

Regulamin Ochrony danych Osobowych
w Wojewódzkim Specjalistycznym Szpitalu Dziecięcym im. św. Ludwika w Krakowie

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

1	Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT	2
2	Zasady korzystania z oprogramowania	2
3	Zasady korzystania z internetu	2
4	Zasady korzystania z poczty elektronicznej.....	3
5	Ochrona antywirusowa	5
6	Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych.....	5
7	Polityka haseł	6
8	Procedura rozpoczęcia, zawieszenia i zakończenia pracy	6
9	Praca w systemie	7
10	Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe	7
11	Postępowanie z danymi osobowymi w wersji papierowej.....	8
12	Zapewnienie poufności danych osobowych	8
13	Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.....	9
14	Procedura monitoringu wizyjnego	10
15	Obowiązek informacyjny.....	12
16	Szkolenie wstępne RODO.....	19
17	Postępowanie dyscyplinarne.....	32

1 Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony
2. Użytkownik zobowiązany jest korzystać ze Sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem
3. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – **tw. Polityka czystego ekranu**
4. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOS + L) lub wylogować się z systemu bądź z programu.
5. Użytkownik zobowiązany jest do zabezpieczenia Sprzętu IT przed dostępem osób nieupoważnionych a w szczególności zawartości ekranów monitorów
6. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT
7. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

2 Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę / Zleceniodawcę na swoje własne potrzeby ani na potrzeby osób trzecich
3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Szpital. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną
6. W przypadku naruszenia któregoś z powyższych postanowień Pracodawca / Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie

3. Zasady korzystania z internetu

1. Dostęp do Internetu odbywa się za pośrednictwem sprzętu i oprogramowania dostarczonego przez Szpital z określonych stacji roboczych. Zabronione jest

- zestawianie indywidualnych połączeń z Internetem przez poszczególnych pracowników przy wykorzystaniu modemów lub innych urządzeń dostępowych
2. Działania Pracodawcy zmierzające do poprawy jakości pracy z komputerem polegające w szczególności na eliminowaniu możliwości pobierania określonych danych z internetu, odciążeniu sieci informatycznej poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnie zainstalowanego oprogramowania, blokowaniu dostępu do treści oraz kontroli antywirusowej, nie wymagają zgody użytkownika
 3. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych
 4. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Inspektora Ochrony Danych i tylko w uzasadnionych przypadkach.
 5. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu
 6. Przy korzystaniu z internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
 7. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)
 8. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł
 9. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:"
 10. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie dotyczy się to żądania podania takich informacji przez rzekomy bank.
 11. W zakresie dozwolonym przepisami prawa, Pracodawca / Zleceniodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z internetu pod kątem wyżej opisanych zasad.

4. Zasady korzystania z poczty elektronicznej

1. Poczta jest udostępniana pracownikom wyłącznie do wypełniania obowiązków służbowych. Dozwolone jest okazjonalne korzystanie z poczty do celów prywatnych i powinno być to ograniczone do niezbędnego minimum.
2. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych
3. Zabronione jest wykorzystywanie prywatnej poczty elektronicznej (prywatnego adresu e-mail) do celów służbowych.
4. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione

5. W przypadku przesyłania informacji wrażliwych oraz wszelkich danych osobowych poza organizację (pocztą zewnętrzną) należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików)
6. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
7. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
8. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata
9. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę
10. **WAŻNE:** Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu” infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy
11. **WAŻNE:** Bez weryfikacji wiarygodności nadawcy, nie należy „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając” na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy
12. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia”, itp.
13. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze
14. Użytkownicy powinni okresowo kasować niepotrzebne maile
15. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW” Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”!
16. Użytkownicy odbierają pocztę co najmniej na początku i końca dnia pracy
17. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób
18. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
19. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
20. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania
21. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

5. Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym dostępnym na stacjach roboczych
2. Zabrania się użytkownikom wyłączania lub ograniczania w jakikolwiek sposób działania programu antywirusowego
3. W przypadku stwierdzenia pojawienia się wirusa lub zatrzymania działania programu antywirusowego, każdy użytkownik powinien powiadomić ASI

6. Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby upoważnione.
2. Za nadawanie upoważnień odpowiada IOD.
3. Przyznanie, anulowanie, zmiana upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym wraz z uprawnieniami do przetwarzania tych danych realizowane jest na podstawie rejestrów osób zatrudnionych (pliki EXEL) uaktualnianych na bieżąco przez Dział Kadr, Dział Umów i Zamówień Publicznych, karty obiegu, karty stażu/praktyki lub pisemny wniosek Przełożonego/Kierownika komórki organizacyjnej. Macierz uprawnień do zasobów informatycznych Szpitala stanowią załączniki do Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych (Z5A-I/1-S/ZI1, Z5B-I/1-S/ZI1). Dokument ten opisuje uprawnienia standardowo przypisane użytkownikowi na danym stanowisku pracy. Standardowe uprawnienia dla użytkowników do poszczególnych systemów/aplikacji znajdujące się w macierzy uprawnień są ustalane z Kierownikami komórek organizacyjnych/Przełożonymi. Dział Informatyki i w przypadku stażystów odpowiedni pracownik Działu Kadr dokonuje odwzorowania uprawnień w systemach informatycznych tworząc odpowiednie grupy uprawnień w poszczególnych systemach/aplikacjach do których przypisywani są użytkownicy. Przełożony/Kierownik komórki organizacyjnej może wnioskować o zwiększenie, zmniejszenie poziomu uprawnień dla poszczególnych użytkowników. Wzór takiego wniosku stanowi załącznik nr 6 do Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych (Z6-I/1-S/ZI1).
4. Każdy użytkownik systemu przed nadaniem upoważnienia musi zapoznać się z:
 - a. niniejszym regulaminem
 - b. przepisami Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.
 - c. obowiązującymi w Szpitalu regulacjami dotyczącymi ochrony danych osobowych
 - d. w przypadku osoby, która będzie miała dostęp do systemów lub zasobów teleinformatycznych Platformy MSIM, dodatkowo z Polityką

Bezpieczeństwa dla Partnerów i wymaganiami bezpieczeństwa w ramach działania Platformy MSIM.

- e. podpisać Oświadczenie o poufności
- 5. Upoważnienie nadawane jest do zbiorów w wersji papierowej i elektronicznej
- 6. W przypadku, gdy upoważnienie udzielane jest do zbioru w wersji elektronicznej, nadawany jest użytkownikowi identyfikator w systemie
- 7. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login).
- 8. W przypadku anulowania upoważnienia, identyfikator użytkownika jest blokowany w systemie.

7. Polityka haseł

- 1. Hasło dostępu do zbioru danych (jakakolwiek aplikacja, komputer, za pomocą którego mamy dostęp do danych osobowych) składa się co najmniej z **12** znaków (**minimum trzech** z dużych i małych liter oraz z cyfr lub znaków specjalnych)
- 2. Zmiana hasła do systemu następuje nie rzadziej, niż co 60 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione
- 3. Jeżeli zmiany hasła nie wymusza system, wówczas do zmiany hasła zobowiązany jest użytkownik
- 4. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło
- 5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów, loginów, ani powyższych z doklejonymi na końcu cyframi.
- 6. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności
- 7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom

8. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

- 1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabrania się pracy wielu użytkowników na wspólnym koncie.
- 2. Użytkownik jest zobowiązany do powiadomienia ASI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje
- 3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi
- 4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wgląd do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu
- 5. Przed czasowym opuszczeniem stanowiska pracy w przypadku użytkownika logującego się do komputera za pomocą indywidualnego loginu (czyli użytkownika mającego dostęp do „katalogu domowego użytkownika”), użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie **10** minut

system automatycznie aktywuje wygaszacz. W przypadku pozostałych użytkowników, użytkownik jest zobowiązany zablokować lub wylogować się z aplikacji przetwarzającej dane.

6. Po zakończeniu pracy, użytkownik zobowiązany jest:
 - a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
 - b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe

9. Praca w systemie

1. Zabrania się użytkownikom samodzielnie instalować żadnego oprogramowania własnego lub dostarczonego przez osoby trzecie, pobranego z internetu, niezależnie od sposobu w jaki zostało nabyte. Instalacji w/w oprogramowania dokonuje ASI lub osoba przez niego upoważniona po uzyskaniu uprzedniej zgody
2. Zabrania się użytkownikom zapisywania na komputerach, laptopach, pamięciach przenośnych jakichkolwiek dokumentów w postaci plików Worda, Excela, OpenOffice, Adobe itp. zawierających dane osobowe, medyczne pacjentów. Dane te należy wpisywać bezpośrednio w system informatyczny Szpitala. Zakaz w stosunku do komputerów i laptopów nie dotyczy użytkowników logujących się do komputera za pomocą indywidualnego loginu i hasła.

10. Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Elektroniczne nośniki, to: Wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash
2. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych)
3. Zabrania się wnoszenia poza obszar Szpitala wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi i pendrive bez zgody ADO
4. Dane osobowe wnoszone poza obszar Szpitala na nośnikach elektronicznych muszą być zaszyfrowane
5. W sytuacji przekazywania nośników z danymi osobowymi poza obszar Szpitala można stosować następujące zasady bezpieczeństwa:
 - a. adresat powinien zostać powiadomiony o przesyłce
 - b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą
 - c. stosować bezpieczne koperty depozytowe
 - d. przesyłkę należy przesyłać przez kuriera
 - e. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji Administratora Bezpieczeństwa Informacji
6. Należy korzystać ze sprawdzonych firm kurierskich

7. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą
8. Osoby wykorzystujące nośniki zobowiązane są do niezwłocznego i trwałego usuwania (kasowania) danych osobowych po ustaniu celu ich przechowywania (chyba, że z powodu odrębnych przepisów należy dane zachowywać). Trwałego zniszczenia nośników CD/DVD (dotyczy to także tych, które zdaniem użytkownika nie zostały nagrane poprawnie można dokonać w Dziale informatyki w przeznaczony do tego niszczenie. Pozostałe nośniki należy przekazać do Działu informatyki celem zniszczenia i utylizacji.
9. Osoby wykorzystujące elektroniczne nośniki z danymi osobowymi są zobowiązane do zabezpieczenia ich (w szafach, biurkach) przed dostępem osób nieupoważnionych, szczególnie poza godzinami pracy (tzw. Polityka czystego biurka)

11. Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz kierownicy właściwych jednostek organizacyjnych
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych
3. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka”. Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
4. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie
5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczeniach niezwłocznie po ustaniu celu ich przetwarzania

12. Zapewnienie poufności danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
 - a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę / Zleceniodawcę zadaniach
 - b. zachowania w tajemnicy danych osobowych do których mam lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę / Zleceniodawcę
 - c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę / Zleceniodawcę
 - d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
 - e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem

2. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności
3. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
4. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych

13. Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Inspektora Ochrony Danych w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych
2. Do sytuacji wymagających powiadomienia, należą:
 - a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
 - b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
 - c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurka)
3. Do incydentów wymagających powiadomienia, należą:
 - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
 - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twarde dyski, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
 - c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. Typowe przykłady incydentów wymagające reakcji:
 - a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania
 - b. dokumentacja jest niszczone bez użycia niszczarki
 - c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
 - d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe
 - e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
 - f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy
 - g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej

- h. telefoniczne próby wyłudzenia danych osobowych
- i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi
- j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
- k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
- l. hasła do systemów przyklejone są w pobliżu komputera

14.Procedura monitoringu wizyjnego

1. Monitoring stosowany jest w celu zapewnienia bezpieczeństwa i porządku publicznego, wspomagania nadzoru medycznego nad pacjentem na oddziałach szpitalnych oraz dla poprawy ochrony osób i mienia, znajdujących się na terenie Szpitala, poprzez umożliwienie obserwacji obrazów z kamer oraz ich rejestracji.
2. System monitoringu wizyjnego został wdrożony tak, aby zachować równowagę pomiędzy prawem do poszanowania godności, intymności i prywatności osób przebywających na terenie Szpitala, a prawnie uzasadnionym interesem podmiotu leczniczego.
3. Administratorem systemu monitoringu jest Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31-503 Kraków
4. Monitoring wizyjny z zapisem obrazu obejmuje miejsca ogólnodostępne: korytarze szpitalne, tereny na zewnątrz wokół obiektów, głównie parkingi i bramy wjazdowe na teren jednostki. Monitoring nie obejmuje ulic wokół szpitala oraz sąsiednich posesji graniczących ze szpitalem.

Monitoring wizyjny bez zapisu obrazu obejmuje: pokoje łóżkowe, salę operacyjną, salę intensywnej terapii. Obrazy z kamer nie są nagrywane, lecz przekazywane na żywo do stanowisk pielęgniarskich/lekarskich w celu zapewnienia bezpieczeństwa oraz wspomagania obserwacji pacjentów przez personel medyczny Szpitala.

Dane z systemu monitoringu obejmują:

-czas i miejsce zdarzeń objętych monitoringiem

-wizerunki osób oraz sposoby zachowania osób, których wizerunek utrwalono na urządzeniu rejestrującym

- numery rejestracyjne samochodów, oznaczenia boczne samochodów w przypadku monitorowania parkingów.

5. Monitoring nie obejmuje pomieszczeń higieniczno – sanitarnych, socjalnych, szatni, przebieralni, pomieszczeń udostępnionych zakładowym organizacjom związków zawodowych, miejsc udzielania świadczeń zdrowotnych za wyjątkiem dozwolonych przepisami prawa.
6. System monitoringu wizyjnego obejmuje zestaw kamer wewnątrz i na zewnątrz budynku, rejestrator, oprogramowanie do obserwacji zapisów, odtwarzania

oraz kopiowania nagrań.

7. Monitoring pozostaje aktywny przez całą dobę.
8. Kamery nie rejestrują dźwięku.
9. Urządzenia rejestrujące obraz znajdują się w zabezpieczonych pomieszczeniach.
10. Zapisane obrazy z monitoringu przechowywane są przez okres 3 dni, a po jego upływie automatycznie kasowane (nadpisywane) przez system, tzn. całkowicie i bezpowrotnie niszczone. Jeżeli w obiektach szpitala lub na zewnątrz doszło do zdarzenia, które można nazwać niepożądanym lub nawet przestępstwem, o którym administrator systemu poweźmie wiadomość w okresie tych 3 dni, to sporządzana jest kopia zapisanych obrazów dla potrzeb osób prowadzących postępowanie wyjaśniające lub organów prowadzących dochodzenie.
11. Do podglądu zapisanych obrazów upoważnione są tylko określone osoby z pośród pracowników i współpracowników Szpitala, posiadający upoważnienie do przetwarzania danych osobowych osób objętych monitoringiem wizyjnym, w związku z wykonywaniem obowiązków służbowych lub świadczeniem usług na zlecenie Szpitala oraz dostawcy usług technicznych i organizacyjnych dla Szpitala (w szczególności dostawcy i podmioty wyspecjalizowane w zapewnieniu obsługi technicznej systemów teleinformatycznych).
12. Nagrania mogą być udostępniane jedynie organom na podstawie obowiązujących przepisów prawa, na podstawie złożonego wniosku. Osoby prywatne mogą wnioskować o zabezpieczenie nagrań zgodnie z załącznikiem nr 1., w sytuacji, o której mowa w pkt 10.
13. Samo nagranie przez system pobytu na terenie szpitala nie jest podstawą do wglądu do nagrań, ponieważ każdy wchodzący na tereny szpitalne jest uprzedzony o prowadzonym monitoringu za pomocą tablic informacyjnych, umieszczonych w widocznym miejscu na budynku, przy drzwiach wejściowych do obiektów. Także pomieszczenia oraz strefy monitorowane są oznaczone w sposób widoczny i czytelny naklejkami z piktogramem kamery, czyli znakiem graficznym informującym o stosowaniu monitoringu w danej przestrzeni. Stąd jego zachowanie nie powinno odbiegać od przyjętych zasad przebywania w miejscach publicznych. Z uwagi na specyfikę naszego systemu monitoringu, który pracuje automatycznie, bez udziału człowieka, przyjmujemy zasadę, że wejście osoby w oznaczoną strefę objętą monitoringiem jest równoznaczne z wyrażeniem przez tę osobę zgody na przetwarzanie jej danych w zakresie wizerunku i wykonywanych czynności, jakie zostaną zarejestrowane przez kamery systemu.
14. Zasady funkcjonowania w Szpitalu systemu monitoringu wizyjnego, w pomieszczeniach Oddziału Psychiatrycznego przeznaczonych do izolacji pacjentów, regulują odrębne przepisy prawa powszechnie obowiązującego (Art. 18e. ustawy o ochronie zdrowia psychicznego)
15. Dane z monitoringu wizyjnego nie stanowią informacji publicznej i nie podlegają udostępnieniu na podstawie ustawy o dostępie do informacji publicznej.
16. Podstawą prawną przetwarzania danych osobowych w systemie monitoringu

wizyjnego w szpitalu jest: art. 6 ust 1 lit f) (prawnie uzasadniony interes realizowany przez Administratora), art. 9 ust. 2 lit h) (niezbędne do celów zapewnienia opieki zdrowotnej) oraz art. 6 ust 1 lit c) (w przypadku monitorowania pomieszczeń przeznaczonych do izolacji pacjentów w ramach stosowania środka przymusu bezpośredniego) 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),

Podstawą prawną stosowania monitoringu jest art. 23a ustawy z dnia 15 kwietnia 2011r. o działalności leczniczej, Rozporządzenia Ministra Zdrowia z dnia 26 marca 2019 r. w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą oraz art. 22² ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.

17. Decyzje w sprawach nieuregulowanych niniejszą Procedurą podejmuje Dyrektor Szpitala.

15. Obowiązek informacyjny

INFORMACJA DLA PRACOWNIKÓW

Zgodnie z art. 13 ust.1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (zwanego dalej „RODO”) informujemy, że:

1) Administratorem Pani/Pana danych osobowych jest Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31-503 Kraków.

2) Inspektorem Ochrony Danych jest Anna Baliga – Nowak, kontakt:
anna.baliga@mcrd.pl

3) Celem przetwarzania jest:

- zatrudnianie, pomoc socjalna, zapewnienie komercyjnych świadczeń socjalnych, organizacji pracy oraz bezpieczeństwa pracy i mienia poprzez monitoring wizyjny/monitoring systemów informatycznych - na podstawie Art. 6 ust. 1 lit. c RODO oraz Art. 222 Kodeksu Pracy z dnia 26 czerwca 1974 r
- na podstawie Art. 6 ust. 1 lit. a, jako zgody osoby, której dane dotyczą na m.in. publikację wizerunku / na przekazanie danych innym podmiotom
- na podstawie Art. 6 ust. 1 lit. b, jako niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub podjęcie działań na żądanie takiej osoby przed zawarciem umowy.

4) Odbiorcami Pani/Pana danych osobowych będą:

- pracownicy administracji w zakresie swoich obowiązków służbowych, na podstawie upoważnienia
- Urząd Marszałkowski Województwa Małopolskiego – Podmiot wiodący w ramach projektu Regionalnej Platformy Wymiany Elektronicznej Dokumentacji Medycznej w Województwie Małopolskim (MSIM), w którym uczestniczy Placówka.
- BIP
- dostawcy poza zatrudnieniowych świadczeń pracowniczych
- podmioty przetwarzające dane osobowe związku z zawartymi umowami z Administratorem, podmioty uprawnione przepisami prawa. Administrator podejmuje wszelkie niezbędne działania, by jego podwykonawcy, udzielali odpowiedniej gwarancji stosowania środków bezpieczeństwa w każdym przypadku, gdy przetwarzają dane osobowe na zlecenie Administratora.

5) Pani/Pana dane osobowe nie będą przekazywane do państw trzecich.

6) Pani/Pana dane osobowe przechowywane będą nie dłużej niż jest to konieczne, tj. przez okres określony obowiązującymi w tym zakresie przepisami prawa.

7) Posiada Pani/Pan prawo do żądania od administratora dostępu do treści swoich danych osobowych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

8) Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

9) Podanie danych osobowych w zakresie wymaganym przez ustawę z dnia 26 czerwca 1974 r. - Kodeks Pracy jest obligatoryjne, a w pozostałym zakresie jest dobrowolne

10) Dane osobowe nie stanowią podstawy do zautomatyzowanego podejmowania decyzji ani do profilowania.

INFORMACJA DLA PERSONELU MEDYCZNEGO

Zgodnie z art. 13 ust.1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (zwanego dalej „RODO”) informujemy, że:

1) Administratorem Pani/Pana danych osobowych jest Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31-503 Kraków.

2) Inspektorem Ochrony Danych jest Anna Baliga – Nowak, kontakt:

anna.baliga@mcrd.pl

- 3) Pani/Pana dane osobowe przetwarzane będą w celu ochrony stanu zdrowia, świadczenia usług medycznych - na podstawie Art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
- 4) Odbiorcami Pani/Pana danych osobowych będą organy upoważnione na podstawie obowiązujących przepisów prawa, Urząd Marszałkowski Województwa Małopolskiego (MSIM)
- 5) Pani/Pana dane osobowe nie będą przekazywane do państw trzecich.
- 6) Pani/Pana dane osobowe będą przechowywane nie dłużej niż jest to konieczne, tj. przez okres określony obowiązującymi w tym zakresie przepisami prawa.
- 7) Posiada Pani/Pan prawo do żądania od administratora dostępu do treści swoich danych osobowych, sprostowania danych nieprawidłowych, uzupełnienia danych niekompletnych lub ograniczenia przetwarzania.
- 8) Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
- 9) Podanie danych osobowych jest obligatoryjne na podstawie przepisu prawa.
- 10) Pani/Pana dane osobowe nie stanowią podstawy do zautomatyzowanego podejmowania decyzji ani do profilowania.

INFORMACJA DLA KONTRAHENTA

Zgodnie z art. 13 ust.1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (zwanego dalej „RODO”) informujemy, że:

- 1) Administratorem Pani/Pana danych osobowych jest Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31-503 Kraków.
- 2) Inspektorem Ochrony Danych jest Anna Baliga – Nowak, kontakt: anna.baliga@mcrd.pl
- 3) Pani/Pana dane osobowe przetwarzane będą w celu:
 - realizacji umowy - na podstawie Art. 6 ust. 1 lit. b) RODO
 - związanym z prowadzeniem ksiąg rachunkowych i dokumentacji podatkowej w celu wypełnienia obowiązku prawnego w myśl art. 6 ust. 1 lit. c) RODO w zw. z art. 74 ust. 2 ustawy z dnia 29 września 1994 r. o rachunkowości;
 - ustalenia, dochodzenia lub obrony roszczeń - na podstawie prawnie uzasadnionego interesu administratora danych w myśl art. 6 ust. 1 lit. f) RODO .
- 4) Odbiorcami Pani/Pana danych osobowych będą:
 - Podmioty uczestniczące w realizacji zlecenia
 - Pracownicy i współpracownicy Szpitala posiadający upoważnienie do przetwarzania danych osobowych Kontrahentów w związku z wykonywaniem obowiązków służbowych;

- Dostawcy usług technicznych i organizacyjnych dla Szpitala (m.in. dostawcy i podmioty wyspecjalizowane w obsłudze technicznej systemów teleinformatycznych);
- Podmioty uprawnione na podstawie przepisów prawa.

5) Pani/Pana dane osobowe nie są przekazywane do państw trzecich.

6) Pani/Pana dane osobowe przechowywane będą nie dłużej niż jest to konieczne, tj. przez okres wymagany przez odpowiednie przepisy prawa w zakresie przechowywania dokumentacji księgowej i podatkowej lub przez okres przedawnienia roszczeń określony w przepisach prawa.

7) Posiada Pani/Pan prawo do żądania od administratora dostępu do treści swoich danych osobowych, ich sprostowania, uzupełnienia i ograniczenia przetwarzania.

8) Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

9) Podanie danych osobowych jest dobrowolne, jednakże niezbędne w celu związanym z zawarciem i realizacją umowy.

10) Dane osobowe nie stanowią podstawy do zautomatyzowanego podejmowania decyzji ani do profilowania.

INFORMACJA DOTYCZĄCA ZAMÓWIEŃ PUBLICZNYCH

Zgodnie z art. 13 ust.1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (zwanego dalej „RODO”) informujemy, że:

1) Administratorem Pani/Pana danych osobowych jest Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31-503 Kraków.

2) Inspektorem Ochrony Danych jest Anna Baliga – Nowak, kontakt: anna.baliga@mcrd.pl

3) Pani/Pana dane osobowe przetwarzane będą w celu dopełnienia obowiązków określonych w przepisach prawa, w szczególności w celu rozpatrzenia ofert, zawierania umów np. o udzielanie zamówień publicznych, umów na udzielanie świadczeń zdrowotnych, umów najmu, umów darowizny przez Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie - na podstawie Art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

4) Odbiorcami Pani/Pana danych osobowych będą pracownicy administracji w zakresie swoich obowiązków służbowych na podstawie upoważnienia. Odbiorcami mogą być instytucje państwowe upoważnione z mocy prawa.

5) Pani/Pana dane osobowe nie będą przekazywane do państw trzecich.

6) Pani/Pana dane osobowe przechowywane będą nie dłużej niż jest to konieczne, tj. przez okres określony obowiązującymi w tym zakresie przepisami prawa.

- 7) Posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania.
- 8) Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
- 9) Podanie danych osobowych jest obligatoryjne na podstawie przepisu prawa
- 10) Pani/Pana dane osobowe nie stanowią podstawy do zautomatyzowanego podejmowania decyzji ani do profilowania.

INFORMACJA DLA STAŻYSTÓW

Zgodnie z art. 13 ust.1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (zwanego dalej „RODO”) informujemy, że:

- 1) administratorem danych osobowych stażystów jest **Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, adres: 31-503 Kraków, ul. Strzelecka 2;**
- 2) administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się w sprawach przetwarzania danych osobowych za pośrednictwem poczty elektronicznej: anna.baliga@mcrd.pl;
- 3) administrator będzie przetwarzał dane osobowe stażystów na podstawie art. 6 ust. 1 lit. b) RODO, gdyż przetwarzanie to jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Jeżeli w dokumentach zawarte są dane, o których mowa w art. 9 ust.1 RODO konieczna będzie zgoda na ich przetwarzanie (art. 9 ust. 2 lit. a RODO), która może zostać odwołana w dowolnym czasie
- 4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz administratora
- 5) administrator nie zamierza przekazywać danych osobowych stażystów do państwa trzeciego lub organizacji międzynarodowej;
- 6) stażyści mają prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.
- 7) dodatkowo zgodnie z art. 13 ust. 2 RODO Szpital Przyjmujący informuje, że dane

osobowe będą przechowywane przez okres wymagany przez odpowiednie przepisy prawa w zakresie przechowywania dokumentacji związanej z odbywaniem stażu.;

8) stażyście przysługuje prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także do wniesienia sprzeciwu wobec przetwarzania, prawo do przeniesienia danych oraz prawo do wniesienia skargi do organu nadzorczego;

9) podanie danych osobowych jest dobrowolne, jednakże niezbędne do zawarcia i realizacji umowy;

10) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o dane osobowe.

INFORMACJA DLA STUDENTÓW - PRAKTYKANTÓW

Zgodnie z art. 13 ust.1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (zwanego dalej „RODO”) informujemy, że:

1) administratorem danych osobowych studentów-praktykantów jest **Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, adres: 31-503 Kraków, ul. Strzelecka 2;**

2) administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się w sprawach przetwarzania danych osobowych za pośrednictwem poczty elektronicznej: anna.baliga@mcrd.pl;

3) administrator będzie przetwarzał dane osobowe studentów- praktykantów, na podstawie art. 6 ust. 1 lit. b) RODO, gdyż przetwarzanie to jest niezbędne w celu wykonania porozumienia, którego stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem porozumienia; Jeżeli w dokumentach zawarte są dane, o których mowa w art. 9 ust1 RODO konieczna będzie zgoda na ich przetwarzanie (art. 9 ust. 2 lit. a RODO), która może zostać odwołana w dowolnym czasie

4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych, w związku z realizacją usług na rzecz administratora

5) administrator nie zamierza przekazywać danych osobowych studentów - praktykantów do państwa trzeciego lub organizacji międzynarodowej;

6) studenci-praktykanci mają prawo uzyskać kopię swoich danych osobowych w

siedzibie administratora.

7) dodatkowo zgodnie z art. 13 ust. 2 RODO Szpital przyjmujący informuje, że dane osobowe będą przechowywane nie dłużej niż jest to konieczne, tj. przez okres określony obowiązującymi w tym zakresie przepisami prawa.

8) studentowi- praktykantowi przysługuje prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także do wniesienia sprzeciwu wobec przetwarzania, prawo do przeniesienia danych oraz prawo do wniesienia skargi do organu nadzorczego;

9) podanie danych osobowych jest dobrowolne, jednakże niezbędne do zawarcia i realizacji porozumienia;

10) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o dane osobowe.

INFORMACJA DLA OSÓB OBJĘTYCH MONITORINGIEM WIZYJNYM

Zgodnie z art. 13 ust.1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1) (zwanego dalej „RODO”) informujemy, że:

1) Administratorem systemu monitoringu jest **Wojewódzki Specjalistyczny Szpital Dziecięcy im. św. Ludwika w Krakowie, ul. Strzelecka 2, 31-503 Kraków**

2) Inspektorem Ochrony Danych jest Anna Baliga – Nowak, kontakt:
anna.baliga@mcrd.pl

3) Monitoring stosowany jest w celu zapewnienia bezpieczeństwa osób i mienia Szpitala, znajdujących się na terenie Szpitala, poprzez umożliwienie obserwacji obrazów z kamer oraz ich rejestracji –na podstawie art. 6 ust 1 lit. f ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

4) Odbiorcami Pani/Pana danych osobowych mogą być

- podmioty uprawnione na podstawie przepisów prawa

- pracownicy i współpracownicy Szpitala posiadający upoważnienie do przetwarzania danych osobowych osób objętych monitoringiem wizyjnym w związku z wykonywaniem obowiązków służbowych lub świadczeniem usług na zlecenie Szpitala

- dostawcy usług technicznych i organizacyjnych dla Szpitala (w szczególności dostawcy i podmioty wyspecjalizowane w zapewnienie obsługi technicznej systemów teleinformatycznych).

5) Pani/Pana dane osobowe nie są przekazywane do państw trzecich.

- 6) Nagrania obrazu zawierające dane osobowe przetwarzane będą wyłącznie do celów, dla których zostały zebrane i przechowywane przez okres 3 dni.
- 7) Osoba zarejestrowana przez system monitoringu ma prawo dostępu do treści swoich danych osobowych.
- 8) Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
- 9) Pani/Pana dane osobowe nie stanowią podstawy do zautomatyzowanego podejmowania decyzji ani do profilowania.

16. Szkolenie wstępne RODO

Przepisy prawa o ochronie Danych osobowych

- ROZPORZĄDZENIE PE I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie o ochronie danych)
- Ustawa o Ochronie Danych Osobowych z dnia 10.05. 2018 r
- Ustawa powołała nowy Urząd Ochrony Danych Osobowych – „UODO”
- UODO może nas kontrolować, czy przestrzegamy zasad ochrony danych osobowych.
 - ✓ kontrolować planowo
 - ✓ z powodu skargi pracownika
 - ✓ z powodu skargi klienta

Definicje RODO

Administrator - to nasz pracodawca - decyduje o celach i środkach przetwarzania danych osobowych

Inspektor Ochrony Danych (IOD) – koordynator wszelkich spraw związanych z danymi osobowymi w organizacji. Nadzoruje, czy Administrator, wszyscy pracownicy i współpracownicy chronią dane w należyty sposób

Administrator Systemu Informatycznego (ASI) –

osoba zarządzająca komputerami, zakładająca konta użytkownikom, odpowiedzialna za prawidłowe funkcjonowanie systemów informatycznych, sprzętu, oprogramowania i jego konserwację, za bezpieczeństwo infrastruktury IT

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 OSOBOWE PRZETWARZANE W PLACÓWCE MEDYCZNEJ:

- Dane o stanie zdrowia (w dokumentacji medycznej)
- Dane zwykłe (kontaktowe, identyfikacyjne)
- Dane niezbędne do przetwarzania w celu zatrudnienia personelu medycznego i administracyjnego
- Dane niezbędne do przetwarzania w celu zawierania umów z kontrahentami
- Inne dane

Przykłady:

imię/nazwisko/adres	imię/nazwisko/numer telefonu
dane z bazy CEIDG	maile (jan.nowak@energa.pl)
monitoring, zapisy rozmów	PESEL
dane o lokalizacji	Adres IP, MAC

Dane wrażliwe (szczególna kategoria danych)

- Dane dotyczące zdrowia fizycznego i psychicznego (*ZFŚS, dane medyczne, stopień niepełnosprawności, dysleksja ucznia*)
- Dane genetyczne (*DNA, próbki biologiczne*)
- Dane biometryczne (*wizerunek lub dane daktyloskopijne*)
- Wyroki skazujące i naruszenia prawa,
- Przynależność związkowa, polityczna, religijna, rasowa

Formy występowania danych osobowych:

Forma papierowa: akta osobowe, segregatory, archiwa, umowy z klientami, umowy-zlecenia, faktury

Forma elektroniczna: programy kadrowo-płacowe, bazy klientów, dane na serwerze i na dyskach komputerów, pliki na pendrive

Forma głosowa: centrala telefoniczna

Forma wizyjna: monitoring wizyjny

Przetwarzanie danych – to operacje na danych osobowych

- Wgląd
- Wprowadzanie
- Modyfikacja
- Usuwanie, Niszczenie, Anonimizacja (zmiana danych, w wyniku której dane tracą charakter danych osobowych)
- Przetwarzanie na serwerze i w biurze
- Archiwizacja, Kopie bezpieczeństwa
- Udostępnianie, powierzanie, przesyłanie

Siedem podstawowych zasad przetwarzania danych osobowych:

1) Zasada zgodności z prawem, rzetelności i przejrzystości – przetwarzanie

danych wyłącznie, gdy istnieje ważna podstawa prawna uzasadniająca ich przetwarzanie, np. przepis prawa, któremu podlega administrator, zgoda osoby, której dane dotyczą

2) Zasada celowości – przetwarzanie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach

3) Zasada adekwatności (proporcjonalności) – przetwarzanie danych tylko w takim zakresie w jakim jest to niezbędne dla realizacji celu przetwarzania

4) Zasada prawidłowości danych – podejmowanie działań mających na celu zapewnienie prawidłowości, kompletności, sprostowanie lub usunięcie nieprawidłowych danych osobowych

5) Zasada ograniczenia czasowego – przechowywanie danych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane

6) Zasada integralności i poufności danych – przetwarzanie danych w sposób zapewniający ich odpowiednie bezpieczeństwo (środki techniczne i organizacyjne), w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem

7) Zasada rozliczalności – administrator danych osobowych musi być w stanie wykazać, że przestrzega wszystkich wymienionych zasad dotyczących przetwarzania danych

Prawa osób, których dane dotyczą:

Prawo do dostępu do danych

Osoba, której dane dotyczą ma prawo do:

- Uzyskania od administratora potwierdzenia, czy przetwarza jej dane osobowe;
- Uzyskania dostępu do swoich danych;
- Uzyskania od administratora wszystkich informacji o warunkach przetwarzania danych;
- Bezpłatnego uzyskania po raz pierwszy w żądanym zakresie kopii swoich danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę. Dotyczy to również **dokumentacji medycznej**. (4 maj 2019 r.- Ustawa sektorowa wdrażająca RODO)

Prawo do sprostowania oraz uzupełnienia danych

Osoba, której dane są przetwarzane, może żądać:

- Niezwłocznego sprostowania danych osobowych, które są nieprawidłowe
- Uzupełnienia niekompletnych danych osobowych
- *Obowiązek poprawności **danych zawartych w dokumentacji medycznej** jest bezwzględnym obowiązkiem podmiotu leczniczego, podobnie jak obowiązek przechowywania tejże dokumentacji w określony sposób oraz przez określony czas. Z tego też względu prawo do sprostowania danych będzie wykonywane przez podmiot leczniczy zgodnie z przepisami sektorowymi regulującymi prowadzenie dokumentacji medycznej.*

Prawo do bycia zapomnianym

Na żądanie osoby, której dane dotyczą, administrator ma obowiązek:

- Natychmiastowego usunięcia jej danych;
- Poinformowania innych administratorów przetwarzających jej dane osobowe, by usunęli oni wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
- PRAWO NIE MA ZASTSOWANIA w przypadku **dokumentacji medycznej**- tu przetwarzanie danych jest niezbędne do wywiązania się z prawnego

obowiązku , któremu podlega administrator (art. 29 u.p.p., który określa terminy przechowywania dokumentacji medycznej.)

Skorzystanie z prawa do bycia zapomnianym jest możliwe, gdy:

- Dane osobowe nie są już niezbędne do celów, w których zostały zebrane;
- Osoba, której dane dotyczą cofnęła zgodę i nie ma innej podstawy prawnej przetwarzania;
- Osoba ta wniosła sprzeciw wobec przetwarzania i nie występują nadrzędne, prawnie uzasadnione podstawy przetwarzania;
- Dane osobowe były przetwarzane niezgodnie z prawem;
- Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego;
- Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą, może żądać ograniczenia zakresu danych przetwarzanych, jeżeli:

- Kwestionuje prawidłowość swoich danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
- Przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony jej roszczeń;
- Wniosła sprzeciw wobec przetwarzania jej danych – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Żądanie pacjenta ograniczenia przetwarzania danych zawartych w dokumentacji medycznej jest bezskuteczne

Prawo do przenoszenia danych

Administrator na żądanie osoby, której dane przetwarza, musi:

- Udostępnić dane osobowe w celu ich przesłania innemu administratorowi;

Przesłać te dane bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Prawo to przysługuje, gdy przetwarzanie danych odbywa się w sposób zautomatyzowany na podstawie zgody osoby, której dane dotyczą lub na podstawie zawartej z nią umowy.

Prawo to co do zasady nie ma zastosowania do podmiotów leczniczych, jeżeli przetwarza dane w celu i zakresie niezbędnym do udzielania świadczeń zdrowotnych. Ponieważ przetwarzanie danych przez podmiot wykonujący działalność leczniczą opiera się głównie na przepisie art. 9 ust 2 lit. H RODO, realizacja prawa do przenoszenia danych nie będzie obowiązkiem podmiotów leczniczych.

Prawo do wniesienia sprzeciwu wobec przetwarzania danych

Osoba, której dane są przetwarzane, może sprzeciwić się przetwarzaniu jej danych:

- Przetwarzania jej danych w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- Przetwarzania jej danych w celu realizacji prawnie uzasadnionych interesów administratora;
- Przetwarzania jej danych w celu marketingu bezpośredniego;
- Przetwarzanie jej odbywa się w sposób zautomatyzowany.
- Żądanie pacjenta o zaprzestanie przetwarzania danych zawartych w dokumentacji medycznej jest bezskuteczne.

Prawo do odszkodowania

- Każda osoba, która poniosła szkodę (**także niemajątkową**) w wyniku naruszenia przepisów RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę;
- Administrator / podmiot przetwarzający zostają zwolnieni z odpowiedzialności, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody;
- Podmioty które dopuściły się naruszenia odpowiadają solidarnie za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

Wymiana danych z innymi podmiotami:

Ujawnianie, przekazywanie - przekazanie danych pomiędzy Administratorami

- „**wymuszone**” przepisem prawa – *jeżeli pracodawca musi przekazać dane pracownika do Urzędu Skarbowego, ZUS lub Komornika*
- „**możliwe**” na podstawie prawa – *kiedy pracodawca przekazuje dane pracownika do ubezpieczyciela (ubezpieczenie grupowe) ale nie musi tego robić*
- **bez przepisu prawa**- na podstawie zgody osoby – *jeżeli pracodawca przekazuje dane do Benefit Systems, kliniki medycznej za zgodą pracownika*

Powierzenie – następuje wtedy, kiedy dane osobowe przekazywane są innemu podmiotowi (*firmie, instytucji*), aby ta przetwarzała je na zlecenie właściciela danych w zakresie przez niego wskazanym.

Nasz pracodawca stosuje umowy powierzenia z podmiotami, które wykonują dla nas badania laboratoryjne, diagnostyczne, konsultacje itd.

Umowa powierzenia gwarantuje, że Szpital współpracuje z podmiotami, które chronią powierzone dane osobowe z należytą starannością zgodnie z Rozporządzeniem.

Udostępnianie danych – Każdy PWDL jest Administratorem danych Pacjentów, których dane przetwarza w celach zdrowotnych. Oznacza to w szczególności, że PWDL jest niezależnym Administratorem i nie jest zasadne na potrzeby realizacji

celów zdrowotnych zawieranie z tym podmiotem jako Podmiotem przetwarzającym umowy powierzenia przetwarzania danych osobowych przekazywanych np. przez:

*Pracodawcę przekazującego dane osobowe pracowników w celu objęcia ich opieką medyczną bez względu na okoliczność, czy opieka ta dotyczy świadczeń zdrowotnych z zakresu medycyny pracy, czy wykracza ona poza ten zakres (tzw. benefity pracownicze);

*Organizatora udzielania świadczeń zdrowotnych lub zakład ubezpieczeń;

*Inny PWDL udostępniający dane na potrzeby zachowania ciągłości usług medycznych, w tym w ramach podwykonawstwa udzielania świadczeń, w tym wykonywania badań diagnostyki laboratoryjnej i obrazowej oraz badań histopatologicznych (obejmuje to m.in. sytuacje, w których Pacjent uzyskuje świadczenia na podstawie skierowania w podmiocie, będącym podwykonawcą PWDL wydającego skierowanie na określony rodzaj badania, celem jego wykonania

OBOWIĄZEK ADMINISTRATORA - OBOWIĄZEK INFORMACYJNY

Przed przystąpieniem do przetwarzania danych osobowych administrator powinien udzielić osobie, której dane dotyczą, szeregu informacji dotyczących celu, podstawy prawnej oraz czasu przetwarzania danych, jak również przekazać jej informacje na temat przysługujących praw.

Informacje te administrator powinien przekazać w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, w szczególności gdy informacje są kierowane do dziecka.

Kodeks branżowy w ochronie zdrowia- przekazanie informacji na co najmniej 2 sposoby:

- w dokumentach przekazanych pacjentowi,
- na stronie internetowej lub w systemie informatycznym podmiotu leczniczego dostępnej dla Pacjenta (tzw. Portal Pacjenta),
- na tablicach informacyjnych w przestrzeniach ogólnodostępnych, najczęściej wykorzystywanych przez pacjentów,
- w regulaminie organizacyjnym.

Incydenty- Przypadkowe lub niezgodne z prawem zdarzenia mogące wywoływać ryzyko naruszenia ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia (np. sfałszowania danych, utraty kontroli nad własnymi danymi osobowymi) – zgłasza je organowi nadzorczemu (UODO).

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, skutki incydentu dotyczą ofiarę, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Istnieje obowiązek wewnętrznej rejestracji incydentów!

O naruszeniu ochrony danych pracownik powinien **niezwłocznie** poinformować przełożonego lub Inspektora Ochrony Danych WSSDz im. św. Ludwika w Krakowie.

Przykładowe incydenty:

- **Pożar, zalanie**
- **Utrata danych** (awarie, brak prądu, wirusy)
- **Świadome skasowanie** danych
- **Włamanie** lub **Kradzież** danych
- **Wyrzucenie** danych na śmietnik
- **Przekazanie danych** osobie nieupoważnionej
- **Zagubienie** dokumentacji, laptopa, pendrive
- **Przypadkowa** modyfikacja danych
- **Upublicznienie** danych w internecie
- **Nieuprawniony** dostęp do danych osobowych
- **Sprzedaż** danych

Fizyczne zabezpieczenie danych osobowych:

- Ochrona pomieszczeń
- Monitoring
- Kontrola dostępu

- Pomieszczenia podczas nieobecności zamykamy na klucz
- Szafy i biurka po godzinach pracy zamykamy na klucz, jeśli to możliwe, stosujemy skrzynki na klucze
- Stosujemy politykę czystego biurka (po godzinach pracy)
- Sprzątanie w obecności pracowników upoważnionych
- Drukarki i ksera zabezpieczone przed dostępem osób postronnych
- Dokumenty niszczymy w niszczarkach!
- Zabezpieczamy dokumenty i nośniki przy wynoszeniu poza teren miejsca pracy

Zabezpieczenia informatyczne:

Każdy użytkownik pracuje na WŁASNYM koncie (identyfikatorze)

- na komputerze
 - na serwerze
 - w programie z danymi osobowymi
 - Włączamy zahasłowane wygaszacze ekranu po czasowym odejściu od stanowiska pracy
 - Obowiązuje polityka czystego ekranu
 - Po zakończeniu pracy wylogowujemy się i wyłączamy komputer
 - hasła powinny składać się z co najmniej 12 znaków
- duże litery + małe litery + cyfry (lub znaki specjalne)**
- hasła muszą być zmieniane raz na 60 dni
 - jeżeli system nie wymusza zmiany haseł, musisz sam zmieniać hasło
 - wystrzegaj się stosowania łatwych do odgadnięcia haseł
 - nie zapisuj haseł na kartkach, nie naklejaj na komputer, nie trzymaj pod klawiaturą lub w szufladzie
 - nie udostępniaj swojego hasła innym osobom, a w przypadku ujawnienia hasła - natychmiast go zmień
 - Nie instaluj (z internetu lub z nośników) programów na komputerach firmowych bez uzyskania zgody informatyka

- Ponosisz odpowiedzialność za szkody spowodowane przez tak samowolnie zainstalowane oprogramowanie!
- Używaj tylko licencjonowanego oprogramowania
- W razie awarii komputera powiadom Informatyka
- Nie wyłączaj programu antywirusowego
- Zakazane jest przeglądanie stron niedozwolonych (np. pornograficznych, terrorystycznych, hackerskich)
- Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł

Zabezpieczenia laptopów i nośników wynoszonych na zewnątrz

- Użytkownicy pisemnie przyjmują regulamin eksploatacji komputerów przenośnych
- Komputer przenośny lub zewnętrzny twardy dysk lub pendrive z danymi osobowymi wynoszony na zewnątrz musi być zaszyfrowany (zahasłowany)
- Przewoź laptop bezpiecznie - w teczce, pod siedzeniem, nie pozostawiaj go w bagażniku
- Po pracy zadбай o zamknięcie laptopa „na klucz”
- Wykonuj **REGULARNIE** kopie bezpieczeństwa z laptopa
- Korzystając z internetu w miejscu publicznym miej włączony firewall

Polityka korzystania z poczty email

- Jeśli wysyłasz mailem pliki z danymi osobowymi, powinienes je zahasłować i ewentualnie spakować a hasło wysłać odbiorcy maila inną drogą (inny mail, SMS)
- Niedozwolone jest uczestniczenie w „łańcuszkach szczęścia”
- Uważaj na wybór adresata – łatwo o pomyłkę przy wysyłce
- Bank NIGDY nie poprosi Cię o podanie numeru karty mailem
- Nie otwieraj w mailach podejrzanych załączników i linków (nawet od znajomych). Jeśli to możliwe, sprawdzaj wysyłaną i odbieraną pocztę programem antywirusowym
- Zgłaszaj informatykowi przypadki podejrzanych maili

Zabezpieczenia osobowe

- Każda osoba przed dopuszczeniem do przetwarzania danych osobowych powinna zapoznać się zasadami ochrony danych
- Jak się możemy zapoznać z w/w zasadami – **OPCJE**:
- Czytamy Regulamin Ochrony Danych Osobowych
- Czytamy Politykę Ochrony Danych Osobowych oraz IZSI służącym do przetwarzania danych osobowych

Po zapoznaniu się jesteśmy zobowiązani do podpisania **Oświadczeń o poufności**.

Nasz pracodawca nadaje nam następnie *Upoważnienia do przetwarzania danych osobowych* wraz z zakresem upoważnienia.

SANKCJE

W przypadku naruszeń w zakresie zabezpieczenia danych osobowych pracodawca musi liczyć się z sankcjami w postaci:

- administracyjnych kar pieniężnych,
- odpowiednich środków nakładanych na mocy RODO przez organ nadzorczy (Prezesa UODO),
- upomnienia.

Uwaga! Sankcje nie są wymierzone poszczególnym pracownikom, lecz pracodawcy jako administratorowi danych osobowych.

Pracownik musi jednak liczyć się z odpowiedzialnością za spowodowanie naruszenia ochrony danych osobowych w zakładzie pracy:

- **Odpowiedzialność materialna**

Jeżeli przez naruszenie doszło do wyrządzenia szkody pracodawcy (pracodawca został obciążony karą pieniężną przez Prezesa UODO lub musiał zapłacić odszkodowanie podmiotowi danych), wówczas w trybie roszczenia regresowego pracodawca może zażądać odszkodowania od pracownika. W przypadku wyrządzenia szkody z winy nieumyślnej odszkodowanie nie może przekraczać równowartości **3-miesięcznego wynagrodzenia** pracownika.

- **Odpowiedzialność porządkowa**

Nawet jeśli pracodawca nie został ukarany za naruszenie ochrony danych osobowych spowodowanych przez pracownika, to i tak pracownik może zostać ukarany karą porządkową **upomnienia lub nagany** za naruszenie porządku pracy.

Kara ulega zatarciu (usunięciu z akt osobowych pracownika) po roku nienaganej pracy.

17. Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.