POLITYKA OCHRONY DANYCH

DOMU POMOCY SPOŁECZNEJ

IM. HR ELIGIUSZA DUCHODOLSKIEGO

W GOŚCIERADOWIE

Spis treści

1 Informacje wstępne

Polityka ochrony danych zwana dalej „Polityką" jest dokumentem wewnętrznym Domu Pomocy Społecznej w Gościeradowie i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

Każda osoba mająca dostęp do danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści, wg ***załącznika nr 1*** do niniejszej Polityki -Wykaz osób zapoznanych z Polityką.

2 Cel wdrożenia Polityki Ochrony Danych

Celem opracowania i wdrożenia Polityki jest zdefiniowanie ogólnych wymagań i zasad ochrony, które będą fundamentem dla wszystkich dokumentów związanych z ochroną danych osobowych.

3 Deklaracja stosowania

Administrator ustanawia Politykę oraz deklaruje:

- podejmowanie wszystkich działań niezbędnych dla zapewnienia legalności przetwarzanych danych,
- stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane w zakresie problematyki bezpieczeństwa tychże danych,
- stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym,
- dążenie do zapewnienia poufności, dostępności oraz integralności informacji chronionych w tym szczególnie danych osobowych.

4 Podstawa prawna

Polityka została przygotowana w oparciu o:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia

dyrektywy 95/46/WE, zwane w dalszej części Polityki „RODO";

2) Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

5 Definicje

1) **Administrator** - Dom Pomocy Społecznej w Gościeradowie, reprezentowany przez Dyrektora; ustala cele i sposoby przetwarzania danych osobowych;
2) **Inspektor Ochrony Danych /IDO/** - osoba, wyznaczona przez Administratora lub podmiot przetwarzający, posiadająca odpowiednie kwalifikacje zawodowe (wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wymagane do wypełniania zadań związanych z ochroną tych danych;
3) **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4) **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;
5) **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;
6) **Ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
7) **Odbiorca** 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;

8) **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
9) **Pseudonimizacja** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
10) **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;
11) **Użytkownik**- osoba posiadająca dostęp do systemu informatycznego przetwarzającego dane osobowe,
12) **Zgoda** 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;
13) **Zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

6 Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych

6.1 Administrator

1) wdraża odpowiednie środki techniczne i organizacyjne, mające na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych;

2) wyznacza Inspektora Ochrony Danych, o czym zawiadamia Prezesa Urzędu Ochrony Danych Osobowych;
3) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia przetwarzanych danych zgodnie z procedurą stanowiącą integralną część niniejszej Polityki;
4) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie;
5) podejmuje decyzje dotyczące przeprowadzenia oceny skutków planowanych operacji przetwarzania danych po konsultacji z Inspektorem Ochrony Danych;
6) wdraża rejestr czynności przetwarzania danych osobowych;
7) wdraża Politykę ochrony danych osobowych.

6.2 Inspektor Ochrony Danych /IOD/

1) informuje Administratora oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy obowiązujących przepisów, kodeksów postępowania i zatwierdzonych mechanizmów certyfikacji;
2) prowadzi szkolenia z zakresu ochrony danych osobowych;
3) aktualizuje i sprawuje nadzór nad dokumentacją z zakresu ochrony danych osobowych;
4) opracowuje rejestr czynności przetwarzania danych i dokonuje jego bieżącej aktualizacji;
5) współpracuje z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych;
6) pełni funkcję punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych.

7 Podstawy przetwarzania danych osobowych

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 RODO w przypadku przetwarzania danych zwykłych. Dane osobowe w jednostce przetwarzane są gdy:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

2) 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;
3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

W przypadku przetwarzania danych na podstawie zgody osoby, której dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, którego wzór stanowi **załącznik nr 2** do niniejszej Polityki, natomiast **załącznik nr 3** stanowi wzór oświadczenia o odwołaniu zgody na przetwarzanie danych osobowych.

7.1 Obowiązek informacyjny przy przetwarzaniu danych

Obowiązek informacyjny spoczywający na administratorze w myśl art. 13 i 14 RODO jest realizowany poprzez przekazanie osobie, której dane są przetwarzane informacji dotyczących pozyskiwania danych osobowych, a także ich dalszego przetwarzania. Obowiązek informacyjny jest realizowany zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak również z innych źródeł.

Jedną z form spełniania obowiązku informacyjnego jest ***załącznik nr 4*** do niniejszego dokumentu, stanowiący jego integralną część.

Administrator realizuje obowiązek informacyjny poprzez wykorzystanie odpowiednich środków, które umożliwią w zwięzłej, przejrzystej i łatwo dostępnej formie udzielenie osobie, której dane dotyczą wszelkich informacji, o których mowa w art. 13 i 14 RODO.

Zwolnienie z realizacji obowiązku informacyjnego znajduje zastosowanie w sytuacji, gdy dane pozyskiwane są od osoby, której te dane dotyczą a podmiot ten dysponuje już informacjami, o których mowa w art. 13 RODO oraz w zakresie uregulowanym przez przepisy krajowe, w szczególności przez ustawę z dnia 10 maja 2018r. o ochronie danych osobowych.

Powyższy obowiązek należy spełnić w momencie zbierania danych.

7.2 Prawa osób, których dane dotyczą

Prawo dostępu do danych, o którym mowa w art. 15 RODO jest realizowane przez Administratora poprzez potwierdzenie faktu przetwarzania danych w miarę możliwości przy użyciu tożsamych środków komunikacji jakie zostały wykorzystane przez osobę kierującą żądanie. W przypadku, gdy przetwarzanie danych w odniesieniu do osoby, której dane dotyczą ma miejsce, wówczas Administrator realizuje uprawnienia dotyczące udzielenia informacji z art. 15 ust. 1 RODO, jak również dostarcza kopię danych, o czym mowa w ustępie 3 ww. artykułu. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze dostępu do danych stanowiącej ***załącznik nr 5*** do niniejszej Polityki.

Prawo do sprostowania danych, o którym mowa w art. 16 RODO jest wykonywane w wyniku żądania osoby, której dane są przetwarzane. Realizacja uprawnienia dotyczy przypadków przetwarzania danych nieprawidłowych, bądź też niekompletnych. Administrator bez zbędnej zwłoki dokonuje sprostowania danych w związku z żądaniem osoby, które może być ponadto potwierdzone poprzez przedłożenie dodatkowego oświadczenia. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze prawa do sprostowania danych stanowiącej ***załącznik nr 6*** do niniejszej Polityki.

Prawo do usunięcia danych spoczywające na administratorze danych jest realizowane, o ile zachodzi jedna z okoliczności, o których mowa w art. 17 ust. 1 lit. a) – f) RODO. Administrator bez zbędnej zwłoki dokonuje usunięcia danych, o ile dalsze przetwarzanie nie jest niezbędne, o czym stanowi art. 17 ust. 3 RODO. Realizacja prawa do usunięcia danych wiąże się również z przekazaniem informacji o konieczności spełnienia żądania przez innych administratorów w sytuacji, gdy dane zostały upublicznione. Administrator weryfikując dostępną technologię oraz koszt realizacji podejmuje rozsądne działania mające na celu poinformowanie innych administratorów. Wykonywanie uprawnień osoby, której dane dotyczą jest zainicjowane żądaniem tej osoby. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze prawo do bycia zapomnianym stanowiącej ***załącznik nr 7*** do niniejszej Polityki.

Prawo do przenoszenia danych jest realizowane w przypadku zaistnienia przesłanek z art. 20 RODO. Wykonywanie uprawnienia, które przysługuje podmiotowi danych jest

inicjowane żądaniem tej osoby. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze prawo do przenoszenia danych stanowiącej ***załącznik nr 8*** do niniejszej Polityki.

Prawo do sprzeciwu w stosunku do przetwarzanych danych jest realizowane w przypadku zaistnienia przesłanek z art. 21 RODO. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze prawo do sprzeciwu przetwarzania danych stanowiącej ***załącznik nr 9*** do niniejszej Polityki.

7.3 Zasady dokonywania anonimizacji danych osobowych w dokumentach publikowanych w stronie internetowej

1) Pracownik, sporządzający dokumenty, które mają zostać umieszczone na stronie internetowej jednostki zobowiązany jest do wstępnej oceny przedmiotowego dokumentu pod względem dopuszczalności publikacji danych osobowych osób fizycznych niepełniących funkcji publicznych lub kierowniczych.
2) W sytuacji stwierdzenia obecności danych osobowych osób fizycznych w dokumentach, o których mowa w pkt. 1, użytkownik zobowiązany jest do dokonania analizy legalności publikacji danych osobowych w przedmiotowym dokumencie oraz dokonania anonimizacji zawartych w nich danych osobowych osób fizycznych tj. imion, nazwisk, adresu, nr PESEL, wieku, numeru telefonu, stanu zdrowia itp.
3) Pracownik odpowiedzialny za publikację ww. dokumentów na stronie internetowej jednostki, zobowiązany jest do weryfikacji poprawności dokonanej anonimizacji danych osobowych w tych dokumentach.

7.4 Procedura nadawania upoważnień do przetwarzania danych osobowych

Do przetwarzania danych osobowych mogą mieć dostęp osoby posiadające pisemne upoważnienia do przetwarzania danych osobowych.

1) Referent administracyjny jest odpowiedzialny za przygotowanie upoważnień do przetwarzania danych osobowych dla pracowników jednostki na podstawie zakresu czynności pracownika oraz w przypadku osób zatrudnionych na podstawie umów cywilnoprawnych – zgodnie z zakresem obowiązków uregulowanych treścią umowy, wg wzoru stanowiącego załącznik nr 10 do niniejszej Polityki.

2) Upoważnienia, o których mowa w punkcie 1 zatwierdza Administrator.
3) Zatwierdzone przez Administratora upoważnienie do przetwarzania danych osobowych referent administracyjny wpisuje do ewidencji nadanych upoważnień - stanowiącej **załącznik nr 11** do niniejszej Polityki.
4) W przypadku zmiany stanowiska, zakresu obowiązków lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych referent administracyjny obowiązany jest wydać nowe lub cofnąć upoważnienie.

8 Środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych

Środki techniczne i organizacyjne są opisane w ***załączniku nr 11*** do niniejszej Polityki.

9 Obowiązki po stronie użytkowników

Ze względów bezpieczeństwa przetwarzanych danych użytkowników zobowiązuje się do:

1) **polityki „czystego biurka”** - w trakcie pracy użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych,
2) **polityki „czystego ekranu”** - w przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych,
3) bieżącego niszczenia w niszczarce niepotrzebnej dokumentacji papierowej oraz przechowywania pozostałej dokumentacji papierowej w szafach zamykanych na klucz;

4) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej,
5) zachowania w poufności wszelkich informacji w tym danych osobowych poprzez złożenie stosownego oświadczenia stanowiącego wzór zawarty w ***załączniku nr 14*** do niniejszej Polityki.

10 Przenośne nośniki danych oraz komputery przenośne

Użytkownicy mogą korzystać wyłącznie z elektronicznych nośników (w szczególności pendriv-y, dysków zewnętrznych, CD-R, DVD) oraz komputerów przenośnych przeznaczonych do użytku służbowego.

Użytkownik korzystający z ww. urządzeń zobowiązany jest do:

1) przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej 8 - znakowym zawierającym: małe, wielkie litery, znaki specjalne lub cyfry,
2) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,
3) zdecydowanego i skutecznego uniemożliwienia korzystania z komputera osobom nieuprawnionym (np. rodzinie, dzieciom, znajomym).

11 Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

Dane osobowe przechowywane są w postaci elektronicznej na:

1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu,
2) przenośnych nośnikach elektronicznych.

Dane mogą być przechowywane na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane.

Po ustaniu czasu przechowywania zawartość nośnika podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w jednostce, a w przypadku nośników optycznych stosuje się niszczarki umożliwiające niszczenie tego typu nośników.

Przenośne elektroniczne nośniki informacji zawierające dane osobowe powinny być przechowywane przez użytkowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach lub zamykanych meblach biurowych.

W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane powinny być kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych zaakceptowanego do użycia w jednostce. W przypadku braku możliwości programowego usunięcia danych nośniki danych (w tym dysk) podlega fizycznemu zniszczeniu. Zniszczenie nośnika powinno być potwierdzane protokołem zniszczenia.

Możliwe jest powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

1) zawarcia umowy, o której mowa w art. 28 RODO,
2) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez Administratora lub osobę przez niego wyznaczoną
3) udokumentowania faktu zniszczenia nośników protokołem.

12 Praca w systemach informatycznych

12.1 Procedura nadawania i odbierania uprawnień dla użytkowników w systemie informatycznym

Poniższa procedura ma zastosowanie w przypadku korzystania z systemów informatycznych przetwarzających dane osobowe.

1) Osoba wyznaczona przez Administratora nadaje uprawnienia użytkownikom do pracy w systemach informatycznych na podstawie upoważnienie do przetwarzania danych osobowych.
2) Osoba wyznaczona przez Administratora dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień użytkowników systemów informatycznych.
3) Wyrejestrowanie, o którym mowa w pkt 3, może mieć charakter czasowy lub trwały

4) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

12.2 Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

W przypadku dostępu do systemów informatycznych (dziedzinowych i operacyjnych) Użytkownik powinien stosować co najmniej dwuetapową metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora/ login'u oraz hasła. Identyfikator jest przydzielany wg zasady przyjętej w jednostce. W identyfikatorze pomija się polskie znaki diakrytyczne.

W przypadku dublowania się identyfikatorów powinien być on rozszerzany o kolejne litery lub cyfry.

Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz znaki specjalne. Użytkownik zobowiązany jest do zmiany hasła oraz do zachowania go w poufności i niezapisywania haseł w sposób jawny.

Hasła administracyjne do urządzeń i systemów informatycznych winny być przechowywane w miejscu wskazanym przez Administratora. Powyższa ewidencja powinna zawierać nazwę użytkownika (administratora), hasło, sposób dostępu, adres IP serwera urządzenia. Hasła te podlegają zmianie w cyklu półrocznym oraz w sytuacji, gdy dochodzi do zmian personalnych wśród osób, które miały do nich dostęp lub je znały. Powinny cechować się one właściwą złożonością tzn. co najmniej 12 znaków, 3 z 4 grup znaków (małe litery, duże litery, cyfry, znaki specjalne).

12.3 Sposoby zabezpieczania systemu informatycznego

1) Komputery stacjonarne i przenośne powinny być zabezpieczone programem antywirusowym, które sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu.
2) Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie powinno odbywać się przy wykorzystaniu ww. oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych.

3) Obowiązkiem Administratora nadzór nad aktualizacją oprogramowania antywirusowego. Użytkownik jest obowiązany każdorazowo zawiadomić Administratora o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.

12.4 Przegląd i konserwacja systemów oraz nośników informacji służących do przetwarzania danych

Osoba wyznaczona przez Administratora jest odpowiedzialna za dokonywanie przeglądu i konserwacji systemów oraz nośników służących do przetwarzania danych.

12.5 Zasady bezpiecznego użytkowania sprzętu IT

Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem. Użytkownik ma obowiązek natychmiast zgłosić utratę lub zniszczenie powierzonego sprzętu IT. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączenie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione. Użytkownicy nie mogą bez zgody Administratora korzystać z prywatnego sprzętu IT (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych.

Administrator ma prawo do monitorowania sprzętu służbowego wykorzystywanego przez pracowników, regulacje w tym zakresie wynikają z ustawy o ochronie danych osobowych z 10 maja 2018 roku Dz.U. z 2018 r. poz. 1000).

O fakcie monitorowania Administrator zobowiązany jest powiadomić pracownika, nie później niż 14 dni przed jego uruchomieniem.

Załącznik nr 15 stanowi wzór oświadczenia o monitorowaniu sprzętu komputerowego, na którym pracują użytkownicy.

12.6 Zasady korzystania z oprogramowania

Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w jednostce. Użytkownicy nie mają prawa do instalowania ani

używania oprogramowania innego, niż przekazane lub udostępnione im przez Administratora. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

12.7 Zasady korzystania z Internetu

Dopuszcza się korzystanie przez pracowników ze stron Internetowych w celach służbowych, a także okazjonalnie w celach prywatnych. Podczas korzystania z sieci internetowych niedozwolone jest przeglądanie, a także ściąganie materiałów, których treści są prawnie zakazane, naruszają dobre obyczaje lub uznawane są za obraźliwe. Od pracowników wymaga się także zachowania szczególnej ostrożności w przypadku żądania lub prośby podania kodów, PIN-ów, hasła, numerów kart płatniczych przez Internet, w szczególności tyczy się to żądania podania takich informacji przez rzekomy bank.

W zakresie dozwolonym przepisami prawa, Administrator zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z Internetu pod kątem wyżej opisanych zasad oraz ma prawo blokować dostęp do wybranych stron internetowych.

12.8 Zasady korzystania z poczty elektronicznej

Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celu prowadzenia korespondencji związanej z działalnością jednostki. Podczas przesyłania danych należy zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy dokumentu. Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

W przypadkach gdy wiadomość jest kierowana jednocześnie do kilku adresatów należy używać metody „Ukryte do wiadomości-UDW".

Zabrania się także rozsyłania za pośrednictwem poczty elektronicznej „łańcuszków szczęścia", itp.

Użytkownicy powinni okresowo kasować niepotrzebne wiadomości (tj. spam, oferty handlowe).

Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

12.9 Zasady korzystania z bankowości elektronicznej

Użytkownicy, którzy w zakresie obowiązków maja za zadanie korzystania z bankowości elektronicznej, zobowiązani są do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem. Zabrania się opuszczania stanowiska pracy bez wylogowania się i zamknięcia przeglądarki. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych. W celu zalogowania się do systemu bankowości elektronicznej pracownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.

13 Sposób postępowania z dokumentami papierowymi zawierającymi dane osobowe

W stosunku do dokumentów papierowych stanowiących wydruki z systemu obowiązują następujące środki ostrożności:

1) wydruki i dokumentacja powinny być niedostępne dla osób postronnych,
2) nie mogą być pozostawione w drukarce ogólnodostępnej
3) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki.

Dokumenty, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

14 Przesyłanie dokumentów za pośrednictwem poczty elektronicznej

Dokumenty przesyłane drogą elektroniczną, które nie stanowią informacji publicznej powinno zabezpieczać się przy pomocy środków ochrony kryptograficznej. Ochrona kryptograficzna systemu lub sieci teleinformatycznej polega na stosowaniu metod i środków

zabezpieczających dane, przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych, gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych danych lub uwierzytelnienie podmiotów lub uwierzytelnienie informacji.

Klucze kryptograficzne (hasła, kody, certyfikaty, karty), powinny być zabezpieczone w sposób uniemożliwiający dostęp osobom nieuprawnionym. Rodzaj i model urządzenia kryptograficznego objęty jest zachowaniem poufności w związku z faktem, iż stanowi on element systemu zabezpieczającego.

15 Szkolenia z ochrony danych osobowych

Inspektor Ochrony Danych przeprowadza okresowe szkolenia dla pracowników jednostki zgodnie z poniższymi zasadami:

1) szkolenia wewnętrzne są przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ochrony danych osobowych.
2) nowi użytkownicy mają obowiązek samodzielnie zaznajomić się z przepisami prawa w zakresie danych osobowych oraz treścią Polityki ochrony danych. Ich wiedza jest weryfikowana poprzez test wykonany na platformie e-learningowej.

Administrator informuje Inspektora Ochrony Danych o konieczności przeprowadzenia szkolenia dla pracowników i stażystów.

16 Umowy powierzenia

Umowa powierzenia przetwarzania danych osobowych zawierana jest pomiędzy Administratorem oraz podmiotem przetwarzającym, który przetwarza dane w imieniu Administratora. Szczegółowe zasady dotyczące zawierania umów powierzenia są uregulowane w RODO.

Umowa powierzenia powinna być zawarta przed rozpoczęciem przetwarzania danych przez podmiot przetwarzający.

Wzór umowy powierzenia stanowi ***załącznik nr 16*** do niniejszej Polityki, natomiast wzór rejestru umów powierzenia stanowi ***załącznik nr 17*** do niniejszej Polityki.

17 Procedura zgłaszania naruszeń ochrony danych osobowych

Procedura zgłaszania naruszeń ochrony danych jest opisana w ***załączniku nr 18*** do niniejszej Polityki.

18 Bezpieczeństwo informacji

18.1 Kontrola uprawnień

Kontrola uprawnień ma zastosowanie w przypadku korzystania z systemów informatycznych przetwarzających dane osobowe.

Osoba wyznaczona przez Administratora przeprowadza okresową kontrolę uprawnień i kont użytkowników co najmniej raz w roku, w celu weryfikacji czy użytkownicy posiadają uprawnienia adekwatne do wykonywanej pracy w systemach informatycznych.

18.2 Inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji

Administrator jest odpowiedzialny za prowadzenie inwentaryzacji sprzętu komputerowego i oprogramowania oraz utrzymywanie jej w aktualności.

18.3 Ochrona przetwarzanych informacji

Monitorowanie dostępu do informacji może być realizowane za pomocą: logów aplikacji dziedzinowych oraz logów systemów operacyjnych. Informacje te zawierają: identyfikator i/lub adres IP komputera, dokładną datę, zakres dostępu (przydzielony/odrzucony) oraz opis wykonanej lub zablokowanej akcji.

Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji realizowane są przez ochronę antywirusową.

Wprowadzenie blokady bezpośredniego dostępu stacji roboczych do sieci Internet:

1) umożliwia zablokowanie bezpośredniego połączenia złośliwego oprogramowania z sieci Internet,
2) utrudnia ominięcie systemów zabezpieczeń,
3) umożliwia kontrolę dostępu i rozliczalność działań użytkowników.

19 Przeprowadzanie okresowych analiz ryzyka w zakresie bezpieczeństwa informacji

Głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenie priorytetów dla zarządzania ryzykami i zabezpieczeniami. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem obejmującego wprowadzenie rozwiązań umożliwiających odpowiednio: unikanie tych ryzyk, ograniczanie ich do akceptowanego poziomu, przeniesienie lub świadomą ich akceptację.

Zaleca się, by zarządzanie ryzykiem w bezpieczeństwie informacji zapewniało:

1) zidentyfikowanie ryzyka,
2) oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia,
3) informowanie o prawdopodobieństwie i następstwach ryzyka oraz zrozumienie tych informacji,
4) ustanowienie priorytetów postępowania z ryzykiem,
5) określenie priorytetów dla działań podjętych w celu zredukowania ryzyka,
6) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,
7) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem,
8) szkolenie kierownictwa w zakresie ryzyka oraz działań podejmowanych w celu postępowania z ryzykiem.

20 Audyt wewnętrzny w zakresie bezpieczeństwa informacji

Podmioty realizujące zadania publiczne zobowiązane są do przeprowadzenia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, bowiem utrzymywanie wysokiego poziomu bezpieczeństwa informacji, wymaga stałego monitorowania i okresowego badania stanu zabezpieczenia wszystkich elementów tego systemu.

21 Aktualizacja Polityki Ochrony Danych

Niniejsza polityka podlega regularnym (nie rzadziej niż raz na rok) przeglądom dokonywanym przez Inspektora Ochrony Danych. W zależności od potrzeb mogą zostać przeprowadzone przez niego także dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w jednostce, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie).

Celem przeglądów polityki jest zapewnienie jej rozliczalności w stosunku do realizowanych zadań oraz możliwości obsługi interesantów w każdych warunkach niezależnie od okoliczności i zmian.

22 Wykaz załączników

Nr 1- Wykaz osób zapoznanych z Polityką Ochrony Danych,

Nr 2- Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych,

Nr 3- Wzór odwołania zgody na przetwarzanie danych osobowych,

Nr 4- Wzór klauzuli informacyjnej,

Nr 5- Procedura prawo dostępu do danych,

Nr 6- Procedura prawo do sprostowania danych do danych,

Nr 7- Procedura prawo do bycia zapomnianym,

Nr 8- Procedura prawo do przenoszenia danych,

Nr 9- Procedura prawo do sprzeciwu,

Nr 10- Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych/ uprawnienia do pracy w systemie informatycznym,

Nr 11- Wzór upoważnienia do przetwarzania danych osobowych,

Nr 12- Wzór ewidencji osób upoważnionych do przetwarzania danych,

Nr 13- Opis środków technicznych i organizacyjnych,

Nr 14- Wzór oświadczenia o zachowaniu w poufności danych,

Nr 15 Oświadczenie o monitorowaniu komputerów służbowych.

Nr 16- Wzór umowy powierzenia,

Nr 17- Wzór rejestru umów powierzenia przetwarzania danych osobowych,

Nr 18- Procedura zgłaszania naruszeń ochrony danych osobowych.