POLITYKA BEZPIECZEŃSTWA

obowiązująca u przedsiębiorcy Bożeny Grudy

prowadzącej działalność gospodarczą pod firmą

NZOZ – PORADNIA STOMATOLOGICZNA Bożena Gruda

z siedzibą w Skierniewicach przy  ul.  Armii Krajowej 59/5, 96-100 Skierniewice, NIP: 8361015866, REGON: 750442190

|  |
| --- |
| **SPIS TREŚCI** |

|  |  |  |
| --- | --- | --- |
| I. | Postanowienia ogólne | 3 |
| II. | Obowiązki Administratora Danych Osobowych | 4 |
| III. | Zasady przetwarzania danych osobowych | 5 |
| IV. | Osoby upoważnione do przetwarzania danych osobowych | 8 |
| V. | Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych | 9 |
| VI. | Procedura postępowania w przypadku naruszenia bezpieczeństwa danych osobowych | 10 |
| VII. | Przeglądy Polityki Bezpieczeństwa i audyty systemu | 12 |
| VIII. | Postanowienia końcowe | 12 |
| IX. | Wykaz załączników | 13 |

|  |
| --- |
| **I. POSTANOWIENIA OGÓLNE** |

1. Niniejszym wprowadza się niniejszą Politykę Bezpieczeństwa w celu zadośćuczynienia obowiązującym przepisom z zakresu ochrony danych osobowych oraz zapewnieniu przetwarzanym danym osobowym bezpieczeństwa.
2. Jeśli w niniejszej Polityce Bezpieczeństwa mowa o:
   1. **Administratorze Danych Osobowych (ADO) –** rozumie się przez to podmiot decydujący o celach i środkach przetwarzania danych osobowych**;** w rozumieniu niniejszej Polityki Bezpieczeństwa ADO jest pani Bożena Gruda prowadząca działalność gospodarczą pod firmą NZOZ – PORADNIA STOMATOLOGICZNA Bożena Gruda z siedzibą w Skierniewicach przy ul. Armii Krajowej 59/5, 96-100 Skierniewice, NIP: 8361015866, REGON: 750442190;
   2. **bezpieczeństwie danych** – rozumie się przez to zapewnienie danym osobowym poufności i integralności;
   3. **danych wrażliwych** - rozumie się przez to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;
   4. **Ewidencji Upoważnień** – rozumie się przez to ewidencję udzielonych upoważnień do przetwarzania danych osobowych;
   5. **Instrukcji** – rozumie się przez to instrukcję zarządzania systemem informatycznym sporządzoną i wdrożoną przez Przedsiębiorcę;
   6. **inspektorze ochrony danych osobowych** - rozumie się przez to osobę, o której mowa w Sekcji 4 RODO;
   7. **integralności danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   8. **odbiorcy danych -** rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów administracji publicznej, które mogą otrzymywać dane osobowe w ramach konkretnego prowadzonego przez nie postępowanie;
   9. **organie nadzorczym** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych;
   10. **poufności danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
   11. **przetwarzaniu** **danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   12. **RODO** - rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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);
   13. **rozliczalności** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   14. **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
3. Polityka Bezpieczeństwa reguluje całościowo dopuszczalny prawem sposób zarządzania i ochrony danych osobowych oraz prawa osób, których dane osobowe są przetwarzane przez ADO.
4. Polityka odnosi się do wszelkich danych osobowych przetwarzanych przez ADO, w zbiorach danych lub poza nimi.
5. Celem Polityki Bezpieczeństwa jest:
   1. wskazanie działań, jakie należy podjąć, formy tych działań oraz sposób ich przeprowadzania, niezbędnych do zadośćuczynienia obowiązkom ciążącym na ADO;
   2. stworzenie podstaw organizacyjnych dla wdrożenia systemu zarządzania bezpieczeństwem danych osobowych przez ADO;
   3. określenie podstawowych zasad i wymagań organizacyjno-technicznych oraz prawnych dla zapewnienia właściwej ochrony bezpieczeństwa danych osobowych;
   4. właściwe udokumentowanie przypadków naruszenia bezpieczeństwa oraz zapewnienie właściwego trybu działania w celu przywrócenia bezpieczeństwa danych.
6. ADO deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania wszelkim zagrożeniom bezpieczeństwa danych osobowych.

|  |
| --- |
| **II. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH** |

1. ADO realizuje zadania w zakresie ochrony danych osobowych, w szczególności:
   1. nadzoruje opracowanie i aktualizację Polityki Bezpieczeństwa i Instrukcji;
   2. nadzoruje przestrzeganie zasad określonych w Polityce Bezpieczeństwa i Instrukcji;
   3. zapewnia środki techniczne i organizacyjne zapewniające ochronę danych osobowych;
   4. zapewnia, że dostęp do danych osobowych mają jedynie osoby upoważnione;
   5. zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez podmiot nieuprawniony, zmianą, utratą, uszkodzeniem lub zniszczeniem;
   6. zapewnia legalność przetwarzania danych osobowych na zasadach określonych w stosownych przepisach;
   7. zapewnia zgodne z przepisami prawa udostępnianie i powierzanie danych osobowych;
   8. podejmuje odpowiednie działania w przypadku zagrożenia bezpieczeństwa przetwarzania danych osobowych.
2. ADO samodzielnie zarządza działającym u niego systemem informatycznym, w którym przetwarzane są dane osobowe, w szczególności:
   1. zapewnia prawidłowe użytkowanie systemu informatycznego;
   2. przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego, ustawia i modyfikuje uprawnienia, wyrejestrowuje oraz usuwa konta użytkowników;
   3. wyjaśnia wszystkie zgłoszone nieprawidłowości i incydenty dotyczące przetwarzania danych z wykorzystaniem środków informatycznych.
3. ADO może upoważnić inny podmiot do zarządzania działającym u niego systemem informatycznym, w którym przetwarzane są dane osobowe.
4. ADO wyznacza inspektora ochrony danych osobowych i publikuje informacje na jego temat w miejscu łatwo dostępnym dla osób, których dane dotyczą.
5. ADO dokonał oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO, a która stanowi Załącznik nr 8 do niniejszej Polityki Bezpieczeństwa.

|  |
| --- |
| **III. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH** |

1. Przetwarzanie danych osobowych u ADO następuje za zgodą osoby, której dane dotyczą, lub na podstawie odpowiednich przepisów zezwalających na ich przetwarzanie. Przez zgodę osoby, której dane dotyczą, rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda osoby, której dane dotyczą, nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być wycofana w każdym czasie. Zgoda osoby, której dane dotyczą, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. Wymagana jest ponowna zgoda osoby, której dane dotyczą, jeżeli cel przetwarzania uległ zmianie.
2. Podczas pozyskiwania danych osobowych przekazuje się osobie, której dane dotyczą, następujące informacje:
   1. dane ADO, ewentualnie dane dalszych administratorów (procesorów),
   2. dane inspektora ochrony danych osobowych,
   3. cele przetwarzania danych osobowych,
   4. podstawę prawną przetwarzania danych osobowych,
   5. informacje o odbiorcach danych osobowych lub ich kategoriach,
   6. okres, przez który dane osobowe będą przechowywane lub kryteria jego ustalania,
   7. informacje o prawie do żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   8. prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   9. prawie wniesienia skargi do organu nadzorczego;
   10. czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
   11. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
3. ADO, z racji charakteru swojej działalności gospodarczej, przetwarza dane osobowe wrażliwe. Ich przetwarzanie następuje w celu ochrony stanu zdrowia, świadczenia usług medycznych (stomatologicznych) lub leczenia pacjentów przez ADO jako osobę trudniącą się zawodowo leczeniem lub świadczeniem innych usług medycznych oraz w celu zarządzania udzielaniem usług medycznych.
4. Przetwarzane są tylko takie dane, które są niezbędne dla realizacji celu, o którym mowa w dziale III ust. 3 oraz do innych prawnie dozwolonych celów, dla których spełnienia zbieranie danych osobowych jest niezbędne w ramach działalności ADO.
5. Przetwarzanie danych dla innych celów niż te, dla których zostały zebrane, jest dopuszczalne jeśli:
   1. cele te są zgodne;
   2. nie narusza praw i wolności osoby, której dane dotyczą;
   3. następuje w celach statystycznych z zachowaniem stosownych przepisów. ADO nie przewiduje jednak gromadzenia ani przetwarzania danych osobowych w celach statystycznych.
6. ADO przetwarza dane osobowe zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
7. ADO stosuje zasadę minimalizacji danych, a zatem przetwarza dane osobowe wyłącznie w zakresie, jaki jest niezbędny do celów, w których są przetwarzane.
8. ADO zapewnia, że dane osobowe są prawidłowe i w razie potrzeby uaktualniane, podejmując wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
9. ADO przechowuje dane osobowe w formie umożliwiającej identyfikację osoby, której dane dotyczą.
10. ADO przetwarza dane osobowe w następujących zbiorach:
    1. CV kandydatów na pracowników (w formie elektronicznej) – zwierającą takie dane jak imię (imiona) i nazwisko, data urodzenia, dane kontaktowe, wykształcenie, przebieg dotychczasowego zatrudnienia; zbiór jest przetwarzany jedynie w momencie prowadzenia rekrutacji pracownika, a po jej zakończeniu wszelkie dokumenty zawierające dane osobowe kandydatów są trwale usuwane (za wyjątkiem CV zatrudnionego, który to dokument jest przenoszony do innego zbioru);
    2. akta pracownicze (w formie papierowej) - zwierającą takie dane jak imię (imiona) i nazwisko, data urodzenia, dane kontaktowe, wykształcenie, przebieg dotychczasowego zatrudnienia, numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość, ewentualnie dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, w uzasadnionych przypadkach także informacje o stanie zdrowia;
    3. elektroniczną dokumentację medyczną – zawierającą takie dane jak imię, nazwisko, PESEL, adres zamieszkania, numer telefonu, data urodzenia oraz informacje o stanie zdrowia, w tym o stosowaniu używek;
    4. elektroniczną bazę danych programu EasyDent - zawierającą takie dane jak imię, nazwisko, PESEL, adres zamieszkania, numer telefonu, data urodzenia oraz informacje o stanie zdrowia, informacje o przeprowadzonych zabiegach medycznych, oraz o stosowaniu używek;
    5. dokumentacji księgowej – zawierającej takie dane jak imię, nazwisko, firma, adres prowadzenia działalności gospodarczej, NIP, REGON, adres mailowy czy numer telefonu kontrahentów ADO.
11. ADO przechowuje dane osobowe przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Ustalając ten okres ADO bierze pod uwagę przepisy dotyczące okresu przechowywania akt pracowniczych, dokumentacji płacowej oraz dokumentacji medycznej. Tę ostatnią, zgodnie z treścią art. 29 ustawy z dnia 6 listopada 2008 roku o prawach pacjenta i Rzeczniku Praw Pacjenta, przechowuje się przez okres 20 lat licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem:
    1. dokumentacji medycznej 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;
    2. zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną pacjenta, które są przechowywane przez okres 10 lat, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie;
    3. skierowań na badania lub zleceń lekarza, które są przechowywane przez okres:
       1. 5 lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza;
       2. 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;
    4. dokumentacji medycznej dotyczącej dzieci do ukończenia drugiego roku życia, która jest przechowywana przez okres 22 lat.
12. Udostępnianie danych osobowych może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać następujące informacje:
    1. oznaczenie wnioskodawcy;
    2. wskazanie podstawy prawnej;
    3. określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia;
    4. wskazanie imienia, nazwiska osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią.
13. Udostępnianie danych osobowych na podstawie ustnego wniosku jest dopuszczalne tylko w przypadku, gdy zachodzi konieczność niezwłocznego działania.
14. Powierzenie przez ADO przetwarzania danych osobowych dalszemu administratorowi (procesorowi) następuje wyłącznie na podstawie pisemnej umowy sporządzonej zgodnie z art. 28 RODO.
15. ADO prowadzi rejestr udostępnień danych osobowych, który stanowi Załącznik nr 1 do niniejszej Polityki Bezpieczeństwa.
16. Wszelkie czynności przetwarzania danych osobowych odnotowuje się w Rejestrze czynności przetwarzania, który stanowi Załącznik nr 5 do niniejszej Polityki Bezpieczeństwa.
17. Obszarem przetwarzania danych osobowych są pomieszczenia przeznaczone do prowadzenia działalności gospodarczej – gabinetu stomatologicznego – w siedzibie ADO w Skierniewicach przy ul.  Armii Krajowej 59/5, 96-100 Skierniewice.

|  |
| --- |
| **IV. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH** |

1. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez ADO oraz która złożyła pisemne oświadczenie o zachowaniu danych osobowych w poufności.
2. Wzór upoważnienia stanowi Załącznik nr 2 do niniejszej Polityki Bezpieczeństwa, a wzór oświadczenia o zachowaniu danych w poufności – Załącznik nr 3. Upoważnienia rejestruje się w Ewidencji upoważnień, która stanowi Załącznik nr 4.
3. Osoba posiadająca upoważnienie do przetwarzania danych osobowych jest uprawniona do ich przetwarzania wyłącznie w zakresie i czasie wskazanym w upoważnieniu.
4. Osoba upoważniona do przetwarzania danych osobowych musi zostać uprzednio odpowiednio przeszkolona, zapoznana z Polityką Bezpieczeństwa, Instrukcją oraz obowiązującymi przepisami dotyczącymi ochrony danych osobowych.
5. Osoba upoważniona do przetwarzania danych osobowych ma obowiązek:
   1. zachować tajemnicę danych osobowych;
   2. przestrzegać procedur bezpiecznego przetwarzania danych osobowych zawartych w szczególności w Polityce Bezpieczeństwa oraz Instrukcji;
   3. zabezpieczać dane osobowe przed ich udostępnianiem osobom nieupoważnionym, utratą oraz niepożądaną zmianą;
   4. nieprzenosić danych osobowych poza zbiór danych;
   5. wylogowywać się w trakcie przerwy a także po zakończeniu pracy na komputerze posiadającym dostęp do zbioru danych;
   6. udostępniać dane osobowe drogą elektroniczną tylko w postaci zaszyfrowanej;
   7. niepozostawiać osób trzecich w pomieszczeniach, w których przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
   8. zamykać okna w razie opuszczania pomieszczeń, w których przetwarzane są dane osobowe;
   9. zamykania drzwi na klucz w razie opuszczania pomieszczeń, w których przetwarzane są dane osobowe.

|  |
| --- |
| **V. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH** |

1. Ochrona danych osobowych jest realizowana poprzez zabezpieczenia fizyczne, zabezpieczenia organizacyjne, zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej, zabezpieczenia narzędzi programowych i baz danych oraz przez osoby upoważnione.
2. Zabezpieczenia organizacyjne:
   1. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
   2. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
   3. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
   4. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane – nie są skierowane w stronę okien ani drzwi oraz są zabezpieczone wygaszaczami ekranu oraz hasłem;
   5. Dokumenty papierowe zawierające dane osobowe przechowywane są w segregatorach umieszczonych w zamkniętych na klucz szafach;
   6. Uruchomione tablety nie są zostawiane bez nadzoru.
   7. Skanowane dokumenty papierowe po skutecznym umieszczeniu ich wersji elektronicznej na dysku twardym komputera stacjonarnego są niszczone w sposób uniemożliwiający ich odczyt.
3. Zabezpieczenia ochrony fizycznej danych osobowych:
   1. Zbiory danych osobowych przechowywane są w lokalu wyposażonym w zabezpieczenia przeciwpożarowe - wentylację grawitacyjną oraz wymuszoną, koce gaśnicze i gaśnicę; lokal ma wyznaczone ścieżki ewakuacji;
   2. Dostęp do lokalu, w którym przetwarzane są dane osobowe, jest nadzorowany przez służbę ochrony;
   3. Lokal jest wyposażony w okna ze szkłem antywłamaniowym typu P2 oraz alarm antywłamaniowy
   4. Do niszczenia dokumentów papierowych używa się niszczarki;
   5. W razie awarii niszczarki i konieczności niszczenia ręcznego – dokument powinien być podarty na paski nie szersze niż 1 cm.
4. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
   1. Do przetwarzania danych osobowych w systemach informatycznych stosowane są wyłącznie komputery stacjonarne;
   2. Dostęp do systemu operacyjnego komputerów, w których przetwarzane są dane osobowe, zabezpieczone są za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
   3. Dostęp do systemu operacyjnego tabletów stosowanych do przetwarzania danych osobowych jest zabezpieczony za pomocą procesu uwierzytelniania;
   4. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity;
   5. Użyto system Firewall do ochrony dostępu do sieci komputerowej;
   6. Do skanowania dokumentów celem umieszczenia ich w dokumentacji medycznej stosuje się oprogramowanie dedykowane tej dokumentacji.
5. Zabezpieczenia narzędzi programowych i baz danych:
   1. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
   2. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
   3. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
   4. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
6. Zastosowane zabezpieczenia mają służyć osiągnięciu celów przetwarzania danych oraz zapewnić poufność, integralność i rozliczalność danych osobowych oraz integralność systemu.

|  |
| --- |
| **VI. PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH** |

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest poinformować ADO o każdym przypadku stwierdzenia naruszenia danych osobowych.
2. Przez naruszenie danych osobowych rozumie się naruszenie bezpieczeństwa danych osobowych, które spowodowało ich nieuprawnione udostępnienie, zniszczenie lub uszkodzenie. Może przyjąć postać:
3. naruszenia poufności – polegającego na ujawnienie danych osobowych osobie nieuprawnionej,
4. naruszenia dostępności – polegającego na trwałej utracie lub zniszczeniu danych osobowych,
5. naruszenia integralności – polegającego na zmianie treści danych osobowych w sposób nieautoryzowany.
6. Aby zdarzenie można było uznać za naruszenie danych osobowych, muszą zostać łącznie spełnione trzy przesłanki:
   1. naruszenie musi dotyczyć danych osobowych przetwarzanych przez ADO,
   2. skutkiem naruszenia musi być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,
   3. naruszenie musi być skutkiem złamania zasad bezpieczeństwa danych.
7. W przypadku stwierdzenia zaistnienia naruszenia danych osobowych ADO prowadzi postępowanie wyjaśniające, w toku którego ustala:
   1. przyczynę sytuacji,
   2. jakie mogą być jej skutki,
   3. stopień ryzyka naruszenia praw i wolności osób, których dane dotyczą,
   4. możliwość i zasadność podjęcia działań, które zminimalizują ryzyko zaistnienia podobnej sytuacji w przyszłości,
   5. osoby odpowiedzialne za sytuację.
8. Stopień ryzyka naruszenia praw i wolności osób, których dane dotyczą może być:
   * 1. niski – jeżeli skutki naruszenia w żaden sposób nie mogą w żaden sposób wpłynąć na prawa i wolności osób, których dane dotyczą; np. doszło do trwałego zniszczenia zbioru danych zwierającego umówionych wizyt w gabinecie stomatologicznym, które miały już miejsce;
     2. średni - jeżeli skutki naruszenia potencjalnie mogą wpłynąć na prawa i wolności osób, których dane dotyczą, jednakże ADO jest w stanie tym skutkom zapobiec lub je zminimalizować; np. doszło do uszkodzenia akt osobowych w wyniku zalania, jednakże w zakresie, jaki pozwala na ich odtworzenie; doszło do powierzenia przetwarzania danych osobowych bez zawarcia umowy powierzenia i bez upewnienia się, że procesor jest w stanie zapewnić danym osobowym bezpieczeństwo, jednakże procedury te zostały dopełnione w późniejszym czasie, a procesor zapewnił danym odpowiednią ochronę;
     3. wysoki - jeżeli skutki naruszenia wpływają na prawa i wolności osób, których dane dotyczą, a skutków tych nie da się zminimalizować; np. wskutek nieprawidłowego zabezpieczenia dokumentacji doszło do jej kradzieży lub całkowitego zniszczenia.
9. W zależności od stwierdzonego stopnia ryzyka naruszenia praw i wolności osób, których dane dotyczą, ADO podejmuje następujące działania:
   * 1. stopień niski – wpisuje naruszenie danych osobowych do Załącznika nr 5 (rejestru naruszeń danych osobowych);
     2. stopień średni - wpisuje naruszenie danych osobowych do Załącznika nr 5 oraz, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza incydent organowi nadzorczemu;
     3. stopień wysoki - wpisuje naruszenie danych osobowych do Załącznika nr 5 oraz, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza incydent organowi nadzorczemu oraz zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
10. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
11. Zgłoszenia organowi nadzorczemu dokonuje się na formularzu publikowanym na stronie Urzędu Ochrony Danych Osobowych. Formularz załącza się do pisma ogólnego na platformie biznes.gov.pl.
12. ADO odnotowuje zgłoszenia naruszeń danych osobowych w Załączniku nr 5, załączając do niego wydruki formularzy, o których mowa w Rozdziale VI ust. 7 niniejszej Polityki Bezpieczeństwa.
13. Zawiadomienie osoby, której dane dotyczą, w przypadku, o którym mowa w Rozdziale VI ust. 6 lit. c niniejszej Polityki Bezpieczeństwa, następuje bez zbędnej zwłoki. Wzór zgłoszenia stanowi Załącznik nr 6 do niniejszej Polityki Bezpieczeństwa.
14. Zawiadomienie, o którym mowa w Rozdziale VI ust. 10, mimo stwierdzenia wysokiego stopnia ryzyka naruszenia praw i wolności osób, których dane dotyczą nie jest konieczne, jeśli:
    1. zostały wdrożone odpowiednie techniczne i organizacyjne środki ochrony uniemożliwiające odczyt danych osobowych, których bezpieczeństwo zostało naruszone;
    2. wymagałoby ono niewspółmiernie dużego wysiłku.
15. W sytuacji, o której mowa w Rozdziale VI ust. 11 lit. b, ADO zamieści publiczny komunikat zawierający odnośne informacje.

|  |
| --- |
| **VII. PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA** |

1. Co najmniej raz w każdym roku kalendarzowym dokonuje się przeglądu niniejszej Polityki Bezpieczeństwa pod kątem aktualności oraz zgodności deklarowanego w niej stanu z prawem.
2. Polityka Bezpieczeństwa podlega aktualizacji w każdym przypadku, gdy zaistnieje taka potrzeba.

|  |
| --- |
| **VIII. POSTANOWIENIA KOŃCOWE** |

1. Przypadki nieuzasadnionego zaniechania obowiązków lub naruszenia innych zasad wynikających z niniejszej Polityki Bezpieczeństwa mogą stanowić podstawę do pociągnięcia danej osoby do odpowiedzialności, adekwatnie do łączącego ją z Przedsiębiorcą stosunku prawnego.
2. W sprawach nieuregulowanych niniejszą Polityką Bezpieczeństwa mają zastosowanie przepisy adekwatnych aktów prawnych.
3. Niniejsza Polityka Bezpieczeństwa – która stanowi zaktualizowaną wersję poprzedniej Polityki Bezpieczeństwa - wchodzi w życie z dniem 25 maja 2018 roku.

|  |
| --- |
| **IX. WYKAZ ZAŁĄCZNIKÓW** |

|  |  |
| --- | --- |
| Załącznik nr 1 | Rejestr udostępnień danych osobowych |
| Załącznik nr 2 | Wzór upoważnienia do przetwarzania danych osobowych |
| Załącznik nr 3 | Wzór oświadczenia o zachowaniu danych w poufności |
| Załącznik nr 4 | Ewidencja upoważnień |
| Załącznik nr 5 | Rejestr czynności przetwarzana danych osobowych |
| Załącznik nr 6 | Rejestr naruszeń danych osobowych |
| Załącznik nr 7 | Wzór informacji o naruszeniu bezpieczeństwa danych osobowych |
| Załącznik nr 8 | Ocena skutków dla ochrony danych |