REGULAMIN OCHRONY DANYCH

METRYKA DOKUMENTU

Nazwa dokumentu:	**REGULAMIN OCHRONY DANYCH**		
Symbol dokumentu:	ROD		
Wersja (numer):	1.0	z dnia	01.02.2024
Klasyfikacja dokumentu:	Wewnętrzny		
Właściciel dokumentu:	Bi-Med sp. z o.o.		

SPIS TREŚCI

I. Wprowadzenie

§1
Cel funkcjonowania Regulaminu Ochrony Danych

1. **Regulamin Ochrony Danych** określa obowiązujące procedury i zasady postępowania w zakresie ochrony danych osobowych obowiązujące w Bi-med sp. z o.o. (dalej: „**Administrator**").
2. **Regulamin Ochrony Danych** przeznaczony jest do użytku wszystkich osób, które przetwarzają dane osobowe na podstawie upoważnienia udzielonego im przez Administratora.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapoznania się z **Regulaminem Ochrony Danych** wraz z załącznikami stanowiącymi jego integralną część oraz do przestrzegania zawartych w nim postanowień.

§2
System Ochrony Danych Osobowych

1. Na dokumentację dotyczącą systemu ochrony danych osobowych składają się w szczególności 3 podstawowe dokumenty:
   1) **Polityka Ochrony Danych Osobowych,**
   2) **Instrukcja Zarządzania Systemem Teleinformatycznym,**
   3) **Regulamin Ochrony Danych**,
2. Wszystkie inne dokumenty obowiązujące u Administratora, dotyczące choćby częściowo kwestii związanych z ochroną danych osobowych również zaliczają się do szeroko rozumianego systemu ochrony danych osobowych.
3. Dokumentacja ochrony danych osobowych obowiązuje w całej organizacji Administratora, tzn. w siedzibie głównej oraz we wszystkich oddziałach lub filiach, chyba że co innego wynika z treści poszczególnych dokumentów.

II. Słownik pojęć

§3
Stosowane pojęcia

1) administrator - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – Bi-Med sp. z o.o.;
2) anonimizacja - przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów lub działań;
3) dane dotyczące zdrowia (dane o stanie zdrowia) - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym informacje o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia;

4) dane osobowe - 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;
5) incydent - 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) integralność - zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób;
7) inspektor ochrony danych - osoba pełniąca funkcję inspektora ochrony danych w rozumieniu art. 37 RODO;
8) instrukcja – Instrukcja Zarządzania Systemem Teleinformatycznym, jeden z dokumentów wymienionych w §2 ust. 1 niniejszego dokumentu.
9) legalność - zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane zgodnie z prawem, po spełnieniu przynajmniej jednego z warunków określonych w art. 6 ust. 1 lub art. 9 ust. 2 RODO;
10) odbiorca - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego czy jest stroną lub osobą trzecią. Odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach postępowania odbywającego się zgodnie z procedurą określoną w prawie Unii Europejskiej lub prawie państw członkowskiego;
11) ograniczenie celu - zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz gwarantująca nieprzetwarzane danych w sposób niezgodny z tymi celami;
12) okresowość - zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane są przetwarzane;
13) organ nadzorczy - niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych w Unii Europejskiej, zgodnie z art. 51 RODO;
14) osoba upoważniona - osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
15) podmiot leczniczy - podmiot wymieniony w art. 4 ustawy z dnia 25 kwietnia 2011 r. o działalności leczniczej;
16) podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

17) polityka - Polityka Ochrony Danych Osobowych, jeden z dokumentów wymienionych w §2 ust. 1 niniejszego dokumentu;
18) poufność - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
19) pracownik - osoba zatrudniona przez administratora na podstawie umowy o pracę, świadcząca usługi na podstawie umowy cywilnoprawnej, w tym umowy B2B, a także praktykanci, wolontariusze, stażyści i studenci;
20) przetwarzanie - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, 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;
21) pseudonimizacja - 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;
22) regulamin – Regulamin Ochrony Danych, jeden z dokumentów wymienionych w §2 ust. 1 niniejszego dokumentu.
23) RODO - 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 (ogólne rozporządzenie o ochronie danych);
24) rozliczalność przetwarzania - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
25) strona trzecia lub osoba trzecia - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
26) system teleinformatyczny - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne;
27) szacowanie ryzyka - całościowy proces analizy i oceny ryzyka;
28) upoważnienie (do przetwarzania danych) - oświadczenie nadane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
29) uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby upoważnionej;

30) użytkownik – pracownik (rozumiany zgodnie z definicją zawartą w niniejszym Słowniku Pojęć), który uzyskał upoważnienie do przetwarzania informacji w systemach teleinformatycznych administratora;
31) zabezpieczenie - środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną;
32) zagrożenie - niepożądane zdarzenie, które powoduje materializację ryzyka w postaci utraty, ujawnienia, zniszczenia lub zmiany danych osobowych;
33) zbiór danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany bądź zdecentralizowany, rozproszony funkcjonalnie lub geograficznie.

III. Podział zadań i obowiązków w systemie ochrony danych

§4

Struktura obowiązków w systemie ochrony danych osobowych

1) Administrator Danych Osobowych – Bi-Med. sp. z o.o. – decyduje o celach i sposobach przetwarzania danych. Reprezentuje go Zarząd Spółki.
2) Inspektor Ochrony Danych – osoba wyznaczona do pełnienia tej funkcji ma następujące zadania:
    a) Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
    d) współpraca z organem nadzorczym;
    e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem
3) Administrator Systemu Informatycznego – Jest odpowiedzialny w szczególności za zapewnienie bezpieczeństwa danych przetwarzanych w systemie teleinformatycznym administratora poprzez m.in.
    a) dokonywanie audytów infrastruktury systemu teleinformatycznego,
    b) inwentaryzację i konserwację stosowanego sprzętu IT,
    c) reagowanie na incydenty cyberbezpieczeństwa,
    d) nadawanie i odbieranie uprawnień do systemu teleinformatycznego.
4) Bezpośredni przełożeni osób upoważnionych do przetwarzania danych. Do ich zadań należy w szczególności:
    a) Określanie każdorazowo niezbędnego zakresu danych (zbiorów danych), do których upoważnienie do przetwarzania otrzymać powinna osoba im podwładna,

b) Wnioskowanie do ASI o nadanie uprawień do systemu teleinformatycznego ich podwładnym, w zakresie uzasadnionym nadanym upoważnieniem do przetwarzania danych,
c) Odbieranie od osób podwładnych protokołów przekazania sprzętu

5) Osoby upoważnione do przetwarzania danych osobowych – Wszystkie osoby upoważnione do przetwarzania danych osobowych maja obowiązek zapoznania się z niniejszym **Regulaminem Ochrony Danych** i przestrzegania jego postanowień.

IV. Zasady dotyczące nowozatrudnionego pracownika

§5

Uzyskanie niezbędnych dostępów

1. Przed dopuszczeniem do pracy, każda nowozatrudniona osoba, jeżeli z zakresu realizowanych przez nią obowiązków wynika, że w toku wykonywania swoich obowiązków może przetwarzać dane osobowe w imieniu i z upoważnienia Administratora, powinna:
   1) zapoznać się z treścią **Regulaminu Ochrony Danych**,
   2) uzyskać pisemne upoważnienie do przetwarzania danych osobowych, pod którego treścią składa własnoręczny podpis, poświadczając jednocześnie zapoznanie się z obowiązującymi u Administratora procedurami i zasadami przetwarzania danych, w tym z treścią **Regulaminu Ochrony Danych**,
   3) otrzymać sprzęt niezbędny do realizowania nałożonych zadań, którego otrzymanie potwierdza podpisaniem protokołu zdawczo-odbiorczego.
2. Bezpośredni przełożony nowego pracownika, wnioskuje do ASI o nadanie nowemu pracownikowi właściwych dostępów do sieci teleinformatycznej oraz wnioskuję o konfigurację sprzętu IT, który ma zostać udostępniony nowo zatrudnionej osobie, jak również o utworzenie skrzynki pocztowej w domenie Administratora (z wyjątkiem sytuacji, gdy nie jest to zasadne).

§6

Obowiązki nowozatrudnionej osoby

1. Nowo zatrudniona osoba zobowiązana jest zapoznać się z aktualnym rejestrem naruszeń ochrony danych osobowych.
2. Nowo zatrudniona osoba powinna przestrzegać postanowień niniejszego Regulaminu Ochrony Danych.

V. Zasady bezpieczeństwa przetwarzania danych na stanowisku pracy

§7

Sprawdzenie stanowiska przed przystąpieniem do pracy

1. Przed przystąpieniem do pracy, pracownik powinien zwrócić uwagę na stan pomieszczenia, w którym dochodzi do przetwarzania danych osobowych, stanowiska pracy (w tym: biurka,

komputera, szafy) oraz poprawności działania systemu teleinformatycznego i programów, które pracownik wykorzystuje w codziennej pracy.

2. Pracownik Jest zobowiązany niezwłocznie powiadomić bezpośredniego przełożonego i *administratora danych osobowych* o zauważonych brakach w wyposażeniu jego miejsca pracy lub innych pomieszczeń, które uniemożliwiają poprawne zabezpieczenie danych osobowych (np. niesprawne zamki, brak szafek i biurek zamykanych na klucz itd.).
3. Pracownik jest zobowiązany do niezwłocznego zgłoszenia swojemu bezpośredniemu przełożonemu oraz i ASI, każdego problemu związanego z niewłaściwym funkcjonowaniem systemu informatycznego, w tym programu lub aplikacji oraz komputera, a jeśli istnieje uzasadnione podejrzenie, że mogło dojść do naruszenia ochrony danych, zgłosi ten problem również administratorowi danych osobowych.

VI. Podstawowe zasady bezpieczeństwa przetwarzania danych w miejscu pracy

§8

Zasady bezpieczeństwa w miejscu pracy

1. Za bezpośrednie zabezpieczenie obszaru przetwarzania danych przed dostępem osób nieupoważnionych odpowiadają pracownicy, w godzinach swojego przebywania na terenie Administratora.
2. Przebywanie osób nieupoważnionych w pomieszczeniach obszaru przetwarzania danych osobowych dopuszczalne jest wyłącznie w obecności co najmniej jednego pracownika Administratora. Wyjątkiem jest sytuacja, gdzie z okoliczności wynika, że byłoby to znacznie utrudnione lub niecelowe, ale dopuszczalne jest to jedynie wtedy, gdy za pomocą odpowiednich środków technicznych i organizacyjnych, osoby trzecie przebywające w pomieszczeniu przetwarzania danych, zostaną pozbawione faktycznej możliwości dostępu do nich.
3. Każdy pracownik zobowiązany jest zwracać uwagę na przemieszczanie się i przebywanie osób nieupoważnionych w obszarze przetwarzania danych osobowych.
4. Klucze do pomieszczeń oraz szaf i biurek służących do przechowywania danych osobowych należy przechowywać tak, aby nieupoważnione osoby nie miały do nich dostępu w trakcie pracy jak również po jej zakończeniu.
5. Pracownik zobowiązany jest do niepozostawiania narzędzi służących do przetwarzania danych osobowych (laptop, telefon komórkowy, dokumentacja papierowa) bez nadzoru.
6. Pomieszczenia obszaru przetwarzania danych zamyka się na czas nieobecności wszystkich użytkowników w sposób uniemożliwiający osobom nieuprawnionym dostęp do danych.
7. Zabrania się pozostawiania kluczy do pomieszczeń obszaru przetwarzania danych osobowych w drzwiach lub miejscach ogólnie dostępnych.
8. Klucze zapasowe do pomieszczeń, szaf i biurek powinny pozostawać w wyłącznej dyspozycji administratora danych osobowych oraz, jeżeli ten tak postanowi, to również w dyspozycji pracownika, któremu udzielono do tego upoważnienia.

9. Niedopuszczalne jest przetwarzanie danych osobowych w trakcie wykonywania przez osoby trzecie prac remontowych, konserwatorskich lub technicznych w obszarze przetwarzania danych osobowych, chyba że zakres prac nie naruszy bezpieczeństwa poufności, integralności ani rozliczalności ochrony danych osobowych.
10. W przypadku pracowników obsługujących rejestrację – dbanie o należyte zapewnienie bezpieczeństwa i poufności danych podczas obsługi osób przy rejestracji; dokonując rejestracji nowego Pacjenta, pracownik rejestrujący ma obowiązek poinformowania o możliwości zapoznania się z wiszącą obok klauzulą informacyjną dot. przetwarzania danych.

VII. Polityka czystego biurka i ekranu komputera

§9

Zasady czystego biurka i ekranu komputera

1. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie.
2. Należy unikać pozostawiania dokumentów zawierających dane osobowe bez nadzoru.
3. Należy unikać przechowywania na wierzchu dokumentów, w danej chwili niepotrzebnych do bieżących zadań, a zawierające dane osobowe.
4. Każdorazowo odchodząc od biurka oraz po zakończeniu pracy z dokumentami zawierającymi (w szczególności) dane osobowe należy przechowywać je w zamknięciu i nie eksponować w miejscu łatwo dostępnym dla osób postronnych.
5. Dokumenty niepotrzebne do dalszej pracy i niepodlegające archiwizacji należy zniszczyć zgodnie z obowiązującymi w Urzędzie zasadami.
6. Ekrany monitorów komputerów powinny być ustawione tak, by uniemożliwiały widok osobom postronnym.
7. Dostęp do komputera powinien być ograniczony hasłem, znanym wyłącznie użytkownikowi danego komputera.
8. Każdorazowo przy odejściu od biurka należy stosować blokadę ekranu komputera używając kombinacji klawiszy Windows + L.
9. Dla bezpieczeństwa dokumentacji papierowej, napoje pozostawione na biurku nie powinny znajdować w naczyniach podatnych na przewracanie.
10. Po zakończeniu pracy, na biurku powinny pozostać tylko przybory biurowe.
11. Niedopuszczalne jest umieszczanie na pulpicie komputera plików z hasłami, loginami umożliwiającymi dostęp do poszczególnych programów/systemów/aplikacji przez osoby postronne.
12. Niedopuszczalne jest umieszczanie na ekranie monitora haseł i loginów, które umożliwiają dostęp do komputera.
13. Drukując dokumenty z użyciem drukarki, która jest ogólnodostępna pracownicy powinni wydrukowane dokumenty niezwłocznie po wydrukowaniu odbierać.

VIII. Polityka postępowania z dokumentami papierowymi

§10

Postępowanie dokumenty papierowe

1. Obowiązkiem każdego jest dbanie o poufność, integralność i ogólne bezpieczeństwo wszystkich dokumentów papierowych Administratora.
2. Po zakończeniu pracy, dokumenty papierowe zawierające dane osobowe należy przechowywać w zamykanych na klucz szafach lub biurkach (w zależności od wyposażenia danego pomieszczenia).
3. Wydruk i kopiowanie dokumentów odbywa się zawsze w przeznaczonych do tego miejscach. Dokumenty papierowe należy niezwłocznie odbierać z drukarek, kserokopiarek lub innych urządzeń, w szczególności znajdujących się w ciągach komunikacyjnych lub innych miejscach, do których osoby trzecie mogą mieć ułatwiony dostęp.
4. Obowiązuje zakaz pozostawiania lub przechowywania dokumentów poza obszarem przetwarzania danych bez należytego nadzoru.
5. Nie powinno pozostawiać się na biurku dokumentów papierowych w czasie, gdy nie są aktywnie używane.
6. W przypadku czasowego opuszczenia stanowiska, dokumenty papierowe powinny być przechowywane w opisany powyżej sposób, chyba że zapewniono odpowiedni dozór innego pracownika, zamknięto pomieszczenie lub w inny należyty sposób zabezpieczano miejsce ich przechowywania.

IX. Zasady postępowania przeznaczone dla użytkowników systemu informatycznego

§11

Postępowanie – system teleinformatyczny

1. Rozpoczęcie pracy w systemie teleinformatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Użytkownik ma obowiązek każdorazowego blokowania ekranu wygaszaczem chronionym hasłem przed opuszczeniem stanowiska pracy.
3. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć utraty danych.
4. Po zakończeniu pracy, użytkownik ma obowiązek wylogować się z systemu informatycznego przetwarzającego dane osobowe oraz z systemu operacyjnego, zabezpiecza nośniki informacji (zarówno elektronicznej jak i w wersji papierowej), a także wyłącza wyłączyć urządzenie, z którego korzystał.
5. W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor/przymknąć ekran laptopa, w sposób uniemożliwiający wgląd w wyświetlaną treść.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe zobowiązany jest niezwłocznie poinformować administratora danych osobowych w przypadku, gdy:

a. wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy, dla danego systemu informatycznego.
b. niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

7. Pracownicy nie powinni zapisywać plików lub skrótów do plików zawierających dane osobowe (w szczególności dane wrażliwe), w miejscach łatwo dostępnych, zwłaszcza na pulpicie swoich urządzeń.
8. Urządzenia, dyski lub inne nośniki informatyczne zawierając dane osobowe, a przeznaczone do likwidacji, należy uprzednio wyczyścić z tych danych, a w przypadku gdy nie jest to możliwe – należy je uszkodzić w sposób uniemożliwiający ich odczytanie.
9. Urządzenia, dyski lub inne nośniki danych (dysk przenośny, karty pamięci, pamięć wewnętrzna telefonów komórkowych), które zawierają dane osobowe, a są przeznaczone do naprawy, muszą zostać zabezpieczone w taki sposób, że na czas naprawy zostaną pozbawione zapisu tych danych, a gdy jest to niemożliwe – muszą być naprawione pod nadzorem osoby upoważnionej, przy jednoczesnym zastosowaniu innego środka chroniącego przed naruszeniem poufności i integralności danych.
10. Każdy użytkownik zobowiązany jest do bezzwłocznego dokonania aktualizacji systemu operacyjnego użytkowanego komputera, gdy otrzyma informację o możliwości dokonania aktualizacji.

§12
Zasady bezpieczeństwa haseł

1. Każdy użytkownik posiadający dostęp do systemu informatycznego, zobowiązany jest do:
    1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie informatycznym, również po zaprzestaniu ich wykorzystywania z powodu np. utworzenia nowego hasła,
    2) Dokonania niezwłocznej zmiany hasła lub haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia danych osobowych,
    3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez administratora danych osobowych,
    4) poinformowania administratora danych osobowych o podejrzeniu lub rzeczywistym ujawnieniu hasła,
    5) stosowania haseł o minimalnej długości 12 znaków, zawierających kombinację małych i dużych liter oraz cyfr i znaków specjalnych,
    6) stosowania haseł nie posiadających w swojej strukturze części lub całości loginu,
    7) zmiany wykorzystywanych haseł nie rzadziej niż raz na 180 dni.
2. Hasła podlegają zachowania poufności również po ustaniu ich użyteczności.
3. Obowiązuje całkowity zakaz:
    1) zapisywania haseł w sposób jawny i umieszczania ich w miejscu dostępnym dla osób innych niż ich użytkownik,

2) stosowania haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby,
3) używania tych samych haseł w różnych systemach operacyjnych i aplikacjach,
4) udostępniania haseł innym użytkownikom, w tym współpracownikom,
5) przeprowadzania prób łamania haseł,
6) wpisywania haseł „na stałe" oraz wykorzystywania opcji auto zapamiętywania haseł.

X. Zasady korzystania z poczty elektronicznej

§13

Zasady korzystania z poczty elektronicznej

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej funkcjonujący w domenie administratora danych osobowych: bimed.com.pl.
2. Informacja o służbowym adresie skrzynki pocztowej może zostać udostępniona na łamach witryny internetowej administratora danych osobowych w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub innych celów wynikających z treści zawartej umowy.
4. Korespondencja realizowana drogą elektroniczną podlega rejestrowaniu i monitorowaniu przez administratora danych osobowych.
5. Informacje przesyłane za pośrednictwem sieci administratora danych osobowych nie stanowią własności prywatnej korzystającego z niej pracownika.
6. Obowiązuje zakaz korzystania z prywatnej poczty elektronicznej w sprawach służbowych.
7. Zabronione jest:
    1) wysyłanie materiałów służbowych na prywatne konta pracownika,
    2) wykorzystywanie systemu poczty elektronicznej do działań szkodzących administratorowi danych osobowych,
    3) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi z rozszerzeniami typu exe, com, itp.,
    4) Przesyłanie pocztą elektroniczną plików wykonalnych z rozszerzeniami typu: bat, com, exe, plików multimedialnych oraz graficznych,
    5) ukrywanie lub dokonywanie zmian tożsamości nadawcy,
    6) przeglądanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika,
    7) odpowiadanie na niezamówione wiadomości reklamowe oraz inne formy wymiany danych określanych spamem,
    8) Wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów / usług w zakresie działalności innej niż wynikająca z potrzeb administratora danych osobowych.
8. Przesyłając pocztą elektroniczną plik zawierający dane osobowe, plik ten powinien zostać zaszyfrowany np. przy użyciu 7-Zip, a kod powinien zostać przekazany adresatowi widomości w inny sposób niż zaszyfrowany plik np. poprzez tekst w wiadomości SMS lub słownie telefonicznie.

Wyjątkiem jest sytuacja, gdy czynniki takie jak zakres, istotność danych oraz adresat, do którego ma być kierowana wiadomość nie uzasadniają tak daleko idącej ostrożności.

9. Użytkownik wysyłając tego samego maila, jednocześnie do kilku osób, ma obowiązek użyć opcji „ukryte do wiadomości" – czyli „UDW", chyba że wskazanym jest aby pozostałe osoby widziały do kogo jeszcze ten mail był adresowany. Podczas tego typu wysyłki konieczne jest jednak zachowanie szczególnej ostrożności, ponieważ wysłanie maila jednocześnie na kilka adresów, bez użycia opcji UDW, stanowić może naruszenie ochrony danych i niekiedy konieczne może być dokonanie zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych.

XI. Procedura postępowania z nośnikami danych

§14
Ogólne zasady postępowanie z nośnikami danych

1. Każdy nośnik danych jest zabezpieczony hasłem o długości co najmniej 12 znaków. W przypadku gdy użytkownik nośnika odkryje iż nie jest on zabezpieczony odpowiednim hasłem, niezwłocznie informuje o tym fakcie administratora danych osobowych.
2. Zabrania się pozostawiania w miejscach publicznych, bez należytej opieki, nośników elektronicznych wykorzystywanych do przetwarzania danych osobowych.
3. Komputery przenośne należy przewozić jako bagaż podręczny.
4. Użytkownik wykonujący czynności zawodowe / umowne poza organizacją zobowiązany jest do zabezpieczenia powierzonego sprzętu przed nieuprawnionym dostępem do niego osób trzecich.
5. Zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością administratora danych osobowych, z wyjątkiem sytuacji przewidzianych w Regulaminie oraz przepisach powszechnie obowiązującego prawa.
6. W przypadku utraty nośnika elektronicznego, użytkownik zobowiązany jest niezwłocznie zgłosić zaistniały fakt administratorowi danych osobowych.
7. Problemy wynikające z nieprawidłowego funkcjonowania nośników elektronicznych użytkownik przekazuje do administratora danych osobowych.
8. Użytkownik korzystając z nośnika danych zobowiązany jest do monitorowania poziomu jego zapełnienia w celu uniknięcia jego przepełnienia.

§15
Urządzenia typu pendrive

1. W całej organizacji obowiązuje zakaz wykorzystywania urządzeń typu pendrive, z wyjątkiem sytuacji gdy dany pracownik otrzyma urządzenie typu pendrive od Dyrektor Zarządzającej, przekazany protokolarnie.
2. Pracownik, który za potwierdzeniem protokolarnym otrzymał, do realizacji swoich obowiązków, urządzenie typu pendrive, jest odpowiedzialny za jego bezpieczne wykorzystywanie. Każdorazowo po ustaniu użyteczności lub zasadności przechowywania określonych plików na urządzeniu, pracownik który je protokolarnie otrzymał, zobowiązany jest do ich natychmiastowego usunięcia.

XII. Postępowanie ze sprzętem służącym do przetwarzania danych

§16
Warunki postępowania ze sprzętem IT

1. Do sprzętu komputerowego administratora danych osobowych zaliczmy: komputery stacjonarne, komputery przenośne typu laptop.
2. Administrator danych osobowych odpowiada za odpowiednie zabezpieczenie w/w urządzeń w zakresie bezpieczeństwa przetwarzania danych osobowych.
3. W przypadku stosowania urządzeń mobilnych obowiązują wprowadzone środki bezpieczeństwa, do których zaliczmy: blokadę ekranu, program antywirusowy, instalowanie oprogramowania wyłącznie z zaufanego źródła, używanie szyfrowania.
4. Administrator danych osobowych prowadzi spis urządzeń będących w jego posiadaniu wraz z kompletną dokumentacją tych urządzeń.
5. Administrator danych osobowych zapewnia użytkownikowi wyposażenie niezbędne do realizacji jego zadań, przy czym przekazanie urządzeń przenośnych następuje za potwierdzeniem odbioru, co zostaje udokumentowane w rejestrze wyposażenia.
6. Urządzenia przekazywane użytkownikom posiadają oprogramowanie z licencją, której okres użytkowania jest aktualny na dzień przekazania.
7. Użytkownik zobowiązany jest do dbania o stan przekazanych mu urządzeń oraz do zabezpieczenia go przeciwko wykorzystaniu przez osoby nieuprawnione, w szczególności poprzez zabezpieczenie go przed kradzieżą lub zgubieniem.
8. Użytkownik zobowiązany jest do dokonania skanu antywirusowego elektronicznego nośnika danych przed uruchomieniem jego zawartości na urządzeniu.
9. W przypadku stwierdzenia pojawienia się wirusa lub braku możliwości usunięcia go przez program antywirusowy, użytkownik informuje o zaistniałym fakcie administratora danych osobowych i informatyka.
10. Użytkownika obowiązuje zakaz samodzielnej zmiany konfiguracji przekazanych urządzeń, w szczególności poprzez instalowanie bądź usuwanie oprogramowania, w tym także używania prywatnego oprogramowania i prywatnych urządzeń służących do przetwarzania danych.
11. Użytkownik nie może przekazywać powierzonego sprzętu osobom trzecim.
12. Użytkownik ma obowiązek korzystać ze wszelkich urządzeń przetwarzających dane w sposób zgodny z ich przeznaczeniem, nie powodując ich ponadprzeciętnego zużycia. W przypadku dostrzeżenia sygnałów wskazujących na nadchodzące, zużycie sprzętu, użytkownik zobowiązany jest niezwłocznie poinformować o tym administratora.
13. W przypadku wystąpienia awarii użytkownik zobowiązany jest niezwłocznie poinformować o tym administratora.
14. Użytkownik nie ma prawa wykorzystywać sprzętu służbowego do prywatnych celów.
15. Użytkownik może korzystać z przekazanych mu urządzeń i oprogramowania wyłącznie w celu wykonywania powierzonych obowiązków, zgodnie z obowiązującymi przepisami prawa. Powyższy obowiązek należy do podstawowych obowiązków pracowniczych z uwagi na konieczność dbałości o mienie administratora.

16. Użytkownik jest zobowiązany do:
    1) niekorzystania z jakiegokolwiek oprogramowania komputerowego innego niż otrzymanego od administratora, w szczególności niedokonywania samodzielnej instalacji obcego oprogramowania na przekazanych mu przez administratora urządzeniach;
    2) niekorzystania z przekazanych mu urządzeń w celach prywatnych, w szczególności poprzez prowadzenie korespondencji e-mail niezwiązanej ze świadczeniem pracy, poprzez korzystanie z komunikatorów, portali społecznościowych oraz witryn www innych niż konieczne do wykonywania obowiązków pracowniczych;
    3) korzystania z przekazanych mu urządzeń w sposób mogący naruszyć prawa osób trzecich, w tym niekopiowania i nierozpowszechniania oprogramowania oraz plików będących częścią składową przekazanych urządzeń;
    4) niezwłocznego udostępniania administratorowi przekazanych mu urządzeń celem umożliwienia wykonania kontroli administratorowi, na każde żądanie administratora.
17. Zabronione jest wykorzystywanie urządzeń w celach niezgodnych z prawem lub regulaminami obowiązującymi u administratora, w szczególności w celach:
    1) naruszania praw autorskich (nielegalnego pobierania bądź udostępniania plików);
    2) infekowania sieci komputerowej wirusami pobieranymi z plikami z Internetu;
    3) korzystania ze służbowej poczty elektronicznej w sprawach prywatnych.

XIII. Postępowanie w przypadku incydentów i naruszeń ochrony danych osobowych

§17
Zaistnienie incydentu/naruszenia ochrony danych

1. Wynikiem zaistnienia incydentu/naruszenia ochrony danych jest zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych.
2. Każdy pracownik administratora, w przypadku stwierdzenia zagrożenia lub podejrzenia naruszenia ochrony danych osobowych lub wystąpienia incydentu, zobowiązany jest do niezwłocznego poinformowania administratora o wystąpieniu tych okoliczności, a w przypadku gdy naruszenie dotyczy kwestii związanych z IT, poinformować należy również ASI. Bezpośredni przełożony, w przypadku powzięcia powyższej informacji zobowiązany jest do jej niezwłocznego przekazania IOD oraz Administratorowi.

§18
Postępowanie pracowników w przypadku stwierdzenia incydentu/naruszenia ochrony danych

W przypadku stwierdzenia okoliczności wskazujących na wystąpienie incydentu lub naruszenia ochrony danych osobowych lub próbę naruszenia, pracownik:

1) niezwłocznie informuje o tym administratora,

2) do czasu otrzymania dalszych instrukcji z zależności od okoliczności i skali zdarzenia powstrzymuje się od rozpoczęcia lub dalszego wykonywania pracy, także w systemie informatycznym,
3) powstrzymuje się od jakichkolwiek działań, które mogłyby spowodować zatarcie śladów bądź utratę dowodów wskazujących na wystąpienie naruszenia,
4) zabezpiecza dokumenty, urządzenie lub nośnik danych w taki sposób, aby uniemożliwić dostęp do danych osobowych osobom nieupoważnionym,
5) przystępuje do dalszej pracy dopiero po otrzymaniu na to zgody lub na wyraźne polecenie administratora,
6) w celu skutecznego przeciwdziałania naruszeniom ochrony danych osobowych tworzy się i na bieżąco aktualizuje rejestr naruszeń.

§19

Przykłady incydentów

Poniżej przedstawione rodzaje incydentów są jedynie przykładowym wyliczeniem. W przypadku jakichkolwiek wątpliwości, należy niezwłocznie skontaktować się z IOD.

1) utracenie lub ujawnienie nieuprawnionym odbiorcom danych przechowywanych w formie elektronicznej (np. w wyniku awarii serwera lub włamania na serwer);
2) zgubienie lub kradzież nośnika/urządzenia – zawierającego dane osobowe;
3) dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji;
4) korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy;
5) nieuprawnione uzyskanie dostępu do informacji;
6) nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń;
7) złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych;
8) uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing);
9) nieprawidłowa anonimizacja danych osobowych w dokumencie;
10) nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora;
11) niezamierzone opublikowanie danych osobowych;
12) ujawnienie danych osobowych nieupoważnionej osobie;
13) wysłanie niezaszyfrowanego maila, zawierającego dane osobowe, do nieuprawnionej osoby
14) nieprzestrzeganie przyjętych zasad ochrony danych osobowych przez upoważnione osoby.
15) incydenty losowe zewnętrzne np. pożar obiektu lub pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
16) wewnętrzne incydenty losowe np. awarie stacji roboczych, awarie serwera, awarie oprogramowania, utrata lub zgubienie danych zapisanych na nośnikach przenośnych;
17) incydenty umyślne np. ataki hakerskie, włamania do pomieszczeń, celowe i świadome zniszczenie dokumentów, szkodliwe oprogramowanie.

XIV. Polityka Kluczy

§20

Postępowanie z kluczami

1. Obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych za pomocą drzwi wyposażonych w zamki.
2. Klucze do pomieszczeń, w których przetwarzane są dane osobowe, jak również do innych pomieszczeń zamykanych na noc, powinny być pobierane przed rozpoczęciem pracy oraz zdawane po zakończeniu jej wykonywania.
3. Klucze do pomieszczeń przechowywane są w sposób uporządkowany w zamykanej gablocie.
4. Na pracownikach dysponujących pobranymi kluczami spoczywa pełna odpowiedzialność za ich bezpieczeństwo do momentu zdania klucza. Każdy przypadek utraty, uszkodzenia lub zniszczenia klucza wymaga zgłoszenia Administratorowi.

§21

Zabronione zachowania

Obowiązuje bezwzględny zakaz:

1) wytwarzania kopii kluczy do pomieszczeń bez uprzedniego uzyskania zgody Administratora,
2) udostępniania kluczy oraz kodów dostępów do pomieszczeń osobom nieupoważnionym,
3) pozostawiania kluczy w drzwiach,
4) pozostawiania kluczy bez nadzoru

XV. Dokumenty powiązane

§22

Główne dokumenty powiązane

Do głównych dokumentów powiązanych należą:

1) Polityka Ochrony Danych Osobowych
2) Instrukcja Zarządzania Systemem Teleinformatycznym
3) Polityka Prywatności

XVI. Postanowienia końcowe

Niniejszy **Regulamin Ochrony Danych** wchodzi w życie z dniem określonym w uchwale zarządu Spółki i zastępuje dotychczasową dokumentację.

XVII. Wykaz załączników

- Polityka realizacji praw osób, których dane dotyczą
- Polityka Retencji (usuwania) danych

Złącznik do Regulaminu Ochrony Danych

Polityka realizacji praw osób, których dane dotyczą

§1

Forma udzielenia informacji

1. Komunikacja z osobami, których dane dotyczą należy prowadzić z zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka – w szczególności, gdy osobą tą jest dziecko. Jeżeli informacji udziela się w formie elektronicznej należy zapewnić, ze nadaje się ona do odczytu maszynowego.
2. Wszelkich informacji na temat przetwarzania danych udziela się na piśmie, w tym w formie elektronicznej. Możliwe jest również udzielenie informacji ustnie, o ile osoba, której dane dotyczą tego zażąda, a osoba rozpatrująca żądanie potwierdzi tożsamość osoby, z którą ma do czynienia, aby uniknąć ujawnienia danych osobowych osobom postronnym.
3. Administrator zapewnia możliwość składania wniosków drogą elektroniczną, jak również tradycyjną.

§2

Procedura

1. Wniosek osoby, której dane dotyczą należy rozpatrzeć niezwłocznie – nie dłużej jednak niż w ciągu miesiąca od jego otrzymania, przy czym przez rozpatrzenie należy rozumieć udzielenie żądanej informacji osobie, której dane dotyczą lub poinformowanie o dokonaniu lub odmowie dokonania czynności.
2. Jeżeli jest to konieczne ze względu na skomplikowany charakter wniosku lub ich liczbę, termin może zostać wydłużony do dwóch miesięcy, czyli o kolejny miesiąc. O wydłużeniu terminu należy poinformować osobę, której dane dotyczą, wraz ze wskazaniem przyczyn opóźnienia. Powinno to nastąpić przed upływem podstawowego terminu na rozpatrzenie wniosku.
3. W przypadku odmowy podjęcia działań w związku z wnioskiem, należy poinformować osobę, której dane dotyczą o powodach niepodjęcia działań, jak również o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz prawie do skorzystania ze środków ochrony prawnej przed sądem w oparciu o wzory określone odrębnie dla poszczególnych rodzajów pism.
4. Komunikacja, z osobą której dane dotyczą prowadzona na jej wniosek jest bezpłatna. Jeżeli jednak zostanie wykazane, że nie ma wątpliwości co do nadmiernego lub niezasadnego charakteru wniosku, to można pobrać rozsądną opłatę. Wysokość opłaty powinna być ustalona z uwzględnieniem kosztów udzielenia informacji, powadzenia komunikacji i podjęcia działań związanych z wnioskiem.
5. Jeżeli osoba rozpatrująca wniosek powzięła uzasadnione wątpliwości co do tożsamości osoby fizycznej kierującej wniosek, może zażądać dodatkowych informacje, które są niezbędne do potwierdzenia jej tożsamości.

6. Ciężar udowodnienia okoliczności uzasadniających odmowę podjęcia działań, nieuwzględnienie wniosku lub pobranie opłaty za jego rozpatrzenie spoczywa na administratorze, a dokonana ocena podlega kontroli ze strony Prezesa Urzędu Ochrony Danych Osobowych. W związku z tym powyższe decyzje należy podejmować jedynie wówczas, gdy nie ma żadnych wątpliwości co do ich zasadności.

§3

Prawo dostępu i informacji o przetwarzaniu danych przysługujące osobie, której dane dotyczą

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy Administrator przetwarza jej dane osobowe. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz pozyskania następujących informacji:
    1) w jakim celu są przetwarzane jej dane osobowe;
    2) jakich kategorii danych osobowych dotyczy przetwarzanie;
    3) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
    4) o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
    5) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
    6) o prawie wniesienia skargi do organu nadzorczego;
    7) o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.
3. Jeżeli osoba, której dane dotyczą zwróci się z wnioskiem o dostarczenie kopii jej danych osobowych podlegających przetwarzaniu żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, o które zwróci się ta osoba, można pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną.
4. Kopię danych, o której mowa w ust. 3 wydaje się w postaci wydruku po ich przepisaniu lub skopiowaniu do tabeli Excel/ Word. Co do zasady nie wydaje się skanów dokumentów ani ich kserokopii, gdyż mogą zawierać dodatkowe dane nie dotyczące osoby występującej z wnioskiem.
5. Prawo do uzyskania kopii, o której mowa w ust. 3 nie może niekorzystnie wpływać na prawa i wolności innych osób.

§4

Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
2. Ponadto osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

3. Wniosek o sprostowanie lub uzupełnienie danych przekazywany jest w formie pisemnej lub drogą elektroniczną na adres Administratora. Pracownik, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej zobowiązany jest dokonać weryfikacji przetwarzanych danych. W przypadku stwierdzenia konieczności wprowadzenia zmian informuje o tym bezpośredniego przełożonego. Następnie niezwłocznie dokonuje zmian, rejestrując ten fakt w aktach sprawy. Uzupełnienie danych następuje zawsze z uwzględnieniem celów przetwarzania.

§5
Prawo do usunięcia danych (prawo do bycia zapomnianym)

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
    1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zarówno danych zwykłych jak i szczególnych kategorii danych, a jednocześnie nie ma innej podstawy prawnej ich przetwarzania;
    3) osoba, której dane dotyczą, wnosi sprzeciw, o którym mowa w pkt. 9 niniejszego dokumentu, wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
    4) dane osobowe były przetwarzane niezgodnie z prawem;
    5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.
2. Jeżeli dane osobowe zostały upublicznione, a w związku z realizacją przez podmiot danych uprawnienia, o którym mowa w ust. 1, istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje się niezbędne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
3. Ustępy 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
    1) do korzystania z prawa do wolności wypowiedzi i informacji;
    2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
    3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych o ile prawdopodobne jest, że prawo, o którym mowa w ust.1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania lub
    4) do ustalenia, dochodzenia lub obrony roszczeń.

4. W sytuacji, gdy żądanie osoby, której dane dotyczą jest uzasadnione, a po stronie Administratora nie ma podstaw prawnych odmowy realizacji żądania zgłasza się sprawę pracownikowi odpowiedzialnemu za prowadzenie archiwum lub systemu, w którym przetwarzane są rzeczone dane, w celu dokonania ich usunięcia. Postępowanie dotyczy zarówno danych przetwarzanych w formie tradycyjnej jak i elektronicznej.

§6

Prawo do ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania jej danych osobowych.
2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
3. Do ograniczenia może dojść w następujących przypadkach:
    1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych. W tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość danych;
    2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
    3) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
    4) jeżeli osoba, której dane dotyczą, wobec przetwarzania wniosła sprzeciw, dotyczący przetwarzania jej danych, to w tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.
4. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każda osoba, która jest upoważniona do przetwarzania tych danych była świadoma, iż dane te można jedynie przechowywać.
5. Przed uchyleniem ograniczenia przetwarzania informuje się o tym osobę, która żądała ograniczenia.

§7

Prawo do powiadomienia o sprostowaniu, usunięciu danych lub o ograniczeniu przetwarzania

1. Po dokonaniu sprostowania, usunięcia danych osobowych lub ograniczenia przetwarzania informuje się o tym każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
2. Jeżeli osoba, której dane dotyczą, tego zażąda informuje się ją o odbiorcach jej danych osobowych.

§8

Prawo do przenoszenia danych

1. Jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy, której stroną jest osoba, której dane dotyczą oraz przetwarzanie odbywa się w sposób zautomatyzowany, osoba ta ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące. Dotyczy to danych, które osoba składająca żądanie wcześniej dostarczyła. Osoba ta ma prawo przesłać te dane osobowe innemu administratorowi.
2. Wykonując prawo do przenoszenia danych na mocy ust. 1 osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe i osoba wykaże, iż administrator, któremu mają zostać dane przekazane akceptuje taki sposób pozyskania danych.
3. Prawo, o którym mowa w ust. 1 nie może niekorzystnie wpływać na prawa i wolności innych.
4. Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku dla prawa do usunięcia danych.
5. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

§9

Prawo do sprzeciwu

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e lub f RODO, w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
2. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
3. Administratorowi nie wolno przetwarzać danych osobowych względem, których wniesiono sprzeciw, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
4. Najpóźniej przy okazji pierwszego kontaktu z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa powyżej, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
5. W momencie złożenia sprzeciwu wobec przetwarzania administrator niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej. Jeżeli Administrator posiada podstawę prawną, o której mowa powyżej informuję osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji.

6. Jeżeli dane osobowe są przetwarzane do celów badań naukowych, celów historycznych lub do celów statystycznych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

§10

Informowanie o naruszeniach ochrony danych

1. Osoby, których dane dotyczą informuje się bez zbędnej zwłoki o naruszeniach ochrony danych osobowych, chyba że naruszenie nie powoduje wysokiego ryzyka naruszenia praw i wolności tych osób. Treść zawiadomienia obejmuje co najmniej: imię i nazwisko oraz dane kontaktowe punktu kontaktowego, który mógłby udzielić informacji – co do zasady IOD, jeżeli jest wyznaczony; opis możliwych konsekwencji naruszenia ochrony danych; opis środków podjętych w celu zaradzenia naruszeniu ochrony danych
2. Dokonanie zawiadomienia, o którym mowa powyżej nie jest konieczne, jeżeli nastąpi co najmniej jedna z poniższych sytuacji: wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie; zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; wymagałoby ono niewspółmiernie dużego wysiłku – w takim wypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. Ciężar udowodnienia zaistnienia wspomnianych w poprzednim zdaniu przesłanek spoczywa na administratorze.

§11

Dokumentowanie komunikacji z podmiotami danych

1. Wszelka korespondencja dotycząca ochrony danych osobowych powinna być prowadzona za pomocą środków, które pozwalają na jej utrwalenie i wykorzystanie na wypadek kontroli, skarg lub innych zdarzeń.
2. Wysłane wiadomości email powinny być przechowywane na dysku twardym lub innym nośniku albo usłudze należącej do administratora lub będącej w jego dyspozycji.
3. Informacje przesyłane pocztą tradycyjną powinny trafiać do adresatów za pośrednictwem przesyłek rejestrowanych.

Złącznik do Regulaminu Ochrony Danych

Polityka Retencji (usuwania danych)

§1
Podstawy prawne

1. Zgodnie z przepisami RODO dane osobowe powinny być przechowane przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane.
2. Ustalenie właściwego okresu przechowywania danych jest obowiązkiem administratora danych osobowych, będzie on zależny od celu, dla którego przetwarzane są dane osobowe.
3. W zależności od celu przepisy powszechnie obowiązującego prawa przewidują różne okresy retencji, np.:
    1) Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa art. 70 § 1 - zobowiązania podatkowe przedawniają się z upływem 5 lat, licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku.
    2) Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy art. 94b pkt. 9b – Pracodawca zobowiązany jest przechowywać dokumentację pracowniczą przez okres 10 lat od licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł.
    3) Ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych art. 125a – Płatnik składek jest zobowiązany przechowywać listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty10 lat od końca roku kalendarzowego, w którym ubezpieczony zakończył pracę u danego płatnika składek lub w określonych sytuacjach 50 lat art. 125a ust. 4 i 4a ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych). Okres 10 lat dotyczy dokumentacji pracowniczej osób zatrudnionych od 1 stycznia 2019 roku. W przypadku, jeżeli stosunek pracy został nawiązany po 31 grudnia 1998 a przed 1 stycznia 2019, pracodawca ma możliwość złożenia raportu informacyjnego (ZUS OSW), który umożliwi mu skrócenie przechowania dokumentacji pracowniczej z 50 lat do 10. Dokumentacja osób zatrudnionych przed 31 grudnia 1998 r. powinna być przechowywana 50 lat.
    4) przepisy prawa zawarte w wielu różnych ustawach mogą przewidywać dłuższy okres przechowywania danych, w szczególności w zakresie dochodzenia lub obrony roszczeń
4. Szczególną uwagę administrator poświęca danym osobowym zawierającym informacje o stanie zdrowia, przez wzgląd na to, że są to dane wrażliwe i przepisy ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta w art. 29 przewidują precyzyjne okresy przez jaki te dane powinny być przechowywane:
    1) Podmiot udzielający świadczeń zdrowotnych, co do zasady, przechowuje dokumentację medyczną przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, ale od owej reguły przewidziane są wyjątki, o których mowa poniżej.

2) Dokumentację medyczną w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia powinno przechowywać się przez okres 30 lat, licząc od końca roku kalendarzowego, w którym nastąpił zgon;
3) Dokumentację medyczną zawierającą dane niezbędne do monitorowania losów krwi i jej składników, należy przechowywać przez okres 30 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu;
4) Zdjęcia rentgenowskie przechowywane poza dokumentacją medyczną pacjenta, powinny być przechowywane przez okres 10 lat, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie;
5) Dokumentacja medyczna dotycząca dzieci do ukończenia 2. roku życia, powinna być przechowywana przez okres 22 lat.
6) W przypadku skierowań na badania lub zleceń lekarza, dokumenty muszą być przechowywane przez okres: 5 lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza oraz 2 lat, licząc od końca roku kalendarzowego, w którym wystawiono skierowanie – w przypadku gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie.
7) Po upływie okresów wymienionych w art. 29 wspomnianej powyżej ustawy podmiot udzielający świadczeń zdrowotnych niszczy dokumentację medyczną w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła. Dokumentacja medyczna przeznaczona do zniszczenia może być wydana pacjentowi, jego przedstawicielowi ustawowemu lub osobie upoważnionej przez pacjenta.

§2

Procedura w przypadku realizowania prawa do usunięcia danych przez osobę, której dane dotyczą

1. W sytuacji żądania usunięcia danych przez osobę, której dane dotyczą, pracownik lub pracownicy zajmujący się danym przypadkiem ma obowiązek, kierując się wskazówkami z Polityki realizowania praw osób, których dane dotyczą, ma ustalić, czy żądanie jest uzasadnione.
2. W razie wątpliwości pracownik zasięga opinii IOD lub osoby wyznaczonej przez administratora do pełnienia obsługi punktu kontaktowego w sprawach związanych z ochroną danych osobowych.
3. Z usunięcia danych osoby, której dane dotyczą sporządza się notatkę, pod którą oprócz pracownika dokonującego zniszczenia podpisuje się również osoba reprezentująca administratora danych osobowych.

§3

Ogólne zasady niszczenia papierowej dokumentacji i innych nośników danych

1. Niszczenie dokumentów papierowych odbywa się za pomocą niszczarki, po wcześniejszym upewnieniu się przez pracownika, że zawarte w treści dokumentu dane powinny zostać usunięte.

2. Zakazane jest wyrzucanie dokumentów zawierających dane osobowe np. do kosza, bez wcześniejszego przepuszczenia ich przez niszczarkę.
3. Dane zawarte na nośnikach elektronicznych typu pendrive, płyty CD itp. usuwane są z wykorzystaniem sprzętu informatycznego, po wybraniu właściwej opcji, po wcześniejszym upewnieniu się przez pracownika, że zawarte na nośniku dane powinny zostać usunięte.

§4

Procedura dokonywania okresowego zbiorczego niszczenia dokumentacji, co do której istnieją przepisy powszechnie obowiązującego prawa, które wymagają przetwarzania danych przez określony czas.

1. Raz w roku, w styczniu, Administrator powołuje komisję złożoną, w miarę możliwości, z co najmniej 3 osób.
2. W miarę możliwości w składzie komisji powinna znajdować się co najmniej jedna osoba mająca przynajmniej podstawową wiedzę na temat przepisów prawnych bądź posiadająca długi staż pracy w administracji.
3. Zadaniem wyżej wspomnianej komisji jest przegląd wszystkich dokumentów i nośników informacji zawierających dane osobowe, w celu wskazania, które z nich należy usunąć.
4. Dokonując analizy komisja bada przede wszystkim czy przesłanka przetwarzania tych danych wygasła, a jeżeli tak, to czy zachodzi inna przesłanka przetwarzania danych.
5. Wykonując swoje zadania członkowie komisji powinni zachować szczególną ostrożności i staranność z uwagi na wagę odpowiedzialności dokonywanych przez nich czynności.
6. Ze zniszczenia danych sporządza się protokół. Wzór protokołu stanowi załącznik do niniejszej **Polityki Retencji**.
7. Protokół z dokonanego zniszczenia danych Administrator zobowiązany jest przechowywać w bezpiecznym miejscu.