

Standardy Ochrony Małoletnich w Uniwersyteckiego Centrum Medycyny Morskiej i Tropikalnej w Gdyni

Każde dziecko ma prawo do szczęśliwego i bezpiecznego dzieciństwa, w którym może rozwijać się fizycznie, emocjonalnie i społecznie, bez obawy przed krzywdzeniem i przemocą. Działając na podstawie art. 22b ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (t.j. Dz. U. z 2024 r., poz. 560), wprowadzono do stosowania w Uniwersyteckim Centrum Medycyny Morskiej i Tropikalnej w Gdyni Standardy Ochrony Małoletnich w celu zapobiegania wszelkim formom przemocy, nadużyć oraz krzywdzenia dzieci, jak również szybkiego reagowania w przypadku podejrzeń lub sygnałów alarmowych dotyczących naruszeń bezpieczeństwa małoletnich.

Rozdział I Postanowienia ogólne

§1

Ilekroć w Standardach Ochrony Małoletnich jest mowa o:

- 1) Standardach – rozumie się przez to niniejszy dokument wraz z załącznikami,
- 2) Podmiocie – rozumie się przez to Uniwersyteckie Centrum Medycyny Morskiej i Tropikalnej w Gdyni,
- 3) Ustawie – rozumie się przez to ustawę z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (t.j. Dz. U. z 2024 r., poz. 560);
- 4) Reprezentancie – rozumie się przez to osobę uprawnioną do reprezentowania i prowadzenia spraw Podmiotu, którą jest Dyrektor
- 5) Koordynatorze – rozumie się przez to pracownika wyznaczonego przez Podmiot odpowiedzialnego za wdrożenie i nadzór nad realizacją Standardów, jak również wykonanie innych obowiązków określonych w Standardach,
- 6) małoletnim lub dziecku – rozumie się przez to każdą osobę, która nie ukończyła 18. roku życia,
- 7) Pracownikowi – rozumie się przez to każdą osobę zatrudnioną w Podmiocie, bez względu na formę zatrudnienia, jak również osobę wykonującą czynności na rzecz Podmiotu, a w szczególności pracownika, współpracownika, zleceniobiorcę, praktykanta, wolontariusza, stażystę itp.;
- 8) Opiekunie – rozumie się przez to przedstawiciela ustawowego małoletniego, w tym rodzica małoletniego pozostającego pod jego władzą rodzicielską lub opiekuna prawnego małoletniego;



- 9) Przemocy – należy przez to rozumieć jednorazowe albo powtarzające się bezprawne działanie lub zaniechanie naruszające prawa lub dobra osobiste małoletniego, w szczególności narażające małoletniego na niebezpieczeństwo utraty życia, zdrowia lub naruszające jego godność, nietykalność cielesną, wolność, w tym seksualną, powodujące szkody na jego zdrowiu fizycznym lub psychicznym, a także wywołujące cierpienie lub krzywdy u małoletniego dotkniętego przemocą.

§2

Celem niniejszych Standardów jest:

- 1) zapewnienie ochrony fizycznej i psychicznej dzieci, w tym zapobieganie wszelkim formom krzywdzenia i nadużyć wobec Dzieci, bez względu na to, kto jest sprawcą przemocy;
- 2) stworzenie środowiska, w którym Dzieci mogą czuć się bezpiecznie, które troszczy się o zdrowie, rozwój i dobrostan małoletnich;
- 3) wczesne wykrywanie i interwencja w przypadku podejrzeń o krzywdzenie, poprzez wprowadzenie wytycznych dotyczących identyfikacji potencjalnych sygnałów alarmowych wskazujących na możliwe przypadki krzywdzenia dzieci oraz określenie kroków do podjęcia w przypadku podejrzeń, włączając w to raportowanie i reagowanie na incydenty;
- 4) edukacja Pracowników Podmiotu, zapewnienie odpowiedniej wiedzy i szkoleń w zakresie rozpoznawania, raportowania i postępowania w przypadku krzywdzenia dzieci, aby Pracownicy byli świadomi swoich obowiązków i potrafili właściwie zareagować w sytuacjach potencjalnego zagrożenia;
- 5) określenie zasad współpracy z odpowiednimi organami i instytucjami, w celu skutecznego wsparcia dzieci i ich rodzin oraz zapewnienia dalszej opieki i interwencji, jeśli jest to konieczne.

§3

1. Wszyscy Pracownicy Podmiotu mają obowiązek przestrzegać postanowień Standardów oraz podejmować działania w celu ochrony małoletnich zgodnie z przepisami prawa powszechnie obowiązującego, Standardami i swoimi kompetencjami.
2. Standardy mają zastosowanie we wszystkich jednostkach i komórkach organizacyjnych Podmiotu, jak również w innych miejscach, w których Podmiot realizuje swoje zadania, jeżeli w tych miejscach przebywają lub mogą przebywać małoletni.
3. Z treścią Standardów zapoznawani są Pracownicy, a także dzieci oraz ich opiekunowie, zgodnie z procedurami określonymi w treści Standardów.

102

Rozdział II

Kontrola Pracowników przed dopuszczeniem do pracy

§4

Przed dopuszczeniem do pracy Pracodawca lub wyznaczona przez niego osoba zapoznaje Pracowników z treścią Standardów oraz ma obowiązek odebrać od Pracowników oświadczenie o zapoznaniu się i akceptacji Standardów. Oświadczenie załącza się do pracowniczych akt osobowych albo do innej dokumentacji dotyczącej danego Pracownika.

§5

1. Zgodnie z art. 21 Ustawy przed nawiązaniem z osobą stosunku pracy lub przed dopuszczeniem osoby do innej działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi na Podmiocie oraz na wskazanym wyżej kandydacie na Pracownika ciąży obowiązki weryfikacyjne. Obowiązki określone w ust. 2 dotyczą też Pracowników, którzy w związku ze zmianą stanowiska lub zakresu powierzonych zadań dopiero mają rozpocząć wykonywać działalność opisaną w zdaniu pierwszym. Wykaz komórek organizacyjnych i stanowisk, które podlegają weryfikacji w Rejestrze Sprawców Przestępstw na Tle Seksualnym oraz przedkładają informację z Krajowego Rejestru Karnego zostały wyszczególnione w załączniku nr 1.
2. Do obowiązków należy:
 - 1) Podmiot uzyskuje informacje, czy dane kandydata na Pracownika wskazanego w ust. 1, są zamieszczone w Rejestrze z dostępem ograniczonym lub w Rejestrze osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze. Pozyskanie informacji następuje poprzez stronę internetową <https://rps.ms.gov.pl/>, po uprzednim założeniu i aktywacji konta;
 - 2) Kandydat na Pracownika wskazany w ust. 1, przedkłada Podmiotowi na swój koszt informację z Krajowego Rejestru Karnego w zakresie przestępstw określonych w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii, lub za odpowiadające tym przestępstwom czyny zabronione określone w przepisach prawa obcego;
 - 3) Jeżeli kandydat na Pracownika posiada obywatelstwo innego państwa niż Rzeczpospolita Polska, ponadto przedkłada Podmiotowi informację z rejestru karnego państwa obywatelstwa uzyskiwaną do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi;
 - 4) Kandydat na Pracownika wskazany w ust. 1, składa Podmiotowi oświadczenie o państwie lub państwach, w których zamieszkiwał w ciągu ostatnich 20 lat, innych niż



Rzeczpospolita Polska i państwo obywatelstwa, oraz jednocześnie przedkłada Podmiotowi informację z rejestrów karnych tych państw uzyskiwaną do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi;

- 5) Jeżeli prawo państwa, o którym mowa w pkt 3 lub 4, nie przewiduje wydawania informacji do celów działalności zawodowej lub wolontariackiej związanej z kontaktami z dziećmi, kandydat na Pracownika jest obowiązany przedłożyć informację z rejestru karnego tego państwa;
- 6) W przypadku gdy prawo państwa, z którego ma być przedłożona informacja, o której mowa w pkt 3-5, nie przewiduje jej sporządzenia lub w danym państwie nie prowadzi się rejestru karnego, kandydat na Pracownika wskazany w ust. 1, składa Podmiotowi oświadczenie o tym fakcie wraz z oświadczeniem, że nie był prawomocnie skazany w tym państwie za czyny zabronione odpowiadające przestępstwom określonym w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii oraz nie wydano wobec niego innego orzeczenia, w którym stwierdzono, iż dopuścił się takich czynów zabronionych, oraz że nie ma obowiązku wynikającego z orzeczenia sądu, innego uprawnionego organu lub ustawy stosowania się do zakazu zajmowania wszelkich lub określonych stanowisk, wykonywania wszelkich lub określonych zawodów albo działalności, związanych z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi;
- 7) Oświadczenia, o których mowa w pkt 4 i 6, składane są pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia. Składający oświadczenie jest obowiązany do zawarcia w nim klauzuli następującej treści: "Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia". Klauzula ta zastępuje pouczenie organu o odpowiedzialności karnej za złożenie fałszywego oświadczenia;
- 8) Informacje wskazane w pkt 1 Podmiot utrwała w formie wydruku i załącza do akt osobowych pracownika albo do innej dokumentacji dotyczącej tego Pracownika, który jest zatrudniony lub wykonuje czynności na innej podstawie niż stosunek pracy. Informacje i oświadczenia wskazane w pkt 2-6 Podmiot załącza do akt osobowych pracownika albo do innej dokumentacji dotyczącej tego Pracownika, który jest zatrudniony lub wykonuje czynności na innej podstawie niż stosunek pracy.

Rozdział III

Zasady bezpiecznych relacji między Pracownikami a małoletnimi

§6

Pracownicy w relacjach z małoletnimi kierują się ich dobrem i działają w ich najlepszym interesie, z poszanowaniem ich godności oraz uwzględnieniem ich emocji i potrzeb.

MR

§7

Pracownicy mają obowiązek:

- 1) dbać o bezpieczeństwo fizyczne i psychiczne małoletnich;
- 2) utrzymywać profesjonalne relacje z małoletnimi i podejmować w stosunku do nich działania niezagrażające ich bezpieczeństwu, adekwatne do ich sytuacji i sprawiedliwe wobec dziecka oraz innych osób;
- 3) prowadzenia otwartej i jasnej komunikacji z dzieckiem, jak również z jego opiekunami, chyba że jest to sprzeczne z interesem dziecka;
- 4) prowadzenia komunikacji z małoletnim w sposób, który nie będzie go zawstydział, lekceważył ani obrażał oraz która będzie zrozumiała dla dziecka, przy uwzględnieniu wieku i stopnia rozwoju dziecka;
- 5) okazywać zainteresowanie sprawami dziecka, wsparcie i gotowość do rozmowy oraz pomocy;
- 6) okazywać zrozumienie dla emocji wyrażanych przez dziecko;
- 7) wyznaczać jasne granice dopuszczalnego postępowania przy jednoczesnym wytłumaczeniu dziecku zasad i przyczyn ich stosowania, a następnie egzekwować ich przestrzeganie bez stosowania jakichkolwiek form przemocy;
- 8) uwzględniać potrzeby dziecka związane z jego wiekiem, stopniem rozwoju, stanem zdrowia oraz ewentualną niepełnosprawnością oraz indywidualnie dostosowywać wymagania oraz stosowane metody do wskazanych wyżej potrzeb.

§8

W relacjach z małoletnim niedopuszczalne jest w szczególności:

- 1) stosowanie wobec małoletnich jakichkolwiek form przemocy, w tym kar fizycznych, zastraszania, przymuszania, czy groźby;
- 2) krzyczenie na dzieci, podnoszenie głosu, używanie słów wulgarnych, czy przekazywanie dziecku treści, które mogłyby wywołać w nim lęk, upokorzyć, ośmieszyć, czy wywołać uczucie dyskomfortu;
- 3) nawiązywanie lub zachęcanie dziecka do nawiązania relacji uczuciowych z Pracownikiem lub inną osobą, składanie propozycji o nieodpowiednim charakterze, jak również naruszanie intymności dziecka;
- 4) dyskryminowanie dziecka z jakiegokolwiek przyczyny, a w szczególności ze względu na wiek, płeć, rasę, niepełnosprawność, status społeczny, religię, orientację seksualną, czy światopogląd;
- 5) ujawniania danych osobowych dziecka osobom nieuprawnionym, jakiegokolwiek przetwarzanie danych osobowych dziecka bez upoważnienia, a w szczególności utrwalanie wizerunku dziecka;

- 6) jakakolwiek forma proponowania lub zachęcania dziecka do spożywania alkoholu, używania wyrobów tytoniowych lub nielegalnych substancji, w tym polegająca na spożywaniu lub używaniu tych wyrobów lub substancji w obecności dziecka.

Rozdział IV

Zasady bezpiecznych relacji między małoletnimi

§9

1. Podmiot dba o to, aby relacje między małoletnimi były nawiązywane z poszanowaniem ich godności, odbywały się w sposób bezpieczny i służyły rozwojowi dziecka, w tym rozwijaniu umiejętności społecznych, nauce współpracy z rówieśnikami i tolerancji.
2. Każdy Pracownik ma obowiązek zwracać uwagę i reagować w przypadku jakiegokolwiek formy nieodpowiedniego zachowania pomiędzy małoletnimi, w szczególności w przypadku zachowań określonych w §8. Zakazy określone w §8 mają zastosowanie również do relacji między małoletnimi.

Rozdział V

Procedura interwencji w przypadku podejrzenia krzywdzenia dzieci

§10

1. Każdy Pracownik jest uprawniony i zobowiązany do reagowania w przypadku podejrzenia, że dziecku dzieje się krzywda.
2. Naruszenie obowiązku reagowania może zostać uznane za ciężkie naruszenie obowiązków pracowniczych lub kontraktowych i jako takie prowadzi do rozwiązania umowy z osobą dopuszczającą się tego naruszenia.
3. Źródłem krzywdy dziecka może być zachowanie Pracownika, zachowanie opiekunów, innej osoby bliskiej, osoby obcej, a także innych dzieci. Krzywda dziecka może przybierać różne formy, w tym:
 - a) popełnienie przestępstwa na szkodę dziecka (np. wykorzystanie seksualne, znęcanie się nad dzieckiem, naruszenie jego nietykalności);
 - b) aktywne formy niebędące przestępstwem (np. krzyk, poniżanie);
 - c) zaniedbanie potrzeb życiowych dziecka (np. związanych z żywieniem, higieną czy zdrowiem).

§11

1. W przypadku powzięcia przez Pracownika podejrzenia, że małoletni jest krzywdzony, lub zgłoszenia takiej okoliczności przez małoletniego, jego opiekuna lub inną osobę, Pracownik

ma obowiązek sporządzenia notatki służbowej i przekazania uzyskanej informacji Reprezentantowi lub Koordynatorowi. Notatka może mieć formę pisemną lub mailową.

2. Interwencja prowadzona jest przez Koordynatora. Jeżeli zgłoszono krzywdzenie ze strony Koordynatora, wówczas interwencja prowadzona jest przez Reprezentanta. W ramach interwencji ustalane są okoliczności zdarzenia, w tym prowadzona jest rozmowa z małoletnim, Pracownikami i innymi potencjalnymi świadkami zdarzenia, w sposób gwarantujący małoletniemu poufność i chroniący jego dalsze bezpieczeństwo.
3. O ustaleniach w ramach prowadzonej interwencji i propozycjach podjęcia działań Koordynator zawiadamia Reprezentanta.
4. Z przebiegu każdej interwencji sporządza się kartę interwencji, której wzór stanowi załącznik nr 2 do Standardów. Osoba przeprowadzająca interwencję opracowuje i wdraża plan dalszego wsparcia małoletniego po ujawnieniu krzywdzenia z uwzględnieniem rodzaju naruszeń, ich sprawcy oraz możliwości Podmiotu.

§12

1. W przypadku podejrzenia popełnienia przestępstwa na szkodę małoletniego, bez względu na osobę sprawcy, Reprezentant składa zawiadomienie o podejrzeniu przestępstwa do prokuratury lub policji.
2. Jeżeli sprawcą przestępstwa może być Pracownik, Reprezentant niezwłocznie odsuwa Pracownika od pracy i czynności, w których mógłby mieć kontakt z pokrzywdzonym małoletnim oraz ocenia zasadność rozwiązania z Pracownikiem umowy będącej podstawą jego zatrudnienia lub powierzenia mu czynności.
3. Jeżeli sprawcą przestępstwa jest inna osoba, Reprezentant w ramach posiadanych kompetencji podejmuje możliwe działania, aby uniemożliwić sprawcy kontakt z pokrzywdzonym małoletnim.

§13

W przypadku podejrzenia zaniedbania potrzeb życiowych dziecka lub stosowania innych form przemocy ze strony opiekunów dziecka, Reprezentant składa wniosek o wgląd w sytuację rodziny do sądu rejonowego, wydziału rodzinnego i nieletnich.

§14

Jeżeli dziecko doznaje innej formy krzywdzenia ze strony Pracownika niż popełnienie przestępstwa na jego szkodę:

- 1) w sytuacji, gdy zachowanie było jednorazowe i o niewielkiej intensywności wkroczenia w dobra dziecka należy przeprowadzić rozmowę dyscyplinującą z Pracownikiem;
- 2) w sytuacji gdy naruszenie dobra dziecka jest znaczne, w szczególności gdy doszło do dyskryminacji lub naruszenia godności dziecka - Reprezentant ocenia zasadność

zastosowania sankcji określonych przepisami prawa, w tym zasadność rozwiązania z Pracownikiem umowy będącej podstawą jest zatrudnienia lub powierzenia mu czynności.

§15

Jeżeli dziecko doznaje innej formy krzywdzenia ze strony innego małoletniego niż popełnienie przestępstwo na jego szkodę:

- 1) w sytuacji, gdy zachowanie było jednorazowe i o niewielkiej intensywności wkroczenia w dobra dziecka - należy przeprowadzić rozmowę ze sprawcą naruszenia i jego opiekunami;
- 2) w sytuacji, gdy naruszenie dobra dziecka jest znaczne lub naruszenie powtarza się pomimo podjętych wcześniej interwencji - należy przeprowadzić rozmowę z opiekunami sprawcy naruszenia i rozważyć zasadność i możliwość podjęcia działań zmierzających do zapobiegania dalszego kontaktu sprawcy z małoletnim. Działania te powinny być adekwatne do sytuacji i poczynione z rozwagą, należy bowiem kierować się również troską o sytuację małoletniego sprawcy.

§16

O przebiegu interwencji, dokonanych ustaleniach i podjętych działaniach Koordynator informuje opiekuna małoletniego. Koordynator nie przekazuje tych informacji, jeśli mogłoby to zagrozić bezpieczeństwu dziecka lub gdy obowiązek zachowania tajemnicy wynika z powszechnie obowiązujących przepisów prawa. Może to dotyczyć np. sytuacji, gdy sprawcą przestępstwa jest dany opiekun.

Rozdział VI

Udostępnianie i aktualizacja Standardów

§17

1. Koordynator jest odpowiedzialny za monitorowanie realizacji Standardów, prowadzenie rejestru interwencji (wzór określa załącznik nr 3), za reagowanie na sygnały naruszenia Standardów oraz za proponowanie zmian w Standardach.
2. Standardy są dostępne dla Pracowników, małoletnich i ich opiekunów, w szczególności poprzez zamieszczenie na stronie internetowej UCMMiT. i wywieszenie w widocznym miejscu w siedzibie Podmiotu, również w wersji skróconej, przeznaczonej dla małoletnich.
3. Koordynator przeprowadza szkolenia wśród Pracowników dotyczące stosowania Standardów, zachęca do zaznajomienia się z nimi przez małoletnich i opiekunów oraz udziela im wyjaśnień w zakresie Standardów i ich stosowania.

4. Co najmniej raz na dwa lata Koordynator przeprowadza ocenę Standardów w celu zapewnienia ich dostosowania do aktualnych potrzeb oraz zgodności z obowiązującymi przepisami. Wnioski z przeprowadzonej oceny oraz ewentualne propozycje zmian Koordynator przedstawia w formie pisemnej Reprezentantowi.
5. Reprezentant wprowadza do Standardów niezbędne zmiany i publikuje zmienioną treść Standardów.
6. W przypadku zmiany Standardów, Koordynator informuje o tym Pracowników, przeprowadza niezbędne szkolenia oraz odbiera od Pracowników oświadczenia o zapoznaniu się i akceptacji Standardów. Postanowienie §4 ust. 2 stosuje się odpowiednio.

Rozdział VII

Bezpieczeństwo w Internecie

§18

1. Małoletni nie mają dostępu do infrastruktury Podmiotu umożliwiającej połączenie z siecią Internet.
2. Komputery znajdujące się w placówkach Podmiotu posiadające dostęp do sieci Internet są zabezpieczone loginem i hasłem oraz są przeznaczone tylko do użytku Pracowników Podmiotu. Sieć WI-FI również jest zabezpieczona hasłem. Loginy i hasła nie są udostępniane małoletnim.
3. Na terenie Podmiotu małoletni mogą korzystać ze swoich urządzeń mobilnych za zgodą swoich opiekunów i na ich odpowiedzialność. Opiekunowie powinni zabezpieczyć urządzenia mobilne przed możliwością uzyskania dostępu do stron i treści szkodliwych dla małoletnich.

§19

1. Należy chronić małoletnich przed dostępem do treści szkodliwych. Szkodliwe treści to takie materiały, które mogą wywoływać negatywne emocje u odbiorcy lub promują niebezpieczne zachowania. Można do nich zaliczyć:
 - a) treści pornograficzne dostępne bez żadnego ostrzeżenia, w tym tzw. pornografię dziecięcą, czyli materiały prezentujące seksualne wykorzystywanie dzieci;
 - b) treści obrazujące przemoc, obrażenia fizyczne, deformacje ciała, np. zdjęcia lub filmy przedstawiające ofiary wypadków, okrucieństwo wobec ludzi lub zwierząt;
 - c) treści nawołujące do samookaleczeń lub samobójstw, bądź zachowań szkodliwych dla zdrowia, np. zachęcanie do zażywania niebezpiecznych substancji np. leków czy narkotyków;
 - d) treści dyskryminacyjne, nawołujące do wrogości, a nawet nienawiści wobec różnych grup społecznych lub jednostek.
2. W celu ochrony małoletnich przed treściami szkodliwymi stosuje się poniższe standardy:



- a) urządzenia przeznaczone dla dziecka powinny być wyposażone w program filtrujący, pozwalający na uchronienie dziecka przed kontaktem ze szkodliwymi treściami;
- b) należy monitorować wyszukiwane przez dzieci treści w Internecie i przeprowadzać z opiekunami rozmowy w przypadku stwierdzenia wyszukiwania szkodliwych treści;
- c) rozmawiać z dziećmi o tym, co robią w Internecie. Jeżeli coś je zaniepokoi, czegoś się przestraszą w sieci, dziecko powinno czuć, że może się zwierzyć każdemu Pracownikowi. W ten sposób można uniknąć negatywnych konsekwencji związanych z przypadkowym, niezamierzonym kontaktem z treściami drastycznymi, ale także w porę wychwycić inne problemy, których rozwiązania dziecko szuka w Internecie.

Rozdział VIII

Postanowienia końcowe

§20

1. Standardy wchodzi w życie z dniem ich ogłoszenia.
2. Ogłoszenie następuje poprzez publikację w sposób określony w §17 ust. 2.



Standardy Ochrony Małoletnich
w Uniwersyteckim Centrum Medycyny Morskiej i Tropikalnej w Gdyni
(wersja skrócona dla małoletnich)

Każde dziecko jest dla nas równie ważne. Nie ma znaczenia w szczególności jaką masz płeć, w jakim jesteś wieku, jak wyglądasz, w którym państwie się urodziłeś, czy i jaką wyznajesz religię, czy jaka jest sytuacja finansowa w Twojej rodzinie itd. – jesteś dla nas tak samo ważny i masz takie same prawa do szczęśliwego i bezpiecznego dzieciństwa.

Tak jak każda inna osoba, tak samo Ty zasługujesz na szacunek. Nikt nie ma prawa Cię krzywdzić, a zwłaszcza bić, popychać, krzyczeć na Ciebie, obrażać Cię, grozić, straszyć czy w inny sposób sprawiać, że będziesz czuł się źle. Nie może tego robić żaden z naszych pracowników, inne dziecko, Twój rodzic, opiekunowie, rodzeństwo ani żadna inna osoba.

Pamiętaj jednak, że to działa w dwie strony – nikt nie może Ciebie krzywdzić, ale Ty też nie możesz krzywdzić innych, a zwłaszcza innych dzieci. Zachowujmy się tak, jak sami chcielibyśmy być traktowani. Bądźmy dla siebie mili i uczynni, pomagajmy sobie nawzajem, zwłaszcza osobom młodszym od siebie.

U nas możesz czuć się bezpiecznie. Jeżeli chcesz o czymś porozmawiać, to zawsze możesz się do nas zwrócić (do któregośkolwiek z naszych pracowników, stażystów, wolontariuszy) – chętnie Cię wysłuchamy.

Jeżeli coś Cię smuci, coś Cię boli, ktoś sprawił Ci krzywdę lub źle Cię potraktował, zawsze możesz do nas przyjść – chętnie Ci pomożemy. Tak samo jeśli widzisz, że inne dziecko jest krzywdzone, to możesz nam o tym powiedzieć i dzięki temu będziemy mogli pomóc temu dziecku.

Jeżeli z jakiegokolwiek powodu czujesz się źle, to nie musisz tego ukrywać. Masz prawo płakać, nie ma w tym nic złego.

Pamiętaj, aby z Internetu korzystać z rozsądkiem. Bardzo ważne jest, abyś nie udostępniał nikomu w Internecie osobistych informacji (np. imienia, nazwiska, gdzie mieszkasz, czy swoich zdjęć), ani abyś nie kontaktował się z nieznanymi. Jeżeli zobaczysz w Internecie cokolwiek, co Cię zaniepokoi, wystraszy lub czego nie rozumiesz – możesz nam o tym powiedzieć, to też Ci pomożemy.

KARTA INTERWENCJI

KARTA INTERWENCJI		
Imię i nazwisko małoletniego		
Osoba sporządzająca kartę interwencji		
Data sporządzenia karty interwencji		
Przyczyna interwencji (forma krzywdzenia)		
Osoba zawiadamiająca o podejrzeniu krzywdzenia (imię i nazwisko, stanowisko lub pokrewieństwo)		
Opis działań podjętych w ramach interwencji	Data i miejsce	Opis
Przeprowadzone rozmowy z opiekunami małoletniego	Data i miejsce	Opis
Forma podjętej interwencji		

Dane dotyczące interwencji (nazwa organu, do którego zgłoszono interwencję) i data interwencji		
Wyniki interwencji: działania organów/działania podjęte przez Podmiot, inne osoby	Data i organ podejmujący interwencję	Opis
Uwagi i podsumowanie		

REJESTR INTERWENCJI

REJESTR INTERWENCJI					
Lp.	Data	Rodzaj naruszenia	Kogo dotyczy	Opis naruszenia, podjęte działania	Uwagi

I. Kontekst

Ustawa z dnia 13 maja 2016 r. (t.j. Dz.U. z 2024 r. poz. 560) o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich, znowelizowana ustawą z dnia 28 lipca 2023 r. o zmianie ustawy - kodeks rodzinny i opiekuńczy oraz niektórych innych ustaw (t.j. Dz. U. z 2023 r. poz. 1606) wprowadza obowiązek wdrożenia standardów ochrony małoletnich (dalej: SOM). Obowiązek ten dotyczy: *"organów zarządzających jednostkami systemu oświaty (przedszkoli, szkół i schronisk młodzieżowych) oraz innych placówek oświatowych, opiekuńczych wychowawczych, resocjalizacyjnych, religijnych, artystycznych, medycznych, rekreacyjnych, sportowych lub związanymi z rozwijaniem zainteresowań, do których uczęszczają albo, w której przebywają małoletni, a także organizatorów tychże działalności oraz podmioty świadczące usługi hotelarskie, turystyczne czy prowadzące inne miejsca zakwaterowania zbiorowego."* Komunikat Prezes Urzędu Ochrony Danych Osobowych (dalej: PUODO) z dnia 14.08.2024 r. (<https://uodo.gov.pl/pl/138/3278>).

Wymienione placówki miały do 15 sierpnia 2024 r. czas na wprowadzenie standardów pracy i postępowania z dziećmi. Pracodawca lub inny organizator działalności zobowiązany jest do sprawdzenia czy dane przyszłego pracownika lub osoby dopuszczanej do działalności są zamieszczone w Rejestrze Sprawców Przestępstw na Tle Seksualnym z dostępem ograniczonym, lub w Rejestrze osób w stosunku, do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze. Nowe wymogi dotyczą też opiekunów oraz wolontariuszy, którzy mają kontakt z dziećmi. Pracodawca musi uzyskać także zaświadczenie o niekaralności z Krajowego Rejestru Karnego (KRK), a w przypadku obcokrajowców – z rejestrów karnych państw, w których mieszkali w ostatnich 20 latach. Katalog przestępstw przedstawił Prezes UODO w ww. komunikacie: *"Dotyczy to przestępstw o charakterze seksualnym, przestępstw przeciwko życiu i zdrowiu (np. pobicie, spowodowanie uszczerbku na zdrowiu), przestępstwa znęcania się, przestępstwa handlu ludźmi, przestępstw z ustawy o przeciwdziałaniu narkomanii lub informacji o odpowiadających tym przestępstwom czynach zabronionych określonych w przepisach prawa obcego."* Ustawa wprowadza szereg nowych regulacji dotyczących ochrony małoletnich, co niesie potencjalne zagrożenia dla ochrony danych osobowych.

W kontekście wdrażania SOM pracodawca musi pamiętać, że przypadku, gdy operacje przetwarzania mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych Administrator zobowiązany jest przeprowadzić ocenę skutków dla ochrony danych (DPIA). Dotyczyć może to w szczególności takich Administratorów, którzy przetwarzają dane z katalogu art. 9 ust. 1 RODO.

II. Cel

Ustawa wprowadza szereg nowych regulacji dotyczących ochrony małoletnich, co niesie szereg zagrożeń dla ochrony danych osobowych. Określenie potencjalnych zagrożeń związanych z przetwarzaniem danych osobowych, szczególnie w odniesieniu do osób pracujących z nieletnimi. Ustawa dotyczy m.in. przetwarzania danych o karalności, dlatego ważne jest, aby zidentyfikować miejsca, gdzie może dojść do wycieku danych, nadużyć, czy błędnego przetwarzania. Na podstawie analizy ryzyka formułuje się zalecenia dotyczące środków technicznych i organizacyjnych, które należy wdrożyć, aby to ryzyko zminimalizować.

III. Analiza ryzyka - metodyka

Określanie poziomu ryzyka polega na przypisaniu danemu zagrożeniu prawdopodobieństwa oddziaływania oraz ustaleniu wpływu materializacji zagrożenia na:

- 1) dostępność systemu lub informacji,
- 2) integralność systemu lub informacji,
- 3) poufność informacji przetwarzanej w systemie,
- 4) rozliczalności informacji, a następnie wyznaczeniu poziomu ryzyka.

Do oszacowania analizy ryzyka zgodnie z art. 32 RODO wykorzystana będzie macierz opracowana i przygotowana przez Urząd Ochrony Danych Osobowych. W oparciu o ocenę prawdopodobieństwa wystąpienia oraz skutków uzyskuje się poziom istotności ryzyka utraty poufności, dostępności, integralności i rozliczalności danych. Przy ocenie skutków wystąpienia ryzyka brane są pod uwagę zarówno skutki finansowe, jak i niefinansowe, np. utrata reputacji, konsekwencje prawne, utrata szansy zrealizowania ważnego zadania, opóźnienie w realizacji zadań, obniżenie jakości pracy itp.

Poziom ryzyka wyznaczono według wzoru: $R = P \times S$

gdzie:

R – poziom ryzyka (istotność)

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia,

S – wartość skutków

			SKUTEK				
			Bardzo niski 1	Niski 2	Średni 3	Wysoki 4	Bardzo wysoki 5
PRAWDOPODOBIEŃSTWO	Prawie pewne	5	Ś	W	K	K	K
	Prawdopodobne	4	Ś	W	W	K	K
	Możliwe	3	N	Ś	W	W	K
	Mało prawdopodobne	2	N	Ś	Ś	W	W
	Rzadkie	1	N	N	Ś	W	W

Poziom ryzyka	Opis działania
Niski (N)	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
Średni (Ś)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
Krytyczny (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

Prawdopodobieństwo wystąpienia zagrożenia	Wartość liczbowa	Opis
Prawie pewne	5	Przewiduje się, że zdarzenie z pewnością wystąpi w ciągu roku
Prawdopodobne	4	Przewiduje się, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku
Możliwe	3	Przewiduje się, że zdarzenie objęte ryzykiem zdarzy się kilka razy w ciągu roku
Mało prawdopodobne	2	Przewiduje się, że zdarzenie objęte ryzykiem zdarzy się dwa w ciągu roku
Rzadkie	1	Przewiduje się, że zdarzenie objęte ryzykiem zdarzy się raz się lub nie zdarzy się w ciągu roku

Wpływ zagrożenia (Skutki)	Wartość liczbowa	Opis
Bardzo wysoki	5	Zdarzenie wywołuje krytyczny skutek. Skutki mogą prowadzić do wysokiego uszczerbku fizycznego, szkód majątkowych dla osób fizycznych. Zagrożenie ustawową karą

		pozbawienia wolności. Koszty kilkuset procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole organów ścigania. Zdarzenie objęte ryzykiem powoduje brak realizacji kluczowych zadań albo osiągnięcie założonych celów – poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa albo reputacji. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się długotrwały i trudny proces przywracania stanu poprzedniego.
Wysoki	4	Zdarzenie wywołuje wysoki skutek. Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych, jednak nie są one wysokie. Wysokie ustawowe kary pieniężne. Koszt kilkudziesięciu procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole i kary UODO. Zdarzenie objęte ryzykiem powoduje znaczną stratę posiadanych zasobów, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, reputację jednostki. Z wystąpieniem zdarzenia objętego ryzykiem może się wiązać trudny proces przywracania stanu poprzedniego.
Średni	3	Zdarzenie wywołuje średni skutek. Nałożenie kar ustawowych w dolnej granicy kary. Koszt nielicznych procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, niewielkie zakłócenie lub opóźnienie w wykonywaniu zadań. Wpływa na reputację jednostki. Skutki zdarzenia można łatwo usunąć.
Niski	2	Zdarzenie wywołuje niski skutek. Szum medialny, np. z powodu ujawnienia danych niepodlegających ochronie prawnej. Zdarzenie objęte ryzykiem powoduje minimalną stratę finansową lub krótkotrwałe zakłócenia lub opóźnienie w wykonywaniu zadań. Nie wpływa na reputację. Skutki zdarzenia można łatwo usunąć.
Bardzo niski	1	Zdarzenie nie wywołuje żadnych skutków

Analiza ryzyka - tabela

Zagrożenie (źródło ryzyka)	Zagrożony atrybut: poufność/integralność/dostępność	Skutki wystąpienia ryzyka	Prawdopodobieństwo	Skutki	Poziom istotności ryzyka	Środki techniczne i organizacyjne redukujące ryzyko	Decyzja dotycząca ryzyka
Nadmierna ilość przetwarzanych danych	Poufność	<ul style="list-style-type: none"> Naruszenie prywatności Trudności w zarządzaniu danymi W przypadku kontroli UODO możliwość nałożenia kar finansowych 	2	3	Sredni	<ul style="list-style-type: none"> Zastosowanie anonimizacji lub pseudonimizacji danych w sytuacjach, gdzie pełne dane osobowe nie są potrzebne Automatyzacja procesów weryfikacji tożsamości Regularne audyty z ochrony danych osobowych Wprowadzenie polityk dotyczących minimalizacji danych, gdzie gromadzone są tylko te dane, które są absolutnie konieczne Szkolenia dla pracowników 	<ul style="list-style-type: none"> wyeliminowane zredukowane zaakceptowane
Nieautoryzowany dostęp do danych	Poufność	<ul style="list-style-type: none"> Wyciek danych osobowych Kradzież tożsamości Szkody finansowe Naruszenie prywatności Utrata zaufania do organizacji Kradzież danych Możliwość modyfikacji danych Kary finansowe nałożone przez organ nadzorczy 	3	3	Wysoki	<ul style="list-style-type: none"> System kontroli dostępu Wymuszenie używania silnych haseł i autoryzacji dwuetapowej Określone role użytkowników systemu Regularne szkolenia pracowników z zakresu bezpiecznego zarządzania hasłami i uwierzytelnienia Szyfrowanie danych Kopie zapasowe 	<ul style="list-style-type: none"> wyeliminowane zredukowane zaakceptowane
Ataki złośliwego oprogramowania (malware, ransomware)	Poufność/Integralność/Dostępność/Rozliczalność	<ul style="list-style-type: none"> Zablokowanie dostępu do danych Utrata danych Koszty odzyskania danych Koszty usunięcia złośliwego oprogramowania Utrata reputacji organizacji 	3	3	Wysoki	<ul style="list-style-type: none"> Umowy serwisowe Zapora i ochrona sieci Edukacja dotycząca rozpoznawania złośliwego oprogramowania i bezpiecznego otwierania załączników Polityka reagowania na incydenty 	<ul style="list-style-type: none"> wyeliminowane zredukowane zaakceptowane

HR

						<ul style="list-style-type: none"> ● Regularnie aktualizowane narzędzia do wykrywania i usuwania złośliwego oprogramowania ● Systemy do filtrowania załączników i linków w wiadomościach e-mail ● Możliwość szybkiej izolacji zainfekowanych systemów od sieci w celu zapobieżenia rozprzestrzenianiu się malware ● System przeciwdziałania utracie danych (data leak prevention — DLP) ● Kopie zapasowe ● Antywirus 	
Wycieki danych	Poufność/Integralność/Dostępność/Rozliczalność	<ul style="list-style-type: none"> ● Dostęp osób trzecich do danych osobowych ● Kradzież tożsamości ● Możliwość zapoznania się z danymi przez osoby trzecie ● Utrata zaufania do jednostki ● Kary finansowe nałożone przez organ nadzorczy ● Pozwy sądowe ● Koszty nowych zabezpieczeń ● Naruszenie prywatności osób ● Stygmatyzacja osób, których dane znajdują się w rejestrach 	2	4	Wysoki	<ul style="list-style-type: none"> ● Wdrożenie silnych zabezpieczeń sieciowych i firewalli ● Wymuszenie używania silnych haseł ● Regularne szkolenia w zakresie ochrony danych dla personelu ● Regularne szkolenia pracowników z zakresu cyberbezpieczeństwa ● Zapora i ochrona sieci ● System przeciwdziałania utracie danych (data leak prevention — DLP) ● Monitoring sieci 	<ul style="list-style-type: none"> ● wyeliminowane ● zredukowane ● zaakceptowane
Braki w zabezpieczeniach sieciowych	Poufność/Integralność/Dostępność	<ul style="list-style-type: none"> ● Próby ujawnienia wrażliwych danych ● Modyfikacja lub odmowa dostępu do usług ● Kradzież danych 	2	3	Średni	<ul style="list-style-type: none"> ● Implementacja funkcji kontroli dostępu ● Szyfrowanie danych ● Zapory sieciowe ● Systemy wykrywania włamań oraz systemy zapobiegania włamaniom ● Regularne przeglądy stosowanych zabezpieczeń 	<ul style="list-style-type: none"> ● wyeliminowane ● zredukowane ● zaakceptowane

102

						<ul style="list-style-type: none"> • Zabezpieczenie środków finansowych na nowe technologie mające wpływ na bezpieczeństwo sieci • System przeciwdziałania utracie danych (data leak prevention — DLP) 	
Ataki hakerskie	Poufność/Integralność/Dostępność	<ul style="list-style-type: none"> • Naruszenie prywatności pracowników, klientów, kontrahentów organizacji • Potencjalne straty finansowe • Kradzież danych • Potencjalne koszty związane z odszkodowaniami dla osób, których prywatność została naruszona • Modyfikacja danych przez osoby nieuprawnione • Spadek zaufania do organizacji • Pozwy od osób fizycznych • Negatywny wpływ na reputację jednostki • Ujawnienie danych • Koszty nowych zabezpieczeń 	2	3	Sredni	<ul style="list-style-type: none"> • Urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym • Kopie zapasowe • Zapory sieciowe i monitoring sieci • Audyty bezpieczeństwa • Umowy serwisowe obejmujące pomoc w przypadku incydentu • Plan reagowania na incydenty 	<ul style="list-style-type: none"> • wyeliminowane • zredukowane • zaakceptowane
Błędy ludzkie np.: przypadkowe usunięcie danych, nieprawidłowe zarządzanie dostępem, przypadkowe ujawnienie danych	Poufność/Integralność/Dostępność	<ul style="list-style-type: none"> • Niezamierzony wyciek danych • Koszty odzyskiwania danych • Utrata zaufania do organizacji • Kary finansowe nałożone przez organ nadzorczy 	3	3	Sredni	<ul style="list-style-type: none"> • Szkolenie pracowników z ochrony danych osobowych • Szkolenia pracowników z obsługi dostępu do rejestrów • Weryfikacja danych przed zapisaniem – implementacja mechanizmów walidacji danych 	<ul style="list-style-type: none"> • wyeliminowane • zredukowane • zaakceptowane
Udostępnienie osobom trzecim lub kradzież danych do logowania do rejestru dostępem	Poufność	<ul style="list-style-type: none"> • Modyfikacja dostępu • Ujawnienie danych z art. 9 ust. 1 RODO oraz 	2	4	Wysoki	<ul style="list-style-type: none"> • Kontrola dostępu • Szyfrowanie danych • Zapory sieciowe 	<ul style="list-style-type: none"> • wyeliminowane • zredukowane • zaakceptowane

Ar2

ograniczonym (dot. Rejestru Sprawców Przepstępów na Tle Seksualnym)		<p>art. 10 RODO osobom trzecim</p> <ul style="list-style-type: none"> • Wtórna wiktymizacja ofiar przestępstw na tle seksualnym • Groźby lub stosowanie przemocy wobec osób skazanych oraz ich rodzin 				<ul style="list-style-type: none"> • Systemy wykrywania włamań oraz systemy zapobiegania włamaniom • Regularne przeglądy stosowanych zabezpieczeń • Zabezpieczenie środków finansowych na nowe technologie mające wpływ na bezpieczeństwo sieci • System przeciwdziałania utracie danych (data leak prevention — DLP) 	
Brak nadzoru nad zaświadczeniami papierowymi pozyskanymi z KRK	Poufność/Integralność/Dostępność	<ul style="list-style-type: none"> • Dostęp osób trzecich do danych osobowych • Możliwość fizycznego zniszczenia dokumentacji papierowej • Możliwość ujawnienia przez osoby trzecie danych art. 10 RODO • Stygmatyzacja osób, których dane przetwarzane są w rejestrze • Groźby słowne i fizyczne wobec tych osób i ich rodzin 	2	3	Średni	<ul style="list-style-type: none"> • Ewidencja dokumentacji • Przechowywanie dokumentacji w szafach zamykanych na klucz • Zakaz wnoszenia oryginałów dokumentacji • Zakaz drukowania dokumentacji w domu • Procedura postępowania z dokumentacją papierową/kadrową • Szkolenia pracowników odpowiedzialnych za pozyskiwanie danych z rejestrów 	<ul style="list-style-type: none"> • wyeliminowane • zredukowane • zaakceptowane
Brak szkoleń pracowników z procesów przetwarzania danych zgodnie z ustawą i RODO	Poufność/Integralność	<ul style="list-style-type: none"> • Brak świadomości pracowników o przetwarzaniu danych i prawidłowej ich ochronie • Ujawnianie danych osobowych zwykłych i szczególnej kategorii • Stygmatyzacja osób, których dane mogą znajdować się w rejestrach • Gromadzenie danych zbędnych • Kary finansowe nałożone przez organ nadzorczy 	3	2	Średni	<ul style="list-style-type: none"> • Regularne szkolenia pracowników • Ograniczenie zakresu monitorowania i zbierania danych wyłącznie do tych, które są niezbędne do wykonywania określonych zadań 	<ul style="list-style-type: none"> • wyeliminowane • zredukowane • zaakceptowane

42

<p>Utrata danych z powodu: awarii sprzętu, błędów w oprogramowaniu, braku kopii zapasowych</p>	<p>Poufność/Integralność/Dostępność</p>	<ul style="list-style-type: none"> ● Niezdolność do odtworzenia danych ● Przerwanie działalności jednostki ● Spadek zaufania klientów ● Wysokie koszty związane z odzyskiwaniem utraconych danych ● Negatywny wpływ na reputację organizacji ● Opóźnienia w realizacji zadań ustawowych ● Straty finansowe ● Kary finansowe nałożone przez organ nadzorczy 	<p>2</p>	<p>3</p>	<p>Sredni</p>	<ul style="list-style-type: none"> ● Kopie zapasowe ● Antywirus ● Zapora i ochrona sieci ● Regularne szkolenia dla pracowników z zakresu ochrony danych osobowych ● Umowy serwisowe 	<ul style="list-style-type: none"> ● wyeliminowane ● zredukowane ● zaakceptowane
<p>Zagrożenia fizyczne np. pożar, zalanie, kradzież sprzętu, inne zdarzenia losowe</p>	<p>Poufność/Dostępność/Integralność</p>	<ul style="list-style-type: none"> ● Zniszczenie fizycznych nośników danych ● Przewidywane w działalności organizacji ● Wysokie koszty napraw ● Utrata danych ● Wysokie koszty przywracania danych 	<p>1</p>	<p>4</p>	<p>Wysoki</p>	<ul style="list-style-type: none"> ● Automatyczne narzędzia do tworzenia kopii zapasowych i odzyskiwania danych ● Plan odzyskiwania danych po awarii (DRP) ● UPS, generatory ● Plan ciągłości działania ● Systemy przeciwpożarowe ● SSNiW ● Monitoring ● Ochrona fizyczna budynku ● System kontroli dostępu do budynku i pomieszczeń ● Silne hasła dostępne do komputerów i laptopów ● Szyfrowanie nośników danych 	<ul style="list-style-type: none"> ● wyeliminowane ● zredukowane ● zaakceptowane
<p>Niewłaściwe zarządzanie uprawnieniami pracowników wyznaczonych do weryfikacji informacji w rejestrach</p>	<p>Poufność/Integralność</p>	<ul style="list-style-type: none"> ● Użytkownicy posiadają zbyt szerokie uprawnienia, co zwiększa ryzyko nieautoryzowanego dostępu do danych osobowych ● Wyciek danych 	<p>2</p>	<p>3</p>	<p>Sredni</p>	<ul style="list-style-type: none"> ● Polityka nadawania dostępu ● Mechanizmy RBAC (Role-Based Access Control) ● Automatyczne wygaszanie uprawnień ● Regularne przeglądy uprawnień pracowników 	<ul style="list-style-type: none"> ● wyeliminowane ● zredukowane ● zaakceptowane

Handwritten signature

		<ul style="list-style-type: none"> • Kary finansowe nałożone przez organ nadzorczy • Możliwość modyfikacji danych 					
Zagrożenia fizyczne	Poufność/Integralność/Rozliczalność	<ul style="list-style-type: none"> • Naruszenia bezpieczeństwa pozostaną niewykryte przez długi czas • Brak szybkiej identyfikacji i reakcji na incydenty bezpieczeństwa • Trudności w identyfikacji odpowiedzialnych za naruszenia • Możliwość utraty danych 	3	3	Wysoki	<ul style="list-style-type: none"> • Wdrożenie systemów do monitorowania działań użytkowników oraz logów systemowych • Automatyzacja procesu raportowania podejrzanych działań oraz generowanie alertów w czasie rzeczywistym • Regularne przeprowadzanie audytów wewnętrznych oraz zewnętrznych, aby ocenić skuteczność zabezpieczeń • Kopie zapasowe • Ustalenie jasnych zasad dotyczących zarządzania kontami użytkowników, w tym procedur przyznawania, modyfikowania i usuwania dostępu 	<ul style="list-style-type: none"> • wyeliminowane • zredukowane • zaakceptowane
Nadużywanie dostępu do danych osobowych przez pracodawców	Poufność	<ul style="list-style-type: none"> • Wykorzystywanie danych o przeszłości kryminalnej może prowadzić do dyskryminacji pracownika • Dochodzenie praw przez pracownika przed sądem • Skargi do UODO • Kary finansowe nałożone przez organ nadzorczy • Odszkodowania dla pracownika 	2	4	Wysoki	<ul style="list-style-type: none"> • Mechanizmy autoryzacji i uwierzytelniania dla osób mających dostęp do danych szczególnej kategorii • Regularne szkolenia dla kadry kierowniczej z ochrony danych osobowych • Audyty uprawnień do dostępu do rejestrów 	<ul style="list-style-type: none"> • wyeliminowane • zredukowane • zaakceptowane

IV. Podsumowanie analizy ryzyka

MR

Przeprowadzona analiza wykazała liczne potencjalne zagrożenia związane z przetwarzaniem danych osobowych. Ryzyko określone jako wysokie, obejmuje przede wszystkim: nieautoryzowany dostęp do danych, ataki złośliwego oprogramowania, wyciek danych, udostępnienie osobom trzecim lub kradzież danych do logowania, zagrożenia fizyczne, nadużywanie dostępu do danych osobowych przez pracodawców. Skutki takich naruszeń mogą wpłynąć negatywnie na zaufanie społeczne do organizacji, powodować kary finansowe, a także naruszenia prywatności osób, których dane są przetwarzane. W celu obniżenia ryzyka zaleca się stosowanie wymienionych w analizie środków technicznych i organizacyjnych. Organizacja powinna dbać o przeprowadzanie regularnych audytów z ochrony danych osobowych ze szczególnym naciskiem na ochronę danych szczególnej kategorii, organizować szkolenia z ochrony danych osobowych oraz pozyskiwania danych z rejestrów państwowych dla pracowników i pracodawcy, oraz weryfikować nadane uprawnienia do dostępu do rejestrów.

MZ

Informacja dla pracownika

Zgodnie z art. 13 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), dalej „RODO”, informujemy:

Administrator danych

Administratorem Pani/Pana danych osobowych jest Uniwersyteckie Centrum Medycyny Morskiej i Tropikalnej z siedzibą w Gdyni, ul. Powstania Styczniowego 9b, 81-519 Gdynia, Tel.:58 699 95 06, adres e-mail: dyrekcja@ucmmit.gdynia.pl.

Inspektor ochrony danych

We wszystkich sprawach dotyczących ochrony danych osobowych, ma Pani/Pan prawo kontaktować się z naszym Inspektorem ochrony danych, na adres e-mail: dane_osobowe@ucmmit.gdynia.pl;

Cele przetwarzania i podstawa przetwarzania danych

Pani/Pana dane osobowe przetwarzane są przez UCMMiT na potrzeby (i na podstawie prawnej):

- a) zawarcia i realizacji zawartej z Panią/Panem umowy (podstawa z art. 6 ust 1 lit. b RODO),
- b) w celu realizacji obowiązków prawnych ciążących na UCMMiT (obsługa kadrowo-płacowa) zgodnie z obowiązującymi przepisami prawa, w szczególności ustawy Kodeks pracy, przepisów szczególnych, aktów wykonawczych do Kodeksu Pracy (w szczególności dotyczących obowiązku prowadzenia dokumentacji pracowniczej, przepisów o systemie ubezpieczeń społecznych), przepisów podatkowych i o rachunkowości; umowy (podstawa z art. 6 ust 1 lit. c RODO),
- c) w celu wynikającym z prawnie uzasadnionych interesów Administratora Danych, jakim jest ustalenie, obrona i dochodzenie roszczeń (podstawa z art. 6 ust. 1 lit. f RODO).
- d) w celu wynikającym z prawnie uzasadnionych interesów Administratora Danych, jakim jest zapewnienie bezpieczeństwa i ochrony mienia - monitoring wizyjny (podstawa z art. 6 ust. 1 lit. f RODO).

Obowiązek podania danych

Podanie danych osobowych jest wymogiem ustawowym, w związku z czym ich podanie jest obowiązkowe. Niepodanie danych uniemożliwia zatrudnienie.

Okres przechowywania danych

Pani/Pana dane osobowe będą przechowywane przez okres wymagany przepisami prawa, nie dłużej jednak niż przez okres przedawnienia roszczeń. W takim przypadku, dla okresu przedawnienia, zastosowanie znajdą ogólne przepisy wynikające z ustawy Kodeks cywilny. Dokumentacja pracownicza przechowywana jest przez okres 10 lat od zakończenia umowy.

Dane osobowe przetwarzane dla celów księgowo-rachunkowych oraz podatkowych będą przechowywane przez okres 5 lat liczonych od końca roku kalendarzowego, w którym powstał obowiązek podatkowy. Po upływie wyżej wymienionych okresów Pani/Pana będą usuwane lub poddane anonimizacji.

Odbiorcy danych

Pani/Pana dane mogą być przekazywane następującym kategoriom odbiorców:

- a) podmiotom uprawnionym na podstawie przepisów prawa;
- b) podmiotom współpracującym z UCMMiT, z którymi Administrator zawarł umowy lub porozumienia, jak:
 - a. dostawcy usług teleinformatycznych i księgowych,
 - b. obsługa prawna i doradcza,
 - c. firmom realizującym usługi związane z utylizacją dokumentacji i innych nośników zawierających dane osobowe

Przekazywanie danych poza Europejski Obszar Gospodarczy (EOG)

Pani/Pana dane osobowe nie będą przekazywane do państw trzecich ani organizacji międzynarodowych.

Zautomatyzowane podejmowanie decyzji

W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, w tym również w formie profilowania.

Prawa osób

Posiada Pani/Pan prawo do:

- a) dostępu do swoich danych osobowych, ich sprostowania, żądania od Administratora usunięcia lub ograniczenia przetwarzania danych osobowych;
- b) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (00-193 Warszawa, ul. Stawki 2, e-mail: kancelaria@uodo.gov.pl), gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

Przyjęłam /Przyjąłem do wiadomości



.....

data i podpis pracownika)

(

MW

**KLAUZULA INFORMACYJNA DLA KONTRAHENTÓW
UNIWERSYTECKIEGO CENTRUM MEDYCYNY MORSKIEJ I TROPICALNEJ**

Zgodnie z art. 13 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), dalej „RODO”, informujemy, że:

Administrator danych

Administratorem Pani/Pana danych osobowych jest Uniwersyteckie Centrum Medycyny Morskiej i Tropikalnej z siedzibą w Gdyni, ul. Powstania Styczniowego 9b, 81-519 Gdynia, Tel.:58 699 85 06, adres e-mail: dyrekcja@ucmmit.gdynia.pl.

Inspektor ochrony danych

We wszystkich sprawach dotyczących ochrony danych osobowych, ma Pani/Pan prawo kontaktować się z naszym Inspektorem ochrony danych, na adres e-mail: dane_osobowe@ucmmit.gdynia.pl;

Cele przetwarzania i podstawa przetwarzania danych

Pani/Pana dane osobowe przetwarzane są przez UCMMiT na potrzeby (i na podstawie prawnej):

- a) zawarcia lub realizacji zawartej z Panią/Panem umowy (podstawa z art. 6 ust 1 lit. b RODO),
- b) podejmowania działań (takich jak np. ustalenie, dochodzenie lub obrona przed roszczeniami), których skuteczne podjęcie wymaga wykorzystania danych przedstawiciela podmiotu trzeciego, na podstawie naszego prawnie uzasadnionego interesu (podstawa z art. 6 ust. 1 lit. f RODO),
- c) w celu zapewnienia bezpieczeństwa i ochrony mienia, na podstawie naszego prawnie uzasadnionego interesu (podstawa z art. 6 ust. 1 lit. f RODO).

Obowiązek podania danych

Podanie danych osobowych jest wymogiem ustawowym, w związku z czym ich podanie jest obowiązkowe.

Okres przechowywania danych

Pani/Pana dane pozyskane w związku z zawieraną umową, będą przechowywane przez okres nie dłuższy, niż 6 lat od zakończenia umowy. W przypadku roszczeń, dla okresu przedawnienia zastosowanie znajdą ogólne przepisy wynikające z Kodeksu cywilnego.

Odbiorcy danych

Pani/Pana dane mogą być przekazywane następującym kategoriom odbiorców:

- a) podmiotom uprawnionym na podstawie przepisów prawa;

- b) podmiotom współpracującym z UCMMiT, z którymi Administrator zawarł umowy lub porozumienia, jak:
- a. dostawcy usług teleinformatycznych i księgowych,
 - b. obsługa prawna i doradcza,
 - c. firmom realizującym usługi związane z utylizacją dokumentacji i innych nośników zawierających dane osobowe.

Przekazywanie danych poza Europejski Obszar Gospodarczy (EOG)

Pani/Pana dane osobowe nie będą przekazywane do państw trzecich ani organizacji międzynarodowych.

Zautomatyzowane podejmowanie decyzji

W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, w tym również w formie profilowania.

Prawa osób

Posiada Pani/Pan prawo do:

- a) dostępu do swoich danych osobowych, ich sprostowania, żądania od Administratora usunięcia lub ograniczenia przetwarzania danych osobowych;
- b) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (00-193 Warszawa, ul. Stawki 2, e-mail: kancelaria@uodo.gov.pl), gdy uzna Pani/Pan, że przetwarzanie danych osobowych dotyczących Pani/Pana narusza przepisy RODO.

Klauzula informacyjna

1. Administratorem Państwa danych osobowych jest Uniwersyteckie Centrum Medycyny Morskiej i Tropikalnej (dalej UCMMiT), 81-519 Gdynia, ul. Powstania Styczniowego 9B, KRS 0000174213. Kontakt z administratorem jest możliwy poprzez tel. 586998506 lub e-mail: dyrekcja@ucmmit.gdynia.pl
2. Administrator powołał Inspektora Ochrony Danych Osobowych: Andrzej Fortuna, z którym można skontaktować się na nr telefonu: 586998506, e-mail: dane_osobowe@ucmmit.gdynia.pl, lub korespondencyjnie na adres siedziby Administratora.
3. Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. c) 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), zwanego dalej RODO (realizacja obowiązku ciążącego na administratorze) w związku z przepisami *ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich*.
4. Dane osobowe będą przetwarzane w celu realizacji ustawowego obowiązku administratora, w związku z ochroną małoletnich, w zakresie weryfikacji kandydata w odpowiednich rejestrach i potwierdzenia niekaralności.
5. Podane dane osobowe będą udostępniane wyłącznie podmiotom uprawnionym do ich przetwarzania na podstawie przepisów prawa. Dane osobowe będą udostępnione podmiotom zapewniającym, na podstawie umów zawartych przez administratora, obsługę działalności administratora (dostawcy usług informatycznych, poczty elektronicznej). Dane osobowe mogą być udostępnione organom właściwym do prowadzenia postępowania w związku z podejrzeniem krzywdzenia małoletniego.
6. Dane osobowe będą przechowywane przez czas trwania stosunku pracy, a po jego ustaniu, przez czas niezbędnej archiwizacji określonej przepisami prawa.
7. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia w przypadkach przewidzianych przepisami prawa oraz ograniczenia przetwarzania.



8. Posiada Pani/Pan prawo wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 3, 00 – 193 Warszaw), jeżeli uzna, iż przetwarzanie danych osobowych narusza przepisy RODO.
9. Podanie danych osobowych jest wymogiem ustawowym. Konsekwencją niepodania danych jest brak możliwości zatrudnienia.
10. Dane osobowe nie będą podlegały profilowaniu ani na podstawie tych danych, nie będą podejmowane decyzje w sposób zautomatyzowany.

MR