Załącznik nr 15 – POLITYKA OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych w Szpitalu Chorób Płuc w Siewierzu Sp. z o.o.

Celem Polityki ochrony danych osobowych, zwanej dalej Polityką jest wprowadzenie i utrzymanie wymaganej przez przepisy rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. oraz ustawy o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) właściwej ochrony danych osobowych w związku z przetwarzaniem danych osobowych w **Szpitalu Chorób Płuc w Siewierzu Sp. z o.o.**

Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych. Dotyczy istniejących oraz przetwarzanych w przyszłości zbiorów danych osobowych. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

W skład obszaru przetwarzania danych osobowych w **Szpitalu Chorób Płuc w Siewierzu Sp. z o.o.** wchodzą budynki i/lub lokale położone w **Siewierzu, przy ul. Zbigniewa Oleśnickiego 21**

Określenia użyte w Polityce ochrony danych osobowych oznaczają:

1. Administrator danych osobowych (ADO)- **Szpital Chorób Płuc w Siewierzu Sp. z o.o.**,
2. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwe do zidentyfikowania osoby fizycznej,
3. przetwarzanie danych osobowych – gromadzenie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4. użytkownik – osoba upoważniona do przetwarzania danych osobowych,
5. system informatyczny – system (urządzenia, narzędzia, programy), w którym przetwarzane są dane osobowe,

6. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą,
8. RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
9. ustawa o ochronie danych osobowych – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

1. Zasady przetwarzania danych osobowych 1.1.

Administrator danych przetwarza dane osobowe:

- zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”),
- zbiera je w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami („ograniczenie celu”),
- adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”),
- prawidłowo i w razie potrzeby uaktualnia zebrane dane („prawidłowość”),
- przechowuje je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”),
- 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 („integralność i poufność”).

1.2.

W celu realizacji tych zasad administrator danych przetwarza dane legalnie, na podstawie przesłanek opisanych w art. 6 RODO. Pobiera dane osobowe adekwatnie do celów przetwarzania i przetwarza je przez określony czas. Wobec osób, których dane przetwarza wypełnia obowiązki informacyjne określone w art. 13 RODO lub w art. 14 RODO (gdy informacje pobierane są w sposób inny niż od osoby, której dane dotyczą) oraz wskazuje przysługujące im uprawnienia takie jak prawo do:

- dostępu do danych,
- sprostowania danych,
- usunięcia danych (prawo do bycia zapomnianym),
- przenoszenia,
- sprzeciwu wobec przetwarzania,
- ograniczenia przetwarzania,
- wniesienia skargi do organu nadzorczego,
- sprzeciwu wobec bycia profilowanym.

Administrator danych zapewnia ochronę danych w przypadku korzystania z usług podmiotów zewnętrznych w postaci zawierania stosownych umów powierzenia oraz korzystając z usług podmiotów przetwarzających realizujących obowiązki wynikające z RODO. W razie wystąpienia incydentu technicznego lub fizycznego administrator danych zapewnia zdolność do szybkiego przywrócenia dostępności do danych osobowych i dostępu do nich.

1.3.

Potwierdzenie spełniania obowiązków informacyjnych przez administratora danych stanowią klauzule informacyjne przekazywane osobom, których dane są przetwarzane. W przypadku pracowników przedstawia się im klauzule do podpisania i zamieszcza w aktach osobowych pracowników.

W przypadku klientów i kontrahentów przekazywane im są w momencie zawierania umowy, umieszczane razem z umową, oraz są również umieszczane w widocznym miejscu na stronie **www.szpital-siewierz.pl**

2. Upoważnienia do przetwarzania danych

Administrator danych zapewnia, aby dostęp do danych osobowych w **Szpitalu Chorób Płuc w Siewierzu Sp. z o.o.** miały tylko osoby legitymujące się nadanym przez ADO upoważnieniem. Upoważnienia określają do jakich operacji użytkownicy są uprawnieni, tj. tworzenia, usuwania, wglądu, przekazywania danych, w jakich systemach oraz na jaki czas. Administrator danych prowadzi ewidencję osób upoważnionych. Upoważnienia do przetwarzania danych osobowych mogą być nadawane na wniosek bezpośredniego przełożonego użytkownika systemu.

3. Analiza ryzyka

Administrator danych prowadzi analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń. Analiza prowadzona jest w przypadku zaistnienia zagrożenia oraz cyklicznie co 12 miesięcy

Analiza danych prowadzona jest osobno dla każdego zbioru danych lub dla kilku zbiorów o podobnym zakresie danych. W przypadku konieczności przeprowadza się ocenę skutków dla oceny ryzyka na mocy art. 35 RODO.

4. Wykaz zabezpieczeń

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

5. Rejestr czynności przetwarzania

Administrator danych prowadzi rejestr czynności przetwarzania. W rejestrze tym zamieszcza się:

1. imię i nazwisko oraz dane kontaktowe administratora,
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, informacje na temat przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację 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.

6. Powołanie inspektora ochrony danych

Administrator Danych Osobowych może być/jest zobowiązany powołać inspektora ochrony danych. W przypadku powołania inspektora ochrony danych do jego zadań należą:

• informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów RODO oraz ustawy o ochronie danych osobowych,

• monitorowanie przestrzegania przepisów RODO oraz ustawy o ochronie danych osobowych oraz Polityki ochrony danych obowiązującej w jednostce, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
- współpraca z organem nadzorczym, tj. Prezesem Urzędu Ochrony Danych Osobowych,

- 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. W przypadku wyznaczenia inspektora ochrony danych należy zgłosić jego powołanie Prezesowi Urzędu Ochrony Danych Osobowych w terminie 14 dni od dnia wyznaczenia, wskazując imię nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

7. Procedura postępowania z incydentami

Administrator danych wprowadza do stosowania procedurę postępowania z incydentami naruszenia ochrony danych osobowych. Celem tej procedury jest wypełnienie obowiązku wynikającego z art. 33 RODO. Procedura określa sposób definiowania incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie, a także procedurę wprowadzenia działań naprawczych. Każda osoba upoważniona do przetwarzania danych osobowych ma obowiązek poinformowania o możliwości wystąpienia incydentu lub o jego wystąpieniu. Taka informacja powinna być przekazana Inspektorowi Danych Osobowych.

Powiadomienia wymagają:

- niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych, udostepnienie haseł osobom postronnym,
- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, przyklejanie kartek z hasłami w szufladach),
- ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
- dokumentacja zawierająca dane osobowe niszczona bez użycia niszczarki,
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,

- obecność osób postronnych w jednostce,
- złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz jednostki bez upoważnienia administratora danych,
- awarie serwera, komputerów, twardych dysków, oprogramowania,
- udostepnienie danych osobowych osobom nieupoważnionym,
- telefoniczne próby wyłudzenia danych osobowych,
- kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi,
- maile nakłaniające do ujawnienia identyfikatora lub hasła,
- zainfekowanie komputerów wirusem lub inne błędne zachowanie komputerów,
- zdarzenia losowe (pożar obiektu, zalanie wodą, utrata zasilania, utrata łączności),
- włamanie do systemu informatycznego lub pomieszczeń,
- kradzież danych/sprzętu,
- świadome zniszczenie dokumentów.

Należy również powiadomić administratora systemów informatycznych. Ponadto należy udokumentować wystąpienie incydentu, jego skutki oraz podjęte działania naprawcze i zaradcze. W przypadku gdy incydent skutkuje naruszeniem praw lub wolności osób fizycznych, administrator danych zgłasza je w ciągu 72 godzin Prezesowi Urzędu Ochrony Danych Osobowych oraz gdy istnieje taki wymóg, powiadamia o tym fakcie osoby, których incydent dotyczył.

8. Regulamin ochrony danych osobowych i szkolenia wewnętrzne

Administrator danych wprowadza w **Szpitalu Chorób Płuc w Siewierzu Sp. z o. o.**

Regulamin ochrony danych osobowych w celu zapewnienia osobom przetwarzającym dane osobowe pełny zakres wiedzy na temat zasad przetwarzania danych osobowych

w jednostce oraz obciążających je obowiązków z tym związanych. Osoby zapoznane z Regulaminem zobowiązane są potwierdzić fakt zapoznania się z tym dokumentem oraz zdeklarować stosowanie się do jego zasad. Każda osoba przed zatrudnieniem powinna zostać zapoznana z Regulaminem. Administrator danych zapewnia również przeszkolenie pracowników z zakresu stosowania przepisów dotyczących ochrony danych osobowych, a obecność pracowników należy potwierdzić pisemnie.

9. Zadania Administratora systemu informatycznego

Administrator systemu informatycznego realizuje zadania w zakresie zarzadzania i bieżącego nadzoru nad systemem informatycznym administratora danych. W związku z tym:

- zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych i serwera z pozycji administratora,
- przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
- przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych,
- przeprowadza szkolenie stanowiskowe użytkownika w zakresie korzystania ze sprzętu komputerowego i zasobów sieci, zapoznaje z obowiązującymi w tym zakresie dokumentami,
- nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych, w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora danych/inspektora ochrony danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
- prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,

- sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego, podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

10. Umowy powierzenia przetwarzania danych osobowych 10.1.

W przypadku zlecania przetwarzania danych osobowych podmiotom zewnętrznym administrator danych zobowiązany jest zawrzeć umowę powierzenia. W jednostce prowadzony jest rejestr umów powierzenia przetwarzania danych osobowych.

10.2.

Umowa określa kategorie osób, których dane dotyczą obowiązki i prawa administratora. Ponadto zobowiązuje podmiot przetwarzający do:

1. przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora – co dotyczy tez przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
2. zapewniania, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
3. podejmowania wszelkich środków wymaganych na mocy art. 32 RODO,
4. przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego,
5. pomagania administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie

   wykonywania jej praw określonych w rozdziale III RODO,

6. pomagania administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO,
7. usuwania lub zwracania administratorowi danych osobowych oraz usuwania wszelkich istniejących kopii, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,
8. udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w przepisach RODO oraz umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji, i przyczynia się do nich.

11. Czynności kontrolne

Nadzór i kontrolę nad ochroną danych osobowych sprawuje Administrator Danych.

Czynności kontrolne przeprowadzane są raz do roku.

Z czynności kontrolnych sporządza się protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynność, a także zalecenia i działania naprawcze. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne.

12. Odpowiedzialność osób upoważnionych do przetwarzania danych

Niezastosowanie się do prowadzonej przez administratora danych Polityki ochrony danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.