POLITYKA OCHRONY DANYCH OSOBOWYCH

AS STOMATOLOGIA SP. Z O.O.

Niniejsza Polityka ochrony danych, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w kancelarii, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

Definicje:

1. **Administrator Danych** – AS STOMATOLOGIA Sp. z o.o. – ul. Pałuków 2, lok. U10, 03-188 Warszawa, wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIV Wydział Gospodarczy pod numerem KRS: 0001201244, NIP: 5681466623, REGON: 387994845, kapitał zakładowy 100.000 zł (dalej również: „**Administrator**");
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, w tym również dane dotyczące zdrowia;
3. **Dane dotyczące zdrowia** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
4. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych;
5. **Użytkownik** – osoba upoważniona przez Administratora do Przetwarzania danych osobowych, w tym w szczególności pracownik, współpracownik, wykonawca, podwykonawca Administratora;
6. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów;
7. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych;
8. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie;
9. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie;
10. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika);
11. **Polityka Ochrony Danych Osobowych** została opracowana na podstawie:
    a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – RODO),
    b) Normy PN-EN ISO/IEC 27001 dotyczącej zarządzania bezpieczeństwem informacji,
    c) Normy PN-ISO/IEC 17799 dotyczącej praktycznych zasad zarządzania bezpieczeństwem informacji,
    d) Normy PN-EN ISO/IEC 27002 dotyczącej praktycznych zasad zabezpieczania informacji,
    e) Normy PN-EN ISO/IEC 27005 dotyczącej zarządzania ryzykiem w bezpieczeństwie informacji,

f) Normy PN-ISO 31000 dotyczącej zarządzania ryzykiem,
g) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

I. Postanowienia ogólne

1. Realizując obowiązki wynikające z przepisów dotyczących ochrony danych osobowych, **Administrator** spełnia wymagania chroniące prywatność i godność każdego pracownika firmy oraz jej kontrahentów, dostawców i pa.
2. Sposób przetwarzania danych osobowych u **Administratora** oraz środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych, ujęte zostały zbiorczo w niniejszym dokumencie określającym **Politykę Ochrony Danych Osobowych (**dalej: **PODO).** PODO wraz z jej wszystkimi załącznikami należy rozumieć jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji, zarówno wewnątrz jak i na zewnątrz organizacji. Zwraca ona uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.
3. Celem opracowania niniejszej Polityki jest określenie zasad ochrony danych osobowych przetwarzanych u **Administratora,** a co za tym idzie organizacyjne, fizyczne i logiczne, zabezpieczenie posiadanych danych osobowych. Zasady określone w Polityce mają zastosowanie do wszystkich osób, które zostały upoważnione do przetwarzania danych osobowych, niezależnie od formy ich zatrudnienia. Utrzymanie bezpieczeństwa przetwarzanych przez **Administratora** danych osobowych oraz informacji, rozumiane jest jako zapewnienie ich poufności, integralności i dostępności oraz rozliczalności, na jak najwyższym, możliwym do uzyskania w danym czasie, poziomie. Pośrednim celem PODO jest systematyczne edukowanie użytkowników systemu ochrony danych osobowych. Jednocześnie, polityka ta zawiera jasną deklarację zaangażowania kierownictwa firmy i wyznacza jej procesowe podejście do zarządzania ochroną danych.
4. Polityka Ochrony Danych Osobowych zapewnia:
    - **poufność –** dane nie są udostępniane lub ujawniane nieupoważnionym osobom, podmiotom i procesom;
    - **integralność –** dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
    - **dostępność –** istnieje możliwość wykorzystania danych na żądanie, w założonym czasie, przez autoryzowany podmiot;
    - **rozliczalność –** możliwość jednoznacznego przypisania działań poszczególnym osobom;
    - **autentyczność –** zapewnienie, że tożsamość podmiotu lub zasobu jest zgodna z zadeklarowaną;
    - **niezaprzeczalność –** uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
    - **niezawodność –** zamierzone zachowania i skutki są spójne.

5. Polityka dotyczy wszystkich Danych osobowych, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
6. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
7. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
8. Dla skutecznej realizacji Polityki Administrator zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
   c) monitorowanie zastosowanych środków ochrony.
9. Monitorowanie przez Administratora zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
10. Administrator zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką oraz odpowiednimi przepisami prawa.
11. Polityka Ochrony Danych Osobowych została przygotowana w celu:
    a) ograniczenia możliwości nieautoryzowanego udostępnienia informacji oraz danych osobowych przetwarzanych przez pracowników lub kontrahentów;
    b) ograniczenia naruszeń przepisów prawa oraz innych regulacji;
    c) ograniczenia strat finansowych;
    d) ograniczenia zakłóceń występujących w przedsiębiorstwie Administratora.
12. Polityka Ochrony Danych Osobowych, w odniesieniu do ochrony danych osobowych zakłada:
    a) zbieranie danych osobowych w jasno określonych celach;
    b) przetwarzanie danych osobowych, które jest zgodne wyłącznie z ustalonymi wcześniej celami;
    c) przechowywanie danych osobowych przez określony czas, przeznaczony na realizację poszczególnych zadań;
    d) przedstawianie danych osobowych w sposób ustrukturyzowany, umożliwiający łatwą identyfikację;
    e) przetwarzanie danych osobowych w sposób zgodny z obowiązującymi przepisami prawa.

II. Dane osobowe przetwarzane u administratora danych

1. Dane osobowe przetwarzane przez Administratora gromadzone są w zbiorach danych.
2. Administrator nie podejmuje żadnych czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw

i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.

3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi rejestr czynności przetwarzania.
5. W związku z udzielaniem przez Administratora świadczeń medycznych (dentystycznych) przetwarza on również dane dotyczące zdrowia pacjentów.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Polityką Ochrony Danych Osobowych, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych u **Administratora**.
2. Każdy z pracowników, wykonawców oraz podwykonawców **Administratora** posiada dostęp tylko do takich informacji, danych osobowych oraz zasobów, które są niezbędne z punktu widzenia wykonywanych przez każdego z nich zadań, pełnionych ról, czy posiadanej wiedzy.
3. Polityka ochrony danych jest dokumentem wewnętrznym, poufnym i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody Administratora. Dla codziennych potrzeb pracowników i współpracowników stworzony został Regulamin Ochrony Danych Osobowych (**załącznik do Polityki Ochrony Danych Osobowych**) zawierający zasady przetwarzania danych osobowych obowiązujące u Administratora.
4. Wszystkie dane osobowe u **Administratora** są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
    a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych;
    b) Dane są przetwarzane są rzetelnie i w sposób przejrzysty;
    c) Dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
    d) Dane są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;
    e) Dane są prawidłowe i w razie potrzeby aktualizowane;
    f) czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one animizowane bądź usuwane;
    g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.
    h) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.
5. Administrator nie przekazuje danych osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust 5 pkt d RODO).

6. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:
    a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
    b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
    c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
    d) niedopełnienie obowiązku zachowania w tajemnicy danych oraz sposobów ich zabezpieczenia;
    e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
    f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
    g) naruszenie praw osób, których dane są przetwarzane.
7. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora o naruszeniu.
8. Do obowiązków Administratora w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:
    a) pracownicy i współpracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków;
    b) każdy z pracowników lub współpracowników przetwarzających dane osobowe był pisemnie upoważniony do przetwarzania danych osobowych;
    c) każdy pracownik lub współpracownik zobowiązał się do zachowania przetwarzanych danych osobowych w tajemnicy.
9. Pracownicy i współpracownicy zobowiązani są do:
    a) ścisłego przestrzegania zakresu nadanego upoważnienia;
    b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
    c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.
10. Każdy z pracowników, współpracowników, wykonawców oraz podwykonawców **Administratora** posiada dostęp tylko do takich informacji, danych osobowych oraz zasobów, które są niezbędne z punktu widzenia wykonywanych przez każdego z nich zadań, pełnionych ról, czy posiadanej wiedzy.
11. Administrator zobligowany jest do prowadzenia rejestru wyżej wymienionych upoważnień wydanych dla pracowników, wykonawców lub podwykonawców.
12. Każdy z pracowników, współpracowników, wykonawców lub podwykonawców **Administratora** informowany jest również, podczas udzielania mu dostępu do informacji, o sankcjach, które będą egzekwowane w przypadku nieautoryzowanego

ich udostępnienia.

13. Osoba odpowiedzialna za środowisko sieciowe w firmie zobligowana jest do wykonywania systematycznego, nie rzadziej niż raz na trzy miesiące, przeglądu praw dostępu Użytkowników do danych osobowych, informacji i zasobów, a co za tym idzie, do systematycznego ich aktualizowania (dodawania lub usuwania).
14. Każdy z Użytkowników może wystąpić z wnioskiem o poszerzenie dostępu do większej ilości informacji i danych osobowych. Wniosek ten powinien zostać skierowany do Administratora, który dokonuje analizy konieczności poszerzenia dostępu dla danego Użytkownika i wydaje odpowiednią decyzję, w postaci upoważnienia.
15. Każdy z Użytkowników zobowiązany jest do nieudostępniania swojego loginu i hasła do konta osobom postronnym (innym użytkownikom, osobom trzecim). Każdorazowe zalogowanie się do systemu powinno nastąpić, tylko i wyłącznie, na urządzeniach, które należą do **Administratora**, chyba że Administrator udzieli stosownego upoważnienia w tej sprawie.
16. W przypadku zmiany stanowiska pracy przez Użytkownika, Administrator może zmienić jego zakres dostępu. Zmiana ta musi być zgodna z zakresem pełnionych przez tego Użytkownika obowiązków, ról i odpowiedzialności.
17. W przypadku rozwiązania umowy z łączącej Użytkownika z Administratorem osoba odpowiedzialna za środowisko sieciowe zobowiązana jest do niezwłocznego usunięcia konta Użytkownika, wraz z udzielonym mu dostępem do informacji.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe na terenie siedziby, obejmuje pomieszczenia biurowe, gabinety oraz recepcję znajdujące się w siedzibie, a także w każdym innym miejscu wyznaczonym przez Administratora.
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.
3. Przy wyznaczaniu pomieszczeń przeznaczonych do przechowywania danych osobowych należy brać pod uwagę miejsca przetwarzania:
   a) dokumentacji papierowej,
   b) stacji komputerowych,
   c) serwerów,
   d) przenośnych nośników danych,
   e) macierzy dyskowych,
   f) sejfów,
   g) innych urządzeń przetwarzających dane osobowe.
4. Powyższe warunki spełniają również miejsca składowania wszelkiego rodzaju uszkodzonych nośników danych (komputerów, dysków, taśm itp.).
5. Miejsce przetwarzania danych osobowych należy określić poprzez wskazanie budynków, pomieszczeń bądź ich części, w których dokonuje się wyżej wymienionej operacji.
6. Dane osobowe są przetwarzane przez Administratora jedynie w pomieszczeniach do

tego przeznaczonych, w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.

V. Monitoring wizyjny

1. Administrator może stosować monitoring w celu zapewnienia bezpieczeństwa pacjentów i personelu w miejscach ogólnodostępnych.
2. Nagrania z monitoringu przechowuje się przez okres nie dłuższy niż 3 miesiące, po czym podlegają one zniszczeniu.
3. Monitoring nie może naruszać intymności pacjenta ani obejmować pomieszczeń innych, niż pomieszczenia wspólne, tj. recepcję oraz korytarze (chyba że przepisy szczególne stanowią inaczej).

VI. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. Każdy kto przetwarza dane osobowe zobowiązany jest zachować w tajemnicy dane osobowe, do których posiada dostęp, sposoby zabezpieczania danych, jak również wszelkie informacje, które powziął w czasie przetwarzania danych, zarówno w sposób zamierzony jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
3. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych. Środki te obejmują, m.in.:
    a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej,
    b) zamykanie pomieszczeń tworzących obszar przetwarzania danych osobowych określony w pkt IV powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich,
    c) wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów,
    d) wykorzystanie niszczarki do skutecznego usuwania dokumentów papierowych zawierających dane osobowe,
    e) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall,
    f) wykonywanie awaryjnych kopii danych na dyskach przenośnych,
    g) ochronę sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem,
    h) zabezpieczenie dostępu do urządzeń Administratora przy pomocy haseł dostępu,

i) wykorzystanie szyfrowania danych przy ich przesyłaniu.

4. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
5. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po ich utracie.
6. Należy dotrzymać należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
7. W przypadku przesyłania, za pomocą środków komunikacji elektronicznej, zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji elektronicznej.
8. Wszelkie dokumenty zawierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz. Osoba będąca dysponentem tych danych osobowych zobowiązana jest nie przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane, osobom nieuprawnionym, a ponadto zobowiązana jest przedsięwziąć działania celem zminimalizowania ryzyka utraty danych. Osoba, która utraciła posiadane klucze do pomieszczeń, w których przetwarzane są dane, niezwłocznie zgłasza Administratorowi tę okoliczność.
9. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia. Zaleca się, aby niszczarka spełniała klasę bezpieczeństwa nie niższą niż 3. Alternatywnym rozwiązaniem do celów niszczenia dokumentacji jest zatrudnienie wykwalifikowanej firmy zewnętrznej, zajmującej się profesjonalną utylizacją dokumentów. Wymogiem jest zawarcie z nią umowy o powierzeniu przetwarzania danych osobowych. Każdy dokument zawierający dane, a nieużyteczny, niszczy się niezwłocznie. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
10. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane, jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

VII. Archiwizacja i niszczenie danych

1. Dokumentacja medyczna jest przechowywana przez okres 20 lat, licząc od końca roku kalendarzowego, w którym została utworzona z następującymi wyjątkami:
   a) dokumentacja medyczna w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym nastąpił zgon;

b) zdjęcia rentgenowskie przechowywane poza dokumentacją medyczną są przechowywane przez okres 10 lat, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie;
c) skierowania na badania lub zlecenia lekarza są przechowywane przez okres:
   - 5 lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza;
   - 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;
d) dokumentacja medyczna dotycząca pacjenta do ukończenia przez niego 2. roku życia jest przechowywana przez okres 22 lat.

2. Po upływie okresu przechowywania dokumentacja jest niszczona w sposób uniemożliwiający identyfikację pacjenta lub wydawana pacjentowi na jego wniosek

VIII. Praca zdalna

1. Praca zdalna to aktualnie powszechny element stosowany w trakcie zatrudnienia. Pracownik zdalny to jednak, poza wygodą, także szereg zagrożeń związanych z faktem, że dane z założenia są przetwarzane poza firmą w środowisku, któremu często daleko do bezpiecznego. Praca zdalna to często pracownicy rozliczani w systemie zadaniowym jak i na co dzień pracujący w terenie. Pracownik dysponuje zwykle telefonem komórkowym, laptopem lub tabletem zawierającym dane firmowe, z dostępem do sieci firmowej.
2. Dla organizacji głównym problemem w takim przypadku będzie nie tyle utrata laptopa czy tabletu, co utrata zawartych w tych urządzeniach danych - w przypadku danych wrażliwych może się to wiązać z poważnymi konsekwencjami finansowymi.
3. Na bezpieczeństwo podczas pracy w biurze składają się elementy takie jak kontrola dostępu do pomieszczeń, systemy alarmowe, gaśnicze, niszczarki dokumentów, sejfy czy chociażby firmowa zapora sieciowa, system wykrywania włamań i antywirusowy.
4. Na bezpieczeństwo podczas pracy zdalnej składają się takie elementy jak wyposażenie sprzętu Użytkownika w zaporę sieciową, szyfrowanie dysków pamięci, system antywirusowy, blokady dostępu do sprzętu w postaci haseł lub kodów PIN.
5. W przypadku pracy zdalnej istotny jest fakt, że pracownik, który przebywa poza biurem to także element poprawiający ciągłość działania firmy w razie braku dostępu do głównej siedziby przedsiębiorstwa (pożar, zalanie, awaria zasilania).

IX. Bezpieczeństwo zasobów danych

1) Etap wyboru pracownika

1. Wszyscy kandydaci do pracy, wykonawcy oraz podwykonawcy **Administratora** podlegają szczegółowej weryfikacji, zgodnie z przepisami prawnymi i regulacjami wewnętrznymi, adekwatnie do wymagań biznesowych, klasyfikacji udostępnionych informacji oraz zidentyfikowanego ryzyka. Weryfikacja ta nie narusza prywatności,

ochrony danych osobowych ani regulacji prawnych dotyczących zatrudnienia i obejmuje m.in.:

a) sprawdzenie autentyczności referencji osobistych i świadectw pracy;
b) sprawdzenie autentyczności przedstawionego życiorysu;
c) potwierdzenie deklarowanego wykształcenia i kwalifikacji zawodowych;
d) niezależne potwierdzenie tożsamości, np. dowód osobisty, paszport.

2. Każdy z nowo zatrudnionych pracowników podpisuje umowę oraz zaznajamia się z regulaminem pracy, które dokładnie określają odpowiedzialność w zakresie ochrony danych. Role i zakresy odpowiedzialności uwzględniają m.in.:
   a) działania zgodne z Polityką Ochrony Danych Osobowych;
   b) ochronę danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem;
   c) wykonywanie działań związanych z ochroną danych;
   d) odpowiedzialność pracownika za jego działania lub niepodejmowanie działań;
   e) raportowanie zdarzeń związanych z ochroną danych.
3. Dodatkowo, w treści każdej z umów znajdują się następujące informacje:
   a) postanowienia o zachowaniu poufności i nieujawnianiu informacji, w przypadku dostępu do informacji wrażliwych;
   b) prawa i obowiązki w odniesieniu do praw autorskich i ochrony danych osobowych;
   c) odpowiedzialność w zakresie przetwarzania informacji otrzymywanej z zewnątrz;
   d) odpowiedzialność w zakresie przetwarzania danych osobowych;
   e) odpowiedzialność rozszerzona, np. w przypadku pracy zdalnej;
   f) konsekwencje nieprzestrzegania procedur bezpieczeństwa.
4. Rekrutacja i zatrudnianie nowych pracowników prowadzona jest na dwa sposoby:
   a) bezpośrednio poprzez Administratora,
   b) poprzez zewnętrzną firmę – korzystanie z portali internetowych.
5. Wewnętrzna rekrutacja odbywa się na poziomie kierownictwa. Kierownicy poszczególnych działów zgłaszają zapotrzebowanie zatrudnienia nowego pracownika do działu kadr. Dział kadr przygotowuje ogłoszenie rekrutacyjne i umieszcza je na stronie internetowej Administratora. Kandydaci mogą przekazać dokument CV osobiście w siedzibie Administratora, wysłać je drogą pocztową na adres siedziby Administratora, lub drogą elektroniczną na specjalnie do tego celu utworzoną skrzynkę. do której dostęp mają jedynie kierownicy. Rozmowy kwalifikacyjne wykonywane są bezpośrednio przez odpowiedniego kierownika działu lub osoby o kompetencjach pozwalających na weryfikację umiejętności przyszłego pracownika w kontekście dostępnego stanowiska pracy. CV lub formularze odrzucone przez osobę przeprowadzającą rekrutację, są przez nich niszczone bezpośrednio w niszczarce, a w przypadku dokumentów elektronicznych usuwane w sposób uniemożliwiający ich przywrócenie. CV papierowe lub formularze w postaci elektronicznej, przechowywane są do celów przyszłych rekrutacji, tylko i wyłącznie w sytuacji, gdy kandydat wyraził stosowną zgodę, jednak przez okres nie dłuższy niż rok. CV lub formularz nowozatrudnionego pracownika jest drukowany w jednym egzemplarzu i umieszczany w teczce pracowniczej.

6. Jeżeli rekrutację na dane stanowisko przeprowadza podmiot zewnętrzny na wszystkich podpisywanych umowach zostaje zamieszczona odpowiednia informacja o odpowiedzialności konkretnej agencji za ten proces. Przy wyborze firmy zewnętrznej dostarczającej pracowników do **Administratora** decydującym czynnikiem powinno być spełnianie przez nią wymagań prawnych dotyczących ochrony danych osobowych (weryfikacja pod kątem wdrożenia przez nią RODO).

2) Zatrudnienie

1. Przestrzeganie zasad Polityki jest bezwzględnie wymagane przez wszystkich pracowników, współpracowników, wykonawców i podwykonawców. Pracownicy, współpracownicy, wykonawcy i podwykonawcy **Administratora** są świadomi swoich obowiązków i odpowiedzialności prawnej oraz zagrożeń związanych z ochroną danych. Świadomość ta budowana jest u wyżej wymienionych osób poprzez:
    a) odpowiednie wprowadzenie w obowiązki i przeprowadzenie szkolenia przed przyznaniem im dostępu do informacji;
    b) uzyskiwanie od tych osób pisemnych potwierdzeń zapoznania się z zasadami dotyczącymi ochrony danych osobowych;
    c) przedstawienie wytycznych dotyczących zależności między procedurami bezpieczeństwa, a zakresem ich czynności;
    d) cykliczne przeprowadzanie odpowiednich kursów i szkoleń z zakresu ochrony danych osobowych;
    e) podtrzymywanie umiejętności i uzyskiwanie nowych kwalifikacji.
2. W przypadku naruszenia zasad ochrony danych oraz danych osobowych przez pracowników, współpracowników, wykonawców i podwykonawców zostaje wszczęte postępowanie dyscyplinarne, w którym gromadzony jest odpowiedni materiał dowodowy. Postępowanie dyscyplinarne uwzględnia przede wszystkim rodzaj i wagę naruszenia zasad ochrony danych, wpływ na procesy biznesowe oraz charakter naruszenia (czy jest to przypadek incydentalny, czy też jest to kolejne naruszenie).

3) Zakończenie lub zmiana zatrudnienia

1. Rozwiązanie umowy z pracownikiem, współpracownikiem, wykonawcą lub podwykonawcą Administratora lub zmiana stanowiska pracy wewnątrz firmy odbywa się w sposób zorganizowany i odpowiednio udokumentowany.
2. Dokumenty pracownicze, po ustaniu zatrudnienia, przechowywane są maksymalnie przez okres 10 lub 50 lat (poza dokumentami nie związanymi z realizacją przepisów Kodeksu Pracy).
3. Po zakończeniu zatrudnienia (zakończenie stosunku pracy lub rozwiązanie innej umowy) pracownicy, współpracownicy, wykonawcy lub podwykonawcy są zobowiązani do zwrotu wszystkich posiadanych zasobów firmy (m.in. sprzętu, oprogramowania, akcesoriów komputerowych, kart dostępu i kart kredytowych, podręczników i książek) oraz wszelkich informacji zapisanych na dyskach i nośnikach przenośnych. Ponadto, powinni oni usunąć wszelkie przetwarzane dane osobowe w sposób uniemożliwiający ich odtworzenie. W przypadku, gdy przy wykonywaniu umowy korzystali ze sprzętu będącego własnością wykonawcy lub podwykonawcy, wszystkie informacje zostają przekazane Administratorowi i skutecznie usunięte z tego sprzętu. Pracownicy, współpracownicy, wykonawcy i podwykonawcy powinni

przekazać Administratorowi odpowiednie oświadczenie, potwierdzające wypełnienie powyższych obowiązków, najpóźniej w dniu rozwiązania umowy z Administratorem.

4. W przypadku zmiany stanowiska podstawową zasadą jest zatrzymanie posiadanego sprzętu i zmiana prawa dostępu stosownie do nowego zakresu czynności.
5. Jedną z podstawowych zasad ochrony danych u **Administratora** jest, aby po każdorazowym zakończeniu zatrudnienia pracownika lub zmianie stanowiska, dokonać przeglądu praw dostępu do aktywów i systemów informatycznych. W takich przypadkach zadaniem osób zarządzających siecią jest natychmiastowa aktualizacja rejestrów dostępu oraz zmiana haseł do kont aktywnych. Jeżeli prawa dostępu były przyznane większej liczbie osób niż tylko osobom odchodzącym, osoba odpowiedzialna za udzielanie dostępów zobowiązana jest do usunięcia odchodzących osób z każdej grupy. Dodatkowo, pozostali pracownicy są informowani na bieżąco na temat zmian w zatrudnieniu oraz zobowiązani są do zachowania poufności w stosunku do odchodzących pracowników.
6. Wybrani pracownicy, współpracownicy, wykonawcy lub podwykonawcy Administratora zobowiązani do realizacji swoich obowiązków wykorzystują zasoby, którymi dysponuje przedsiębiorstwo. Za każdy z zasobów przedsiębiorstwa odpowiada osoba, której zostały one przekazane. Podczas przekazywania zasobów danej osobie, spisywany jest odpowiedni protokół zdawczo-odbiorczy, w którym zamieszczane są informacje o udostępnianym zasobie. W protokole tym znajdują się m.in.:
    a) rodzaj i nazwa zasobu (np. telefon komórkowy, laptop, samochód);
    b) stan urządzenia (np. nowy, używany, po regeneracji);
    c) dodatki (np. ładowarka, uchwyt na telefon);
    d) imię i nazwisko osoby odpowiedzialnej za dany zasób;
    e) inne.

    Każdy z zasobów, udostępniony przez **Administratora** powinien być użytkowany zgodnie z jego przeznaczeniem, tj. do celów związanych z realizacją zadań wynikających z umowy. Zasoby te powinny być również utrzymywane w stanie pozwalającym na ich bezawaryjne użytkowanie, natomiast każde uszkodzenie zasobu, czy jego podzespołu, powinno być natychmiast, niezwłocznie po jego wykryciu, usunięte.

    W momencie zakończenia współpracy pomiędzy **Administratorem**, a poszczególnymi pracownikami firmy lub kontrahentami, nakazany jest zwrot zasobów do siedziby przedsiębiorstwa. Zasoby te powinny być zwracane w stanie pozwalającym na ich dalsze wykorzystanie. Podczas ich zwrotu, dokonuje się spisania protokołu zdawczego, który zawiera te same informacje, które umieszczane są w protokole odbiorczym. Za wszelkie wady i uszkodzenia zasobów, które nie zostały w porę zgłoszone do naprawy lub usunięte, odpowiada osoba, która była za nie odpowiedzialna. Przy okazji podpisywania protokołu odbiorczego należy uzyskać oświadczenie o zwrocie lub usunięciu wszelkich przetwarzanych danych osobowych.

X. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw

lub wolności osób fizycznych.

2. Celem Procedury Zarządzania Incydentami Związanymi z Ochroną Danych jest określenie zadań pracowników w zakresie:
   a) ochrony wszystkich informacji przed ich modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem, a także utratą oraz ochroną zasobów technicznych;
   b) prawidłowego reagowania pracowników przy przetwarzaniu danych, w przypadku stwierdzenia ich naruszenia (zwłaszcza naruszenia ochrony danych osobowych) lub naruszenia zabezpieczeń systemu informatycznego;
   c) ograniczenia ryzyka powstania zagrożeń oraz minimalizacji skutków wystąpienia zagrożeń.
3. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych (organowi nadzorczemu) bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
4. W przypadku naruszenia ochrony danych osobowych, należy oprócz zgłoszenia przełożonemu, zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zgłosić to naruszenie właściwemu organowi nadzorczemu, a także w uzasadnionych przypadkach, wszystkim osobom, których to naruszenie dotyczy.
5. Zarządzanie ciągłością działania ma na celu zapewnienie ciągłości realizacji krytycznych dla organizacji procesów biznesowych również w sytuacji kryzysowej, w której nie są dostępne aktywa niezbędne do realizacji tych procesów. Zarządzanie ciągłością działania powinno uwzględniać wszelkie kategorie zdarzeń, które uniemożliwiają realizację krytycznych procesów przez czas dłuższy, niż dopuszczalny dla organizacji – zarówno te, które noszą znamiona katastrofy (pożar, powódź itp.), jak i te, które dotyczą wyłącznie wewnętrznych spraw danej organizacji (np. awaria krytycznego systemu informatycznego, niewywiązanie się dostawcy usług z obowiązków określonych w umowie, itp.).
6. Zapewnianie ciągłości działania jest zwykle utożsamiane tylko z wykonywaniem i przechowywaniem tzw. kopii zapasowych (nazywanych także kopiami bezpieczeństwa) oraz w razie potrzeby, odtwarzaniem z nich zasobów informacyjnych organizacji. Jest to w istocie problem znacznie bardziej skomplikowany i wymagający znacznie większej wiedzy i nakładów (organizacyjnych, finansowych, pracy ludzkiej itd.) niż zwykłe wykonywanie kopii zapasowych.
7. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
8. Ochrona bezpieczeństwa danych osobowych u Administratora, to nie tylko szereg działań technicznych prawnych i organizacyjnych, ale również zarządzanie zasobami informatycznymi oraz zarządzanie informacją. Wymogi te stawiane są wszystkim przedsiębiorstwom przetwarzającym dane osobowe, bez względu na ich charakter działalności, wielkość czy obrót roczny.

9. Dobór zabezpieczeń u Administratora z uwagi na koszty, został zaimplementowany stosownie do wartości szkód, które mogłaby ponieść firma w sytuacji ich niezastosowania. Na tej podstawie określane zostały cele bezpieczeństwa przedsiębiorstwa i jego systemów, na które składają się między innymi:
    a) identyfikacja zasad bezpiecznego przetwarzania danych osobowych;
    b) szkolenie wstępne oraz systematyczne szkolenia;
    c) bieżące uświadamianie pracowników o zagrożeniach;
    d) monitorowanie aktualnego stanu bezpieczeństwa;
    e) monitorowanie zmian;
    f) doskonalenie systemów bezpieczeństwa.
10. Administrator, zgodnie z art. 33 ust. 5 RODO, dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
11. W przypadku stwierdzenia naruszenia zasad ochrony danych osobowych będącego skutkiem działań pracownika, Administrator może zastosować wobec tego pracownika karę zgodnie z zasadami określonymi w kodeksie pracy oraz innych przepisach prawa pracy. W przypadku, gdy naruszenie tych zasad jest wynikiem działań współpracownika, wykonawcy lub podwykonawcy, kwestia odpowiedzialności powinna być uregulowana w odpowiedniej umowy.

XI. Powierzenie przetwarzania danych osobowych

1. Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
3. Administrator nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.
4. Wzór umowy, o której mowa w pkt 7 ust. 1, stanowi załącznik do niniejszej polityki.

XII. Przekazanie danych do państwa trzeciego

1. Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

XIII. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową. W przypadku współpracowników, wykonawców lub podwykonawców podstawą odpowiedzialności jest umowa z Administratorem oraz przepisy powszechnie obowiązujące, w tym przepisy dotyczące odpowiedzialności kontraktowej lub deliktowej wynikające z Kodeksu cywilnego.

2. Niniejsza Polityka określa podstawowe cele, zasady, kierunki zarządzania ochroną danych. Stanowi ona jednocześnie pewnego rodzaju podręcznik dla osób odpowiedzialnych za przetwarzanie danych u **Administratora**.
3. Ogólnym celem zarządzania ochroną danych jest, m.in.: redukcja strat związanych z wyciekiem lub incydentem w zakresie danych osobowych a także troska o ww. dane w obrębie zatrudnianej kadry pracowniczej i wśród współpracowników/pacjentów.
4. Wszystkie incydenty związane z ochroną danych każdorazowo powinny być zgłaszane do Administratora.
5. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora.
6. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora;
7. Każdy, kto przetwarza dane posiadane przez Administratora, zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
8. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
9. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy RODO oraz ustawy o ochronie danych osobowych.
10. Integralną część niniejszej Polityki ochrony danych stanowią załączone dokumenty.