

POLITYKA OCHRONY DANYCH OSOBOWYCH

POLSKIE TOWARZYSTWO MEDYCYNY NUKLEARNEJ
ul. Banacha 1A 02-097 Warszawa

:

Podpis administratora danych

Warszawa, 2026 r.

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia 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) w stowarzyszeniu **Polskie Towarzystwo Medycyny Nuklearnej z siedzibą w Warszawie** wprowadza się Politykę Ochrony Danych Osobowych (PODO), której celem jest wskazanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Rozdział 1

Definicje

§ 1. Ilekroć w dokumencie jest mowa o:

- a) **administratorze** – oznacza to **Polskie Towarzystwo Medycyny Nuklearnej z siedzibą w Warszawie, adres: ul. Banacha 1A 02-097 Warszawa, NIP 701-03-32-196, Regon 010139693,**
- b) **danych osobowych** – oznacza 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,
- c) **naruszeniu 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,
- d) **odbiorcy danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania,
- e) **organie nadzorczym** – Prezes Urzędu Ochrony Danych Osobowych lub ewentualnie właściwy organ nadzorczy w zakresie Danych osobowych wyznaczony przez inne państwo członkowskie Unii Europejskiej,
- f) **państwie trzecim** – oznacza państwo nienależące do Europejskiego Obszaru Gospodarczego,

- g) **podmiocie przetwarzającym** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,
- h) **PODO** – Polityce Ochrony Danych Osobowych - oznacza to niniejszy dokument,
- i) **współpracownika** – oznacza osobę fizyczną świadczącą na rzecz Administratora usługi na podstawie umowy cywilnoprawnej (zlecenia, o dzieło lub innych),
- j) **przetwarzaniu danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nieautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
- k) **rozporządzeniu lub RODO** – oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

Rozdział 2

Zasady ogólne

§ 2. Niniejsza PODO stanowi podstawowy dokument regulujący zasady przetwarzania Danych osobowych przez Administratora.

§ 3. Wdrożenie PODO ma na celu zapewnienie zgodności z RODO procesów przetwarzania Danych osobowych przez Administratora, bez względu na formę (elektroniczną bądź papierową), w jakiej to przetwarzanie następuje. W tym celu Administrator danych w szczególności uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne.

§ 4. Środki, o których mowa w § 2, są w razie potrzeby poddawane przeglądowi i uaktualniane.

§ 5. W związku z prowadzoną działalnością Administrator zbiera i przetwarza Dane osobowe zgodnie z następującymi zasadami przetwarzania:

- a) Administrator zapewnia, że przetwarzanie przez niego Danych osobowych jest zgodne z prawem i odbywa się w oparciu o jedną z podstaw przetwarzania określonych w RODO, tj. w art. 6 ust. 1, art. 9 ust. 2 albo art. 10 (zasada zgodności z prawem);
- b) Administrator zapewnia rzetelność i przejrzystość przetwarzania Danych osobowych, w szczególności zawsze informuje o przetwarzaniu Danych osobowych w momencie ich zbierania, w tym o celu i podstawie prawnej przetwarzania (zasada rzetelności i przejrzystości);
- c) Administrator zapewnia, że Dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie są przetwarzane dalej w sposób niezgodny z tymi celami (zasada ograniczenia celu);
- d) Administrator zapewnia, że przetwarza dane wyłącznie w zakresie niezbędnym do realizacji celu, dla którego Dane osobowe zostały zebrane (zasada minimalizacji);

- e) Administrator zapewnia, że przetwarzane przez niego Dane osobowe są prawidłowe i w razie potrzeby uaktualniane oraz że podejmuje on wszelkie rozsądne działania, aby Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości);
- f) Administrator zapewnia, że Dane osobowe są przetwarzane tylko przez okres, w jakim jest to niezbędne dla zrealizowania celów przetwarzania (zasada ograniczenia czasowego);
- g) Administrator zapewnia bezpieczeństwo Danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez wdrożenie odpowiednich środków technicznych lub organizacyjnych (zasada integralności i poufności).
- h) Administrator poprzez odpowiednie środki techniczne i organizacyjne zapewnia możliwość wykazania zgodności przetwarzania Danych osobowych z RODO oraz pozostałymi przepisami dotyczącymi Danych osobowych (rozliczalność).

§ 6. Administrator zapewnia przestrzeganie PODO przez wszystkich Współpracowników Administratora.

§ 7. Administrator do przetwarzania danych dopuszcza wyłącznie osoby upoważnione przez administratora na podstawie udzielone upoważnienia do przetwarzania danych zgodnie z załącznikiem nr 1 – Oświadczenie wraz z upoważnieniem do przetwarzania danych osobowych.

Rozdział 3

Środki techniczne i organizacyjne

§ 8. W celu ochrony danych osobowych stosuje się następujące **środki ochrony fizycznej danych osobowych**:

- a) zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi (niewzmacnianymi, nieprzeciwpożarowymi);
- b) zbiory danych osobowych w formie papierowej, kopie zapasowe/archiwalne przechowywane są w zamkniętych niemetalowych szafach;
- c) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;
- d) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

§ 9. W celu ochrony danych osobowych stosuje się następujące **środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej oraz środki ochrony w ramach narzędzi programowych**:

- a) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
- b) zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji;
- c) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
- d) użyto system Firewall do ochrony dostępu do sieci komputerowej;

- e) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
- f) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 10. W celu ochrony danych osobowych stosuje się następujące **środki organizacyjne**:

- a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
- b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
- c) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy,
- d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
- e) administrator danych określił podstawowe zasady bezpieczeństwa, obowiązujące wszystkich współpracowników, czyli:
 - zasada wiedzy koniecznej – ograniczanie dostępu do danych jedynie do tych, które są niezbędne do wykonywania obowiązków na danym stanowisku,
 - zasada odpowiedzialności za zasoby – osoba przetwarzająca jest odpowiedzialna za dane, które przetwarza i zobowiązana jest przestrzegać ustanowionych procedur bezpieczeństwa w tym zakresie,
 - zasada zamkniętego pomieszczenia – niepozostawianie osób postronnych samych w pomieszczeniu (pod nieobecność osoby upoważnionej),
 - zasada czystego biurka – niepozostawianie bez nadzoru dokumentów papierowych oraz nośników danych na biurku (płyty CD, DVD, pamięci flash USB itp.),
 - zasada poufności haseł i kodów dostępu – zachowanie poufności i nieprzekazywanie osobom nieuprawnionym haseł i kodów dostępu, w szczególności zasada ta dotyczy osobistych haseł dostępu do systemów teleinformatycznych i stref chronionych,
 - zasada zmiany haseł – obowiązek zmiany haseł co najmniej co 60 dni,
 - zasada czystego ekranu – blokowanie komputera przed każdym opuszczeniem pomieszczenia, w przypadku dłuższej nieobecności w pomieszczeniu konieczne jest wylogowanie się z systemu,
 - zasada czystego pulpitu – na pulpicie komputera powinny znajdować się jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty do folderów pod warunkiem, że w nazwie nie zawierają danych, w szczególności danych osobowych, które mogą zostać w sposób niekontrolowany ujawnione (np. podczas prezentacji),
 - zasada czystych drukarek/kserokopiarek – zabieranie dokumentów z drukarek zaraz po ich wydrukowaniu, w szczególności zasada ta dotyczy dokumentów pozostawianych w drukarkach znajdujących się w innym pomieszczeniu,

- zasada czystego kosza – dokumenty papierowe z wyjątkiem materiałów promocyjnych powinny być niszczone w niszczarkach lub za pośrednictwem firmy zewnętrznej,
- zasada legalności oprogramowania – zakaz samodzielnego instalowania oprogramowania na sprzęcie służbowym, w tym w szczególności przechowywania na komputerze treści naruszających prawa autorskie oraz innych nielegalnych danych,
- zasada zgłaszania incydentów bezpieczeństwa – każdy przetwarzający dane zobowiązany jest do zgłaszania incydentów związanych z bezpieczeństwem informacji, tj. nieuprawnionym ujawnieniem, zniszczeniem lub modyfikacją informacji, zgodnie z trybem określonym w rozdziale 8,
- zasada korzystania z zasobów– dane, będące w posiadaniu administratora danych, mogą być przetwarzane wyłącznie w środkach przetwarzania dopuszczonych do wykorzystania u administratora,
- zasada nieużywania nazw zawierających dane osobowe w zakresie określania plików, folderów, itp.
- zasada szyfrowania (hasłowania) plików zawierających dane osobowe przed wysłaniem ich za pomocą poczty elektronicznej – wysyłając pliki/dokumenty zawierające dane osobowe, należy je zabezpieczyć hasłem i dopiero przestać mailem, następnie innym kanałem komunikacji (telefon, sms) podać odbiorcy hasło do rozkodowania pliku/dokumentu,
- zasada korzystania ze sprzętu (komputerów przenośnych, telefonów, smartfonów i tabletów) – tego typu urządzenia wykorzystywane do obowiązków służbowych muszą posiadać licencjonowany i aktualny program antywirusowy, dostęp do takiego urządzenia musi być zabezpieczony hasłem, a użytkownik ma dochować należytej staranności, aby przetwarzane na tych urządzeniach dane osobowe, przetwarzane były w sposób prawidłowy zgodny z przepisami ochrony danych oraz bezpiecznie, w szczególności nie zezwalać na używanie sprzętu przez osoby nieupoważnione.

Rozdział 4

Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 11. Administrator danych przeprowadza analizę ryzyka dla zasobów biorących udział w procesach zgodnie z załącznikiem nr 2 – Proces zarządzania ryzykiem.

§ 12. Analiza ryzyka stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.

§ 13. Na podstawie wyników przeprowadzonej analizy ryzyka, administrator danych samodzielnie wdraża sposoby postępowania z ryzykiem.

Rozdział 5

Ocena skutków dla ochrony danych

§ 14. Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii- ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator

przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Administrator zobowiązany jest wtenczas w szczególności:

1. opisać planowane operacje przetwarzania i cele przetwarzania,
2. określić zagrożenia we wszystkich aktywach biorących udział w procesie przetwarzania,
3. sporządzić mapy ryzyka ze wskazaniem istotności ryzyka, zaplanować środki techniczne, organizacyjne i informatyczne dla ryzyk przekraczających optymalną istotność.

Rozdział 6

Procedura współpracy z podmiotami zewnętrznymi

§ 15. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych. zgodnie z załącznikiem nr 3 – Wzór umowy powierzenia przetwarzania danych.

§ 16. Każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z rozporządzeniem wszystkich podmiotów przetwarzających, z których usług ma zamiar skorzystać z wykorzystaniem procedury współpracy z podmiotami zewnętrznymi, zgodnie z załącznikiem nr 4 – Lista kontrolna.

Rozdział 7

Procedura domyślnej ochrony danych

(uwzględnianie ochrony danych w fazie projektowania)

§ 17. W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania. Wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były tylko te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (ilość zbieranych danych, zakres i okres przetwarzanych danych oraz ich dostępność).

Rozdział 8

Procedura zarządzania incydentami

§ 18. Każdy współpracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych, w szczególności danych osobowych, bądź pozyskania informacji o naruszeniu postanowień PODO, w szczególności:

- a) niewłaściwego zabezpieczenia fizycznego pomieszczeń, urządzeń bądź dokumentów,
- b) niewłaściwego zabezpieczenia sprzętu informatycznego, oprogramowania przed kradzieżą, utratą danych,
- c) nieprzestrzegania zasad ochrony danych, w tym danych osobowych, przez współpracowników (np. poprzez niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
- d) pewności lub podejrzenia, że jego hasło zostało ujawnione osobie niepowołanej,
- e) pewności lub podejrzenia wtargnięcia do komputera przez osoby niepowołanej,
- f) pewności lub podejrzenia podłączenia do gniazda sieciowego lub do stacji roboczej urządzenia bez wiedzy administratora,

- g) pewności lub podejrzenia obecności oprogramowania, które zostało zainstalowane bez wiedzy administratora,
- h) znalezienia danych administratora bez należytej ochrony (np. dyskietka/CD/DVD/pendrive poza pomieszczeniami biurowymi, pliki w Internecie, itp.),
- i) znalezienia w dowolnym miejscu zapisanego identyfikatora sieciowego wraz z hasłem,

zobowiązany jest natychmiast zgłosić takie naruszenie do administratora lub osoby przez niego wyznaczonej.

§ 19. W każdym przypadku naruszenia ochrony danych osobowych, administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

§ 20. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu **72 godz.** od identyfikacji naruszenia.

§ 21. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności zgodnie z załącznikiem nr 5 - Zawiadomienie osoby, której dane dotyczą, o naruszeniu.

§ 22 Administrator danych dokumentuje naruszenia oraz prowadzi rejestr naruszeń, które skutkują naruszeniem praw i wolności osób fizycznych.

Rozdział 9

Procedura realizacji praw osób

§ 23. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.

§ 24. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

- a) prawo do informacji o przetwarzaniu danych – Administrator przekazuje osobie zgłaszającej żądanie informację o przetwarzaniu Danych osobowych, w tym przede wszystkim o celach i podstawach prawnych przetwarzania, zakresie posiadanych Danych osobowych, podmiotach, którym są ujawniane, i planowanym terminie usunięcia Danych osobowych;
- b) prawo uzyskania kopii danych – Administrator przekazuje osobie zgłaszającej żądanie kopię Danych osobowych, które jej dotyczą;
- c) prawo do sprostowania danych – Administrator usuwa na żądanie ewentualne niezgodności lub błędy przetwarzanych Danych osobowych oraz uzupełnia je, jeśli są niekompletne;
- d) prawo do usunięcia danych – Administrator na żądanie usuwa albo zanonimizuje Dane osobowe, których przetwarzanie nie jest już niezbędne do realizowania żadnego z celów, dla których zostały zebrane;
- e) prawo do ograniczenia przetwarzania danych – Administrator na żądanie zaprzestaje wykonywania operacji na Danych osobowych – z wyjątkiem operacji, na które Podmiot danych wyraził zgodę – oraz ich przechowywania, zgodnie z przyjętymi zasadami retencji lub dopóki nie ustaną przyczyny ograniczenia przetwarzania Danych osobowych (np. zostanie wydana decyzja Organu nadzorczego zezwalająca na dalsze przetwarzanie);

- f) prawo do przenoszenia danych – w zakresie, w jakim Dane osobowe są przetwarzane w sposób zautomatyzowany w związku z zawartą umową lub wyrażoną zgodą, Administrator na żądanie wydaje Dane osobowe dostarczone przez osobę, której dotyczą, w formacie pozwalającym na odczyt Danych osobowych przez komputer;
- g) prawo sprzeciwu wobec przetwarzania danych w celach marketingowych – Podmiot danych może w każdym momencie sprzeciwić się przetwarzaniu Danych osobowych w celach marketingowych, bez konieczności uzasadnienia takiego sprzeciwu;
- h) prawo sprzeciwu wobec innych celów przetwarzania danych – Podmiot danych może w każdym momencie sprzeciwić się – z przyczyn związanych z jego szczególną sytuacją – przetwarzaniu Danych osobowych, które odbywa się na podstawie prawnie uzasadnionego interesu Administratora;
- i) prawo wycofania zgody – jeśli Dane osobowe przetwarzane są na podstawie wyrażonej zgody, Podmiot danych ma prawo wycofać ją w dowolnym momencie, co jednak nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.

§ 25. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

§ 26. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Rozdział 10

Procedura obowiązku informacyjnego oraz odbierania zgód na przetwarzanie danych

§ 27. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych spełnia obowiązek informacyjny wobec osoby, której dane dotyczą, zgodnie z załącznikiem nr 6 - Wzór klauzuli informacyjnej przy pobieraniu danych osobowych od osoby, której dane dotyczą.

§ 28. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych spełnia obowiązek informacyjny wobec osoby, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z załącznikiem nr 7 - Wzór klauzuli informacyjnej przy pobieraniu danych osobowych od innej osoby niż ta, której dane dotyczą.

§ 29 W każdym przypadku odbierania zgody na przetwarzanie danych od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z załącznikiem nr 8 – Klauzula zgody.

Rozdział 11

Postanowienia końcowe

§ 30. Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.

§ 31. Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.

Załączniki:

1. Załącznik nr 1 - Oświadczenie wraz z upoważnieniem do przetwarzania danych osobowych (wzór),
2. Załącznik nr 2 - Proces zarządzania ryzykiem,
3. Załącznik nr 3 - Umowa powierzenia przetwarzania danych osobowych (wzór),
4. Załącznik nr 4 - Procedura współpracy z podmiotami zewnętrznymi – lista kontrolna,
5. Załącznik nr 5- Zawiadomienie osoby, której dane dotyczą, o naruszeniu (wzór),
6. Załącznik nr 6 - Klauzula informacyjna przy pobieraniu danych osobowych od osoby, której dane dotyczą (wzór),
7. Załącznik nr 7 - Klauzuli informacyjnej przy pobieraniu danych osobowych od innej osoby niż ta, której dane dotyczą (wzór),
8. Załącznik nr 8 - Klauzula zgody (wzór).