP ZOZ w Warszawie	Wydanie 1
		Data obowiązywania: od 04.10.2021 r.

ZAŁĄCZNIK nr 1

do Zarządzenia Dyrektora Centrum Odwykowego SP ZOZ Nr 141 z dnia 4 października 2021 r.

**Polityka ochrony danych osobowych obowiązująca
w Centrum Odwykowym
Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej
w Warszawie**

Opracował:	Zatwierdził:
	Dyrektor
Data:	Data:
Podpis i pieczętka:	Podpis i pieczętka:

I. Zagadnienia wstępne i podstawowe definicje

Niniejszą *Politykę* przygotowano celem opisu sposobu przetwarzania danych osobowych w Centrum Odwykowym Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej, z siedzibą w Warszawie przy ul. Zgierskiej 18a. Dokument jest polityką ochrony danych osobowych w rozumieniu *RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 osobowych)* oraz uwzględnia przepisy Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).

1. Cel i zadania Polityki ochrony danych osobowych

Zadaniem niniejszego dokumentu jest opracowanie zadań stanowiących mapę wymogów, zasad i regulacji ochrony danych osobowych, które są zbierane, przetwarzane i gromadzone w Centrum Odwykowym SP ZOZ metodami informatycznymi, jak i tradycyjnymi. Dokument reguluje ponadto zarządzanie przepływem informacji, ochronę oraz dystrybucję informacji wrażliwych, w szczególności danych osobowych, wewnątrz i na zewnątrz Centrum Odwykowego SP ZOZ. Polityka ochrony danych osobowych określa również procedury realizacji praw osób, których dane dotyczą oraz powiadamiania osób odpowiedzialnych za ochronę danych osobowych o sytuacjach stanowiących potencjalne naruszenie danych osobowych.

Celem *Polityki ochrony danych osobowych* w Centrum Odwykowym SP ZOZ jest określenie właściwej strategii zapewniającej poufność, integralność, dostępność i autentyczność informacji, gdzie:

- *poufność* jest rozumiana jako zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym, tzn. nie jest ujawniana nieautoryzowanym podmiotom,
- *integralność* oznacza zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania, oraz tego, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- *dostępność* jest definiowana jako zapewnienie, że osoby upoważnione uzyskują dostęp do informacji i związanych z nią aktywów, gdy jest to potrzebne;
- *autentyczność* oznacza zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak zadeklarowana; autentyczność dotyczy: użytkowników, procesów, systemów i informacji.

2. Zasady bezpiecznego przetwarzanych danych osobowych

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych stosuje się następujące zasady generalne:

- **wiedzy koniecznej** – każdy pracownik posiada dostęp wyłącznie do takich danych osobowych, które są mu niezbędne do realizacji powierzonych obowiązków służbowych,
- **bezwzględnej poufności** – każdy pracownik, który posiada dostęp do danych osobowych ma obowiązek ich ochrony i zachowania w tajemnicy, także po ustaniu stosunku pracy,

- **indywidualnej odpowiedzialności** – każdy pracownik posiada jednoznacznie określony zakres indywidualnej odpowiedzialności za przetwarzane dane osobowe,
- **czystego biurka** – zabronione jest pozostawianie na stanowisku pracy jakichkolwiek dokumentów lub nośników zawierających dane osobowe po zakończeniu dnia pracy lub w trakcie czasowej nieobecności.

3. Zakres obowiązywania

Polityka ochrony danych osobowych w Centrum Odwykowym SP ZOZ odnosi się kompleksowo do problemu ochrony danych osobowych i dotyczy ona wszystkich procesów, w ramach których przetwarzane są dane osobowe niezależnie od sposobu ich gromadzenia. Zasady oraz wytyczne zgromadzone w dokumencie obowiązują wszystkich pracowników oraz współpracowników Centrum Odwykowego SP ZOZ, bez względu na formę zatrudnienia, rodzaj i wymiar czasu wykonywania pracy oraz zajmowane stanowisko.

4. Odpowiedzialność za bezpieczeństwo danych osobowych w Centrum Odwykowym SP ZOZ

Za wdrożenie, utrzymanie i przestrzeganie niniejszej Polityki odpowiedzialny jest Administrator danych (Centrum–Dyrektor Centrum) oraz wyznaczony przez niego Pełnomocnik Dyrektora ds. Bezpieczeństwa Informacji, natomiast nadzór, monitorowanie oraz czynności kontrolne dotyczące przestrzegania *Polityki* wykonuje w ramach swoich uprawnień Inspektor Ochrony Danych.

Za stosowanie niniejszej Polityki odpowiedzialni są:

- Centrum,
- komórka organizacyjna odpowiedzialna za obszar bezpieczeństwa informacji,
- wszystkie jednostki i komórki organizacyjne Centrum Odwykowego SP ZOZ, w ramach których przetwarzane są dane osobowe,
- wszyscy członkowie personelu.

Centrum Odwykowe SP ZOZ powinien także zapewnić zgodność postępowania kontrahentów z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do powierzenia im danych osobowych przez Centrum Odwykowe SP ZOZ.

5. Skróty i definicje

Administrator Danych Osobowych (dalej „ADO”) - rozumie się przez to Centrum Odwykowe Samodzielny Publiczny Zakład Opieki Zdrowotnej (Dyrektor Centrum),

bezpieczeństwo danych - ochrona danych przed nieuprawnioną modyfikacją, zniszczeniem lub ujawnieniem stanu, a także przed niekontrolowanym dostępem,

bezpieczeństwo fizyczne - środki zastosowane w celu fizycznej ochrony zasobów przed zagrożeniem (zniszczeniem),

dane - oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu,

dane osobowe - oznaczają wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby fizycznej („podmiotu danych”),

dane szczególnych kategorii - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej,

dane karne - oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa,

dane dzieci - oznaczają dane osób poniżej 16 roku życia,

dane genetyczne - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej,

dane biometryczne - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne,

eksport danych - oznacza przekazanie danych, w tym do Państwa trzeciego lub organizacji międzynarodowej,

hasło - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

identyfikator użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

Inspektor Ochrony Danych (IOD) - rozumie się przez to osobę, której ADO powierzył pełnienie obowiązków Inspektora Ochrony Danych ,

naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa 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,

osoba dająca się zidentyfikować - oznacza osobę, której tożsamość można określić bezpośrednio lub pośrednio, szczególnie przez odniesienie się do numeru identyfikacyjnego lub innych wskaźników charakterystycznych dla jej fizycznej, fizjologicznej, umysłowej, gospodarczej, kulturowej lub społecznej tożsamości,

Pełnomocnik Dyrektora ds. Bezpieczeństwa Informacji (PBI) - rozumie się przez to osobę, której ADO powierzył pełnienie obowiązków Pełnomocnika Dyrektora ds. Bezpieczeństwa Informacji,

podmiot danych - każda osoba fizyczna, której dane osobowe są przetwarzane ,

podmiot przetwarzający - oznacza organizację lub osobę, której Centrum Odwykowe SP ZOZ powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość, itp.),

Polityka - oznacza niniejszą *Politykę ochrony danych osobowych*, o ile co innego nie wynika wyraźnie z kontekstu,

poufność danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

pracownik - osoba świadcząca pracę na rzecz Centrum Odwykowego SP ZOZ na podstawie stosunku pracy, jak również na innej niż stosunek pracy podstawie prawnej, bez względu na nazwę lub rodzaj łączącej strony umowy,

procesor - osoba prawna, osoba fizyczna, jednostka organizacyjna nie posiadająca osobowości prawnej lub inny podmiot nie decydujący o celach i środkach przetwarzania danych osobowych, z którym Centrum Odwykowe SP ZOZ zawarł umowę powierzenia przetwarzania danych osobowych,

przetwarzanie danych osobowych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza te, które wykonuje się w systemach informatycznych,

pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,

PUODO - Prezes Urzędu Ochrony Danych Osobowych,

RCPD lub Rejestr - oznacza Rejestr Czynności Przetwarzania danych osobowych,

RODO - oznacza rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 roku 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 osobowych).

rozliczalność - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

sieć telekomunikacyjna - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. z 2000 r., Nr 73, poz. 852 ze zm.),

sieć publiczna - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. z 2000 r., Nr 73, poz. 852 ze zm.),

system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

teletransmisja - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

Ustawa – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000),

upoważnienie – jedno z poniższych:

- pisemne upoważnienie do przetwarzania danych osobowych nadane Pracownikowi lub pracownikowi Procesora przez ADO lub osobę posiadającą stosowne pełnomocnictwo,
- umowa powierzenia przetwarzania danych osobowych,

usuwanie danych - zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

zabezpieczenie danych - wdrożenie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

zagrożenia - potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji,

zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda może być odwołana w każdym czasie.

II. Zadania i zakres czynności Inspektora Ochrony Danych

Zadania IOD zostały określone w art. 39 RODO:

1. 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 osobowych i doradzanie im w tej sprawie,
2. monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych osobowych 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,
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 z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Szczegółowe obowiązki wynikające z konieczności realizacji zadań określonych w art. 39 RODO zawiera opis stanowiska IOD, stanowiący integralną część umowy zawartej z IOD.

ADO zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych oraz wspiera go w wypełnianiu przez niego zadań, o których mowa powyżej poprzez zapewnienie mu zasobów niezbędnych do wykonania tych zadań oraz dostępu do danych osobowych i operacji przetwarzania.

Inspektor ochrony danych wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

III. Ogólne zasady Ochrony danych osobowych w Centrum Odwykowym SP ZOZ

1. Filary ochrony danych osobowych :

- a) legalność – oznacza dbanie o ochronę prywatności i przetwarzanie danych zgodnie z prawem,
- b) bezpieczeństwo – oznacza zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych poprzez stałe podejmowanie działań w tym zakresie,
- c) prawa jednostki – oznacza umożliwienie osobom, których dane dotyczą, wykonywanie swoich praw oraz zrealizowanie tych praw,
- d) rozliczalność – oznacza dokumentowanie, w jaki sposób Centrum Odwykowe SP ZOZ spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

2. Zasady ochrony danych osobowych

Centrum Odwykowe SP ZOZ przetwarza dane osobowe z poszanowaniem następujących zasad:

- a) w oparciu o podstawę prawną i zgodnie z prawem (**legalizm**):
 - zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych osobowych i dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania,
 - wskazuje w dokumencie ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel Instytutu). Centrum Odwykowe SP ZOZ dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to konieczne, np. dla zgody wskazując jej zakres, a gdy podstawą jest prawo – wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując konkretny cel, np. dochodzenie roszczeń.
 - wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
- b) rzetelnie i uczciwie (**rzetelność i uczciwość**),
- c) w sposób przejrzysty dla osoby, której dane dotyczą (**transparentność**),
- d) w konkretnych celach i nie na zapas (**minimalizacja**) poprzez wprowadzenie zasad:
 - zarządzania adekwatnością danych,
 - reglamentacji i zarządzania dostępem do danych,
 - zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.
- e) nie więcej niż potrzeba (**adekwatność**),
- f) z dbałością o prawidłowość danych (**prawidłowość**),
- g) nie dłużej niż potrzeba (**czasowość**),
- h) zapewniając odpowiednie bezpieczeństwo danych (**bezpieczeństwo**), np. poprzez:
 - przeprowadzanie analizy ryzyka dla czynności przetwarzania danych,

- przeprowadzanie oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
- dostosowanie środków ochrony danych do ustalonego ryzyka,
- stosowanie procedury pozwalającej na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych osobowych Urzędowi Ochrony Danych – zarządza incydentami i naruszeniami ochrony danych osobowych.

3. System ochrony danych Centrum Odwykowego SP ZOZ

System ochrony danych osobowych składa się z następujących elementów:

1. **Inwentaryzacja danych** - następuje poprzez identyfikację zasobów danych osobowych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja).
2. **Rejestr czynności przetwarzania danych osobowych** - Centrum opracowuje, prowadzi i utrzymuje dokument określający wszystkie czynności, w ramach których przetwarzane są dane osobowe. Rejestr jest narzędziem rozliczania zgodności z ochroną danych.
3. **Obsługa praw jednostki** - Centrum spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
 - a) *obowiązki informacyjne* – Centrum przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.
 - b) *możliwość wykonania żądań* – Centrum weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
 - c) *obsługa żądań* – Centrum zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO.
 - d) *zawiadomienie o naruszeniach* – Centrum stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
4. **Privacy by design** – Centrum Odwykowe SP ZOZ zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów medycznych i inwestycji w Centrum uwzględniają konieczność oceny wpływu zmiany na ochronę danych osobowych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

4. Inwentaryzacja

Centrum Odwykowe SP ZOZ identyfikuje przypadki, w których:

- a) przetwarza lub może przetwarzać dane szczególnych kategorii oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przetwarzania danych szczególnych kategorii lub danych karnych Centrum Odwykowe SP ZOZ postępuje zgodnie z przyjętymi zasadami w tym zakresie,

- b) przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane,
- c) dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Centrum Odwykowe SP ZOZ postępuje zgodnie z przyjętymi zasadami w tym zakresie.

5. Rejestr czynności przetwarzania danych

Rejestr czynności przetwarzania danych stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy procesów przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

W Rejestrze czynności przetwarzania danych, Centrum Odwykowe SP ZOZ inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Rejestr jest jednym z podstawowych narzędzi umożliwiających rozliczenie większości obowiązków ochrony danych osobowych. W dokumencie Centrum Odwykowe SP ZOZ odnotowuje:

- nazwę zbioru,
- nazwę czynności,
- cel przetwarzania,
- opis kategorii osób,
- opis kategorii danych,
- podstawę prawną przetwarzania,
- źródło zbierania danych,
- okres retencji,
- nazwę współadministratora (jeśli dotyczy),
- nazwę podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy),
- kategorię odbiorców (innych niż podmiot przetwarzający),
- nazwę systemu, w którym przetwarzane są dane osobowe,
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,
- ocena skutków dla ochrony danych (jeśli dotyczy)
- prawa dostępne dla osób fizycznych,
- istnienie automatycznego podejmowania decyzji, w tym profilowania (jeśli dotyczy),
- opis kategorii odbiorców danych,
- informacje o przekazywaniu poza EU/EOG.

6. Cele oraz podstawy prawne przetwarzania danych przez administratora

Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel) Centrum Odwykowe SP ZOZ dookreśla

podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Np. dla zgody – wskazując jej zakres, gdy podstawą jest prawo – wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując konkretny cel, np. dochodzenie roszczeń.

Wszyscy kierownicy jednostek, komórek oraz kierownik innej wyodrębnionej jednostki organizacyjnej Centrum Odwykowego SP ZOZ ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych.

a) Dane kontaktowe

Wszystkie dane osobowe zawarte zarówno w korespondencji tradycyjnej jak i elektronicznej oraz zebrane poprzez kontakt telefoniczny kierowane do Centrum Odwykowego SP ZOZ w sprawach nie związanych ze świadczeniem na rzecz nadawcy usługi są przetwarzane wyłącznie w celu komunikacji z nadawcą wiadomości. W takim wypadku podanie określonych danych jest wymagane przez Administratora tylko w przypadku, gdy jest to niezbędne dla powyższego celu, a brak podania takich danych skutkuje brakiem możliwości załatwienia sprawy. W powyższym przypadku podstawą prawną przetwarzania danych jest prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na prowadzeniu korespondencji kierowanej do niego w związku z prowadzoną działalnością gospodarczą.

Centrum Odwykowe SP ZOZ dokłada wszelkich starań, aby ilość przetwarzanych danych w korespondencji była zgodna z zasadą minimalizacji danych i by miały do niej dostęp jedynie osoby uprawnione.

b) Zbieranie danych w związku ze świadczeniem usług lub wykonywaniem innych umów

W razie zbierania danych dla celów związanych z wykonaniem konkretnej umowy, Centrum Odwykowe SP ZOZ przekazuje osobie, której dane dotyczą, szczegółowe informacje dotyczące przetwarzania jej danych osobowych, w momencie zawierania umowy.

7. Odbiorcy danych

W celu zapewnienia sprawnej realizacji zadań w zakresie działalności leczniczej oraz chcąc zapewnić realizację praw pacjentów, Centrum Odwykowe SP ZOZ może przekazywać dane osobowe:

- a) innym podmiotom leczniczym lub podmiotom wykonującym działalność leczniczą, w celu kontynuacji leczenia lub rozliczenia finansowego udzielonego świadczenia,
- b) podmiotom upoważnionym na podstawie przepisów prawa w zakresie niezbędnym do wykonywania przez te podmioty ich zadań,
- c) dostawcom usług zaopatrujących Centrum Odwykowe SP ZOZ w rozwiązania techniczne oraz organizacyjne, umożliwiające udzielanie świadczeń zdrowotnych,
- d) audytorom, kontrolerom lub podmiotom upoważnionym z mocy przepisów prawa do dokonywania kontroli udzielonych świadczeń medycznych lub dokumentacji medycznej,
- e) kancelariom prawnym i firmom doradczym współpracującym z Centrum Odwykowym SP

ZOZ,

- f) właściwym organom bądź osobom trzecim w wypadku, gdy żądając ujawnienia takich informacji powołają się one na odpowiednią podstawę prawną oraz będzie to zgodne z przepisami obowiązującego prawa.

8. Okres przetwarzania danych osobowych

Centrum Odwykowe SP ZOZ przetwarza dane osobowe przez okres zgodny z przepisami ustaw oraz w zależności od celu przetwarzania:

- a) *Niezbędność do zawarcia i wykonania umowy* - dane osobowe będą przetwarzane do momentu jej zakończenia.
- b) *Zgoda* - do czasu jej wycofania.
- c) *Uzasadniony interes Administratora* - dane osobowe przetwarzane są przez okres umożliwiający jego realizację lub do zgłoszenia skutecznego sprzeciwu.
- d) *Ochrona przed roszczeniami* – dane osobowe będą przetwarzane przez okresy przedawnienia roszczeń cywilnoprawnych, tj. maksymalnie przez 3 lata dla roszczeń o świadczenia okresowe oraz roszczeń związanych z prowadzeniem działalności gospodarczej oraz 6 lat dla roszczeń majątkowych.
- e) *Dokumentacja medyczna* – dane osobowe ujęte w dokumentacji medycznej są przechowywane przez 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu z wyjątkiem:
 - **30 lat** w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia. Termin liczony jest od końca roku kalendarzowego, w którym nastąpił zgon.
 - **30 lat** w przypadku dokumentacji medycznej zawierającej dane niezbędne do monitorowania losów krwi i jej składników. Termin liczony jest od końca roku kalendarzowego, w którym dokonano ostatniego wpisu.
 - **10 lat** w przypadku zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną pacjenta. Termin liczony jest od końca roku kalendarzowego, w którym wykonano zdjęcie.
 - **5 lat** w przypadku skierowań na badania lub zleceń lekarza. Termin liczony jest od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza.
 - **2 lata** w przypadku skierowań na badania lub zleceń lekarza. Termin liczony jest od końca roku kalendarzowego, w którym wystawiono skierowanie – w przypadku gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie.
 - **22 lata** w przypadku dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia.

W wypadku upływu okresu retencji dane osobowe są niezwłocznie usuwane lub anonimizowane.

9. Realizacja praw osób, których dane dotyczą

Realizując prawa osób, których dane dotyczą, Centrum Odwykowe SP ZOZ wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, dobra osobiste), Centrum może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu. W przypadku odmowy osoba, której dane dotyczą, jest informowana o decyzji i o prawach osoby z tym związanych w ciągu miesiąca od otrzymania żądania.

1. *Dostęp do danych* - na żądanie osoby dotyczące dostępu do jej danych Centrum Odwykowe SP ZOZ informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonywaniu prawa dostępu do danych Centrum nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.
2. *Wydanie kopii dokumentacji medycznej* – działania jakie należy podjąć w przypadku otrzymania wniosku o wydanie kopii dokumentacji medycznej zostały opisane w Instrukcji dot. udostępniania dokumentacji medycznej.
3. *Sprostowanie danych* – Centrum Odwykowe SP ZOZ dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Centrum Odwykowe SP ZOZ ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Centrum Odwykowe SP ZOZ informuje osobę o odbiorcach danych, na żądanie tej osoby.
4. *Uzupełnienie danych* - Centrum uzupełnia i aktualizuje dane na żądanie osoby. Centrum ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Centrum nie musi przetwarzać danych, które są zbędne). Centrum może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
5. *Usunięcie danych* - na żądanie osoby Centrum Odwykowe SP ZOZ usuwa dane, gdy:
 - dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
 - zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
 - osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
 - dane były przetwarzane niezgodnie z prawem,
 - konieczność usunięcia danych wynika z obowiązku prawnego,

Centrum Odwykowe określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO. Jeżeli dane podlegające usunięciu zostały upublicznione przez Centrum, Centrum podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Centrum Odwykowe informuje osobę o odbiorcach danych, na żądanie tej osoby.

6. *Ograniczenie przetwarzania* - Centrum Odwykowe dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich przetwarzania,
- nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony przed roszczeniami,
- osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, po stronie Centrum zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W takiej sytuacji Centrum Odwykowe informuje osobę o odbiorcach danych, na żądanie tej osoby. W trakcie ograniczenia przetwarzania Centrum Odwykowe przechowuje dane, natomiast nie przetwarza ich w inny sposób (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony przed roszczeniami lub w celu ochrony praw innej osoby fizycznej lub prawnej lub z uwagi na ważne względy interesu publicznego. W przypadku uchylecia ograniczenia przetwarzania danych przez Centrum osoba, której dane dotyczą, zostanie uprzednio o tym poinformowana.

7. *Przenoszenie danych* - na żądanie osoby, Centrum wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane dotyczące tej osoby lub przekazuje innemu podmiotowi, jeśli jest to możliwe.

8. *Sprzeciw w szczególnej sytuacji* - jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Centrum w oparciu o uzasadniony interes Centrum Odwykowe lub powierzone zadanie w interesie publicznym, Centrum uwzględni sprzeciw, o ile nie zachodzą po jego stronie ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony przed roszczeniami.

9. *Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych* – osoba, której dane dotyczą może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Centrum Odwykowe uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

10. *Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu* – systemy informatyczne służące do przetwarzania danych osobowych w Centrum Odwykowym nie posiadają mechanizmu profilowania.

Wszystkie prośby o realizację poszczególnych praw należy kierować:

- a. listownie na adres: ul. Zgierska 18a, 04-092 Warszawa
- b. lub drogą elektroniczną na adres: niejestessam@wp.pl

Odpowiedź na zgłoszenia powinna być udzielona w ciągu miesiąca od jego otrzymania. W razie konieczności przedłużenia tego terminu, Administrator informuje wnioskodawcę o przyczynach takiego przedłużenia.

10. Minimalizacja

1. Centrum Odwykowe SP ZOZ dba o minimalizację przetwarzanych danych pod kątem:

- adekwatności danych do celów (ilości danych i zakresu przetwarzania),
- dostępu do danych,
- czasu przechowywania danych.

Na tej podstawie Centrum zweryfikowało zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

2. Centrum dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok oraz przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (Privacy by design).
3. Minimalizacja dostępu w Centrum następuje poprzez ograniczenia dostępu do danych osobowych: prawne (zobowiązania do zachowania poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykane pomieszczenia) i logiczne (ograniczanie uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
4. W Centrum stosuje się kontrolę dostępu fizycznego do obszarów przetwarzania danych osobowych oraz dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających. Ponadto okresowo przeglądane w systemach są ustanowieni użytkownicy. Ewentualne niezgodności są aktualizowane. Czynności te są podejmowane nie rzadziej już raz na rok.

11. Bezpieczeństwo

Centrum Odwykowe SP ZOZ zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych poprzez cykliczne przeprowadzanie analizy ryzyka i adekwatności środków bezpieczeństwa danych osobowych. W tym celu Centrum:

- a) zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyber-bezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
- b) kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

- c) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.
- d) analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
- e) ustala możliwe do zastosowania organizacyjne i technologiczne środki bezpieczeństwa i ocenia koszt ich wdrożenia.
- f) dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka – ryzyko naruszenia praw i wolności osób jest wysokie.

Centrum Odwykowe stosuje metodykę oceny skutków oraz stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

12. Szkolenia i zapoznawanie pracowników z zasadami ochrony danych osobowych

Przed przystąpieniem do wykonywania czynności związanych przetwarzaniem danych osobowych, każdy nowy pracownik jest zaznajamiany z tym jakie powszechne przepisy prawa oraz wewnętrzne uregulowania obowiązują w Centrum Odwykowym SP ZOZ. Za dopilnowanie, aby pracownik zapoznał się z wszystkimi wymaganiami dot. ochrony danych osobowych odpowiada jego przełożony. Informacje o zapoznaniu się z obowiązującymi w Centrum Odwykowym SP ZOZ zasadami dotyczącymi ochrony danych osobowych oraz zobowiązanie do ich przestrzegania jest udokumentowane pisemnym oświadczeniem pracownika.

13. Działania korygujące i zapobiegawcze

1. Inicjowanie działań korygujących lub zapobiegawczych związanych z wystąpieniem zagrożeń lub naruszeń bezpieczeństwa danych osobowych należy do obowiązków IOD.
2. Decyzja o podjęciu działań, o których mowa powyżej może opierać się w szczególności na informacjach przekazywanych przez pracowników, podmioty przetwarzające, w wyniku kontroli lub informacjach pozyskanych samodzielnie przez IOD.
3. W przypadku stwierdzenia konieczności podjęcia działań korygujących, IOD wskazuje:
 - a) osobę odpowiedzialną za określenie przyczyn powstania naruszenia lub zagrożenia naruszenia obowiązujących standardów,
 - b) zakres niezbędnych działań korekcyjnych,
 - c) termin realizacji powyższych działań.
4. IOD nadzoruje poprawność i terminowość prowadzenia działań korekcyjnych, jak również dokonuje oceny skuteczności i prawidłowości ich zastosowania.

IV. Postanowienia końcowe

1. Niniejsza Polityka stanowi regulację wewnętrzną Centrum Odwykowego Samodzielnego

Publicznego Zakładu Opieki Zdrowotnej z siedzibą w Warszawie przy ul. Zgierskiej 18a..

2. Centrum Odwykowe SP ZOZ udostępnia Politykę w siedzibie Zakładu w zwyczajowo przyjęty sposób, tak aby umożliwić Pracownikom oraz podmiotom przetwarzającym wgląd do Polityki w każdym możliwym czasie.
3. Wszelkie regulacje zawarte w Polityce, a dotyczące przetwarzania danych osobowych w systemie informatycznym, mają odpowiednie zastosowanie do przetwarzania danych osobowych w każdej innej formie, w tym w szczególności w zbiorach papierowych.
4. Pracownicy zobowiązani są do przestrzegania zasad niniejszej Polityki.
5. Naruszenie obowiązków wynikających z niniejszej Polityki traktowane będzie jako ciężkie naruszenie obowiązków pracowniczych, a także może stanowić podstawę odpowiedzialności dyscyplinarnej, natomiast w przypadku Procesorów - jako brak należytego wykonania zawartej umowy cywilnej.
6. W sprawach nieuregulowanych w niniejszym dokumencie zastosowanie mają odpowiednie przepisy Ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
7. Niniejsza Polityka zostaje wprowadzona Zarządzeniem Dyrektora Centrum Odwykowego Samodzielnego Publicznego Zakładu Opieki Zdrowotnej nr 141/2021 i obowiązuje od dnia 04.10.2021 r.
8. Wszelkie zmiany w niniejszej polityce będą wprowadzane w życie w formie Aneksu.