Polityka bezpieczeństwa danych osobowych

KMM Grzegorz Mączka ul Leśna 1A 84-230 Rumia NIP 588-219-01-80

WSTĘP

1. Dokument, zwany dalej Polityką Bezpieczeństwa stanowi politykę bezpieczeństwa danych osobowych KMM Grzegorz Mączka ul Leśna 1A 84-230 Rumia. Polityka Bezpieczeństwa reguluje całościowo dopuszczalny przez prawo sposób zarządzania i ochrony danych osobowych oraz prawa osób, których dane osobowe są przetwarzane w ramach działalności jednostki.
2. Celem Polityki jest wskazanie działań, jakie należy podjąć, formy tych działań, oraz sposób ich przeprowadzania, aby wykonać ciążące na podmiotach przetwarzających dane osobowe obowiązki, o których mowa w Rozporządzeniu 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), zwane dalej Rozporządzeniem oraz innych obowiązujących przepisach prawa.
3. Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwe udokumentowanie przypadków naruszenia bezpieczeństwa oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych. Polityka określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
4. Postanowienia niniejszej Polityki mają zastosowanie do wszelkich danych osobowych, w rozumieniu 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), a także Dyrektywy Parlamentu Europejskiego i Rady UE 2016/680 z dnia 27 kwietnia 2016 r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.
5. Polityka bezpieczeństwa w sposób szczegółowy opisuje zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych metodami tradycyjnymi oraz w systemie informatycznym.

POSTANOWIENIA OGÓLNE

Definicje

Urząd Ochrony Danych Osobowych – organ do spraw ochrony danych osobowych

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 lub społeczną tożsamość osobie fizycznej.

Dane wrażliwe – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, jak również dane o stanie zdrowia, genetyczne, biometryczne oraz dane dotyczące seksualności lub orientacji seksualnej. Pojęcie to oznacza również dane dotyczące wyroków skazujących i naruszeń prawa.

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

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

Dane dotyczące zdrowia - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej- w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

Administrator Danych – dalej ADO – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych**. Administratorem Danych w firmie [***dane działalności***]**

Przedstawiciel – rozumie się przez to osobę powołaną przez ADO w celu nadzorowania przestrzegania danych osobowych.

Zbiór danych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów.

Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Przetwarzanie danych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub łączenie.

Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się

Odbiorca – oznacza osobę fizyczną lub prawną, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Strona trzecia – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zgoda osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

Uwierzytelnianie – działanie, które celem jest weryfikacja deklarowanej tożsamości podmiotu

§1

Zakres podmiotowy i przedmiotowy Polityki

1. Polityka odnosi się do wszelkich zasobów związanych z realizacją procesów przetwarzania danych osobowych.
2. Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

§2

Zasady ogólne przetwarzania danych osobowych

1. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane: były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą oraz aby zapewniona była rozliczalność, integralność i poufność danych, gdzie przez:
   a. rozliczalność - rozumie się właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   b. integralność danych - rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c. poufność danych - rozumie się właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.
2. Dane osobowe przetwarzane są w sposób transparentny, rzetelny i bezpieczny.
3. Dane osobowe przetwarzane są w konkretnym celu a administrator nie przetwarza większej niż potrzebna do realizacji obowiązku, funkcjonowania administratora l ilości danych osobowych.
4. Administrator dba o prawidłowość przetwarzanych danych, zapewnia możliwość aktualizacji oraz usunięcia w dowolnym momencie.

§3

Zasada celowości i adekwatności

1. Przetwarzanie danych może nastąpić jedynie dla wyraźnie oznaczonych celów.
2. Celem przetwarzania danych osobowych w jednostce są w szczególności:
    a. podejmowanie działań zgodnych z przedmiotem działalności firmy - prowadzeniem gabinetów psychologicznych, prowadzeniem szkoleń, czy warsztatów,
    b. działania marketingowe i promocyjne,
    c. działania informacyjne,
    d. realizacja ciążących na administratorze obowiązków prawnych.
3. Przetwarzane dane muszą być adekwatne do celu, w jakim są zbierane, co oznacza, że możliwe jest przetwarzanie tylko takich danych, które są niezbędne dla realizacji określonego celu.
4. Przetwarzane informacje są w szczególności informacjami dotyczącymi:
    a. danych podstawowych takich jak imię i nazwisko,
    b. dane otrzymane od klientów podczas prowadzenia spotkań, terapii, warsztatów, czy szkoleń (w tym dane wrażliwe dotyczące m.in. stanu zdrowia),
    c. adresu zamieszkania, numeru telefonu, adresu e – mail, numeru NIP,
5. ADO przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. ADO analizuje, czy celowe jest dalsze przetwarzanie danych dla celów marketingowych i promocyjnych.
6. Dane przetwarzane przez Administratora powinny być merytorycznie poprawne, co oznacza, że powinny odzwierciedlać stan faktyczny.
7. Wymagana jest ponowna zgoda na przetwarzanie danych, jeżeli cel przetwarzania uległ zmianie.

§ 4

Wewnętrzne i zewnętrzne ograniczenia dostępu

1. Administrator stosuje ograniczenia dostępu do danych osobowych: prawne (umowy powierzenia, zobowiązania do zachowania poufności, w przypadku zatrudnienia pracowników udzielanie upoważnień do przetwarzania danych osobowych wraz ze wskazaniem zakresu upoważnień) oraz fizyczne (zamykanie pomieszczeń, zamykanie szafek, opieka nad sprzętem komputerowym).
2. Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach w zakresie obowiązków osób, oraz zmianach podmiotów przetwarzających.

3. Dane dot. stanu zdrowia pacjentów gabinetu psychologa sportu pozostają poufne i tylko ADO posiada do nich dostęp. Dane pacjentów gabinetu powinny być przechowywane w sposób uniemożliwiający dostęp do nich i otrzymanie informacji kto jest pacjentem, np. poprzez umieszczenie kartoteki każdego pacjenta osobno w teczkach lub kopertach oznaczonych kodem lub numerem.

POSTANOWIENIA SZCZEGÓŁOWE

§5

Upoważnienie

1. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby upoważnione do przetwarzania danych osobowych przez ADO lub osoby, z którymi zawarto umowy powierzenia danych osobowych.
2. Każda osoba upoważniona do przetwarzania danych osobowych zostaje zapoznana z niniejszą Polityką Bezpieczeństwa, co potwierdza własnoręcznym podpisem.
3. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania poufności.
4. Upoważnienie powinno zawierać:
    a. datę z którą zostało nadane;
    b. datę z którą upoważnienie wygasa jeżeli jest ono nadane na czas określony;
    c. zakres upoważnienia.
5. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.

§6

Zgodność przetwarzania z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z poniższych warunków:
    a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie konkretnie określonych celów;
    b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy;
    c. przetwarzanie jest niezbędne do wykonania obowiązku prawnego ciążącego na administratorze;

d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem.

2. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów administratora, jak też z akt. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez administratora.

§7

Zgoda na przetwarzanie danych osobowych

1. Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, zgoda powinna być udzielona w sposób świadomy, konkretny i jednoznaczny, w możliwy do udokumentowania sposób.
2. Administrator Danych Osobowych jest obowiązany każdorazowo, w przypadku, gdy zgoda jest wymagana, udokumentować udzielenie zgody przez osobę, której dane dotyczą.
3. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
4. Zgoda udzielona przez osobę, której dane dotyczą, może zostać wycofana w każdym momencie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Wycofanie zgody powinno odbywać się w podobny pod względem technicznym sposób, jak jej wyrażenie.
5. Oceniając, czy zgodę wyrażono dobrowolnie, należy uwzględnić, czy od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych nie jest niezbędne do wykonania umowy.
6. Przetwarzanie danych osobowych osoby niepełnoletniej może odbywać się wyłącznie za zgodą osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem. Zabronione jest

przetwarzanie danych osobowych osoby poniżej 16 roku życia bez pisemnej zgody rodzica lub prawnego opiekuna.

§8

Przetwarzanie szczególnych kategorii danych osobowych

1. Administrator w ramach działalności psychologa sportu może przetwarzać dane dot. zdrowia pacjentów. Administrator nie przetwarza danych wrażliwych, genetycznych oraz biometrycznych w ramach prowadzonej działalności na dużą skalę.
2. Gdyby zaszła taka potrzeba, dane wrażliwe, genetyczne i biometryczne mogą być przetwarzane jedynie wówczas, gdy:
    a. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych,
    b. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
    c. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
    d. przetwarzania dokonuje się w ramach uprawnionej działalności z zastosowaniem odpowiednich zabezpieczeń,
    e. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznianych przez osobę, której dane dotyczą.

§9

Obowiązek informacyjny

1. Podczas pozyskiwania danych osobowych osoby, której dane dotyczą, należy podać następujące informacje:
    a. tożsamość i dane kontaktowe Administratora
    b. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania,
    c. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców.
2. W przypadku prowadzenia rekrutacji, klauzule informacyjne wymagane przy zatrudnianiu i rekrutacji znajdą się w aktach osobowych.
3. Obowiązek informacyjny będzie realizowany poprzez:

a. wysyłanie e-maila z informacjami, o których mowa w § 9 ust. 1 niezwłocznie po ujawnieniu e – maila osoby podczas korzystania z formularza kontaktowego na stronie internetowej Administratora,
b. Umieszczenie Polityki Prywatności na stronie internetowej,
c. W przypadku umów zawieranych osobiście, podanie pisemnej informacji w formie wydruku.

§10

Prawo dostępu

1. Osoba, której dane dotyczą jest uprawniona do otrzymania od administratora potwierdzenia, czy przetwarzane są dane jej dotyczące, a jeżeli ma to miejsce jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
    a. cele przetwarzania,
    b. kategorie danych osobowych,
    c. informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
    d. w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
    e. informacje o prawie do do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
    f. informacje o prawie wniesienia skargi do organu nadzorczego,
    g. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle.
2. Jeżeli dane osobowe przekazywane są do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.
3. Administrator danych osobowych dostarcza osobie, której dane dotyczą, na jej żądanie kopie danych osobowych podlegających przetwarzaniu.
4. Prawo do uzyskania kopii, o której mowa w ust. 3 nie może naruszać praw innych osób.

§11

Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

2. Osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych.
3. Administrator informuje o powyższych prawach najpóźniej przy pierwszym kontakcie z osobą, której dane dotyczą.

§12

Prawo do bycia zapomnianym

1. Osoba, której dane dotyczą ma prawo żądania od administratora niezwłocznego usunięcia całości lub części jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć jej dane osobowe, jeśli zachodzi jedna z poniższych okoliczności:
    a. dane osobowe nie są już niezbędne do celów, do których zostały zebrane lub w inny sposób przetwarzane,
    b. osoba, której dane dotyczą cofnęła zgodę,
    c. osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawne podstawy przetwarzania,
    d. dane osobowe były przetwarzane niezgodnie z prawem,
    e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.
2. Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.
3. Jeżeli dane podlegające usunięciu zostały upublicznione, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować inne podmioty przetwarzające te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.
4. W przypadku usunięcia danych Administrator informuje osobę, której dane dotyczą o odbiorcach danych, na żądanie tej osoby.
5. Administrator informuje o powyższych prawach najpóźniej przy pierwszym kontakcie z osobą, której dane dotyczą.

§13

Naruszenia

1. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania art. 33 RODO.
2. Rejestr zawiera okoliczności naruszeń, skutki, oraz podjęte działania zaradcze, w tym przekazanie informacji ADO.
3. W przypadku naruszenia przez osobę inną niż administrator, należy w pierwszej kolejności poinformować ADO.
4. ADO jest zobowiązany zgłosić fakt naruszenia organowi nadzorczemu, chyba, że jest mało prawdopodobne, aby doszło do naruszenia praw lub wolności osób fizycznych. Zgłoszenie powinno nastąpić nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.
5. Zgłoszenie naruszenia zawiera: opis charakteru naruszenia ze wskazaniem kategorii i liczby osób, których dane dotyczą, imię nazwisko i informacje kontaktową do ADO, opis możliwych konsekwencji, opis zastosowanych lub planowanych środków zaradczych.
6. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:
    a. **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu**, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
    b. **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
    c. **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub sabotaż;
    d. **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
    e. **pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego** wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
    f. **naruszenie lub próba naruszenia** integralności systemu lub bazy danych w tym systemie;
    g. stwierdzona **próba modyfikacji lub modyfikacja danych lub zmiana** w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
    h. **niedopuszczalna manipulacja** danymi osobowymi w systemie;

i. **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
j. **nieprzypadkowe odstępstwa od zasad bezpieczeństwa pracy w systemie lub sieci komputerowej** wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;
k. **istnienie nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki" itp.;
l. **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;

§14

1. Zapewnia się stosowanie ustawień zapewniających ochronę danych jako pierwotnych ustawień systemu informatycznego czy oprogramowania.
2. Domyślnie przetwarzane są wyłącznie dane osobowe, które są niezbędne dla celu przetwarzania.
3. Administrator Danych Osobowych zapewnia, by domyślnie przetwarzane dane osobowe nie były udostępniane bez aktywności osoby, której dane dotyczą nieokreślonej liczbie osób fizycznych.
4. Niezbędność danych do osiągnięcia konkretnego celu przetwarzania jest rozpatrywana poprzez:
    a. ilość zbieranych danych osobowych,
    b. zakres ich przetwarzania,
    c. okres ich przechowywania,
    d. ich dostępności.

§15

Bezpieczeństwo przetwarzania

1. Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia

praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

2. Administrator, biorąc pod uwagę stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku.
3. Czynności zmierzające do zapewnienia bezpieczeństwa przetwarzania mogą polegać na:
    a. szyfrowaniu danych osobowych poprzez wysyłki systemem informatycznym przy zastosowaniu kwalifikowanego podpisu,
    b. ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
    c. przywracanie dostępności danych w razie incydentu fizycznego lub technicznego;
    d. regularne testowanie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
    e. zapewnienie odpowiedniego stanu wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i możliwych do podjęcia działaniach − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
4. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko związane z przetwarzaniem, to jest ryzyko:
    a. przypadkowego lub niezgodnego z prawem zniszczenia, utraty lub modyfikacji danych osobowych;
    b. nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
5. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.
6. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
7. Jeśli okaże się, że wysokie ryzyko naruszenia praw i wolności osób występuje w kilku przypadkach, to administrator decyduje, gdzie ryzyko naruszenia jest największe i ten przypadek jest rozpatrywany jako pierwszy.

§16

Zasada czystego biurka i czystego ekranu

1. Zabronione jest pozostawianie dokumentów zawierających dane osobowe podczas nieobecności osoby upoważnionej przy stanowisku pracy, jak również nośników danych. Pokój, w którym znajdują się dokumenty i nośniki danych z danymi osobowymi powinien zostać zamknięty w sposób uniemożliwiający dostęp osób nieuprawnionych. Po zakończeniu pracy należy dokumenty oraz nośniki z danymi przechowywać w zamkniętych szafach i w zamkniętych pokojach.
2. Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone wylogowaniem się użytkownika lub zablokowaniem dostępu do systemu informatycznego, aby uniemożliwić dostęp do systemu osobom trzecim. Komputery i inne urządzenia służące do pracy w jednostce posiada system automatycznego uruchamiania wygaszacza ekranu. Monitory ekranów powinny być ustawione w taki sposób, aby uniemożliwić osobom trzecim wgląd w dane osobowe na nich wyświetlane. Po zakończeniu pracy należy wylogować się i wyłączyć urządzenie.
3. Zabrania się przebywania osób nieuprawnionych w pomieszczeniach, w których przetwarzane są dane osobowe, chyba że ADO wyraził zgodę na powyższe lub osoby te przebywają w obecności osoby upoważnionej do przetwarzania danych osobowych.

§17

Obowiązki komunikacyjne

1. Administrator Danych Osobowych dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. ADO ułatwia osobom korzystanie z ich praw poprzez działania takie jak: zamieszczenie na stronie internetowej administratora informacji o prawach osób, sposobie korzystania z tych praw, w tym wymagań dotyczących identyfikacji, metodach kontaktu z administratorem.
3. Administrator dba o dotrzymywanie terminów realizacji obowiązków przewidzianych przez prawo.
4. Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki.
5. Administrator dokumentuje realizację obowiązków informacyjnych oraz realizację żądań osób, których dane dotyczą.
6. Administrator danych osobowych informuje każdą osobę, której dane dotyczą o każdym przypadku pobierania danych.
7. W przypadku wykorzystania wizerunku osoby fizycznej np. do celów promocyjnych, administrator pobiera stosowną zgodę, a ponadto informuje w sposób szczegółowy w jaki sposób wizerunek może zostać wykorzystany.

§18

Podmiot przetwarzający

1. Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. W przypadku pacjentów gabinetu psychologa sportu, wymaga się, by wyrazili pisemną zgodę na podpowierzenie danych osobowych kolejnemu podmiotowi.
2. Podmiot, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.
3. Podmiot, któremu powierzono przetwarzanie danych obowiązany jest przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające przetwarzanie danych, o których mowa w ustawie oraz w rozporządzeniu.
4. Miejscem przetwarzania danych osobowych które powierza się podmiotowi zewnętrznemu będzie siedziba tego podmiotu.

POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych w niniejszej Polityce, zastosowanie znajdują przepisy 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) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018 r. poz. 1000).
2. Przy zarządzaniu ryzykiem należy dążyć do minimalizacji ryzyka wysokiego na rzecz ryzyka małego i średniego stosując w tym celu adekwatne środki zapobiegawcze i monitoring wskazany przez Administratora Danych Osobowych.
3. Administrator Danych Osobowych sporządza samodzielnie Analizę Ryzyka, podobnie jak zbiory danych przetwarzanych przez Administratora, uwzględniając specyfikę przedmiotu swojej działalności.
4. Zmiany niniejszej Polityki Bezpieczeństwa wymagają każdorazowo formy pisemnej.