

UWARUNKOWANIA PRAWNE ZWIĄZANE Z BEZPIECZEŃSTWEM WRAŻLIWYCH DANYCH MEDYCZNYCH W TYM DANYCH ELEKTRONICZNYCH.

Zakres i znaczenie informacji zawartych w danych medycznych sprawia, że wymagają one szczególnej ochrony. Symbolem owej szczególnej ochrony była niegdyś tajemnica lekarska. Obecnie jednak, wobec postępu technicznego, który umożliwił przetwarzanie danych - w tym danych o stanie zdrowia - w szerokim zakresie w systemach informatycznych, dających nie tylko możliwość gromadzenia danych, ale ich szybkie opracowanie, a także nieporównanie szerszy dostęp do danych w porównaniu z sytuacją, gdy przetwarzanie odbywa się w systemach tradycyjnych (kartotekach, zbiorach akt), niezbędne stało się wprowadzenie szczególnych zasad ochrony danych.

Wyrazem owej szczególnej ochrony są przepisy prawa regulujące dostęp do danych, m. in. poprzez wskazanie kręgu podmiotów upoważnionych do żądania informacji o stanie zdrowia i prawnych podstaw gromadzenia tych danych

I. Dane medyczne stanowią szczególną kategorię danych o osobach. Pojęcie danych osobowych definiuje Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926). Zgodnie z art. 6 ust. 1: „w rozumieniu ustawy za **dane osobowe** uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej”. Zgodnie z ust. 2 tego artykułu: „Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne”. Natomiast ust. 3 stanowi, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Pojęcie "danych osobowych" nie ma jednorodnego charakteru. Należy wyróżnić **dane o szczególnym charakterze, tzw. dane wrażliwe ("delikatne", "sensytywne"), do których zaliczamy dane medyczne.** Są one przeciwstawiane tzw. danym zwykłym (pospolitym), po to, aby w odniesieniu do danych wrażliwych wprowadzić bardziej intensywną ochronę, a przetwarzanie poddać odrębnym zasadom.

Za dane wrażliwe ustawa o ochronie danych osobowych uznaje m.in. dane dotyczące: **stanu zdrowia, kodu genetycznego, nałogów, życia seksualnego.** Dane te zaliczyć możemy do kategorii **danych medycznych.**

W obowiązującym prawie w Polsce brak jest definicji ustawowej, która wyznaczałaby sposób rozumienia pojęcia **dane medyczne.** Pomocnym przy wykładni tego pojęcia może być tekst Rekomendacji nr (97)5 Komitetu Ministrów Rady Europy. Zgodnie z art. 1 tej Rekomendacji wyrażenie „dane medyczne” odnosi się do wszystkich danych wiążących się ze zdrowiem jednostki, jak i wszelkich danych w sposób oczywisty i bliski związanych ze zdrowiem oraz danych genetycznych. Zgodnie z oficjalnym komentarzem do Rekomendacji pojęcie danych medycznych obejmuje dane odnoszące się do przeszłego, obecnego i przyszłego stanu zdrowia podmiotu danych, zarówno zdrowia fizycznego, jak i psychicznego. Ponadto pojęcie to odnosi się do wszelkich informacji, które nie są informacjami upublicznionymi, a które pozwalają na ustalenie szeroko pojętego stanu zdrowia jednostki, takich jak styl życia osoby, życie seksualne czy nałogi¹.

Za dane medyczne należy uznać dane pozwalające na ustalenie stanu zdrowia zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, oraz informacje, z których tego rodzaju wiadomości przeciętny odbiorca może „wyprowadzić z dużą dozą prawdopodobieństwa”².

Danymi medycznymi są nie tylko informacje bezpośrednio informujące o stanie zdrowia jednostki, ale i informacje, z których te informacje można wyprowadzić. Zakres pojęcia „dane medyczne” jest szerszy niż pojęcia „dane o stanie zdrowia”.

¹ M. Jackowski: *OCHRONA DANYCH MEDYCZNYCH*, Dom Wydawniczy ABC, 2002, s. 27.

² J. Barta, R. Markiewicz: *Ochrona danych*....s.424.

Kryterium wyróżnienia danych medycznych-wrażliwych stanowi okoliczność, iż **dotyczą one bezpośrednio sfer należących do prywatności czy nawet intymności osoby fizycznej. Dane wrażliwe, w przeciwieństwie do pozostałych, wiążą się ze znacznie większym poczuciem zagrożenia oraz niebezpieczeństwem wywołania na różnych polach decyzji dyskryminacyjnych.** Ich ujawnienie może mieć ogromny wpływ nie tylko na realizację ogólnych szans życiowych (np. dane genetyczne dotyczące zwiększonego ryzyka określonych chorób mogą spowodować odmowę zatrudnienia lub ubezpieczenia), lecz także być wykorzystane przeciwko osobie w najmniej oczekiwanych przez nią sytuacjach (np. ujawnienie danych zdrowotnych lub chorobowych osoby publicznej).

II. PRZETWARZANIE DANYCH MEDYCZNYCH

Art. 27 ust. 1 ustawy o ochronie danych osobowych stanowi, że zabrania się przetwarzania danych ujawniających dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym.

Przepis art. 27 dotyczy danych osobowych w znaczeniu, jakie temu terminowi nadaje przepis art. 6 u.o.d.o. (musi istnieć zatem możliwość określenia tożsamości, której dane dotyczą). Tak więc zbieranie i przetwarzanie informacji dotyczących kwestii wymienionych w ust. 1 nie jest zabronione lub ograniczone, jeśli będą to informacje anonimowe.

W zakresie danych wrażliwych zastosowanie znajduje także przepis art. 2 ust. 3 u.o.d.o., w myśl którego: "W odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5."

Jeżeli jednak przetwarzane dane nie mają charakteru anonimowego ani nie są usuwane albo poddawane anonimizacji (zgodnie z art. 2 ust. 3), to - nawet jeśli byłoby to usprawiedliwione celem i metodą badań (np. zamiarem uzyskania odpowiedzi od tych samych osób po upływie kilku lat, aby wychwycić zmianę nastawień) - **konieczne jest dla legalności działań zasadniczo bądź uzyskanie zgody na piśmie od osoby, której dane dotyczą, bądź wskazanie na przepis szczególny innej ustawy zezwalający na przetwarzanie takich danych bez jej zgody, a przy tym stwarzający pełne gwarancje ochrony słuszych interesów jednostki.**

Ustawodawca posługuje się zwrotem "**dane ujawniające (...)**" z czego wnioskować można, iż danymi wrażliwymi będą zarówno informacje "same, wprost stwierdzające", określone w ust. 1 przymioty osoby (np. "osoba A jest chora na cukrzycę"), jak i informacje, z których tego rodzaju wiadomości przeciętny odbiorca może "wyprowadzić" z dużą dozą prawdopodobieństwa (np. "osoba A zmuszona jest do regularnego zażywania insuliny").

Przepis art. 27 ust. 1 wprowadza **zasadę zakazu przetwarzania danych wrażliwych-medycznych**, i to bez względu na to, czy przetwarzanie ma następować w formie zautomatyzowanej czy "tradycyjnej" (manualnej). Postanowienia zezwalające na przetwarzanie takich danych mają zatem charakter przepisów wyjątkowych i w żadnej mierze nie mogą podlegać wykładni rozszerzającej.

Od zasady, iż przetwarzanie danych wrażliwych, w tym danych medycznych jest zakazane, ustawa o ochronie danych osobowych wprowadza **szereg wyjątków, ujętych w zamknięty katalog (ust. 2)**. Przesądza to o zakazie prowadzenia rozszerzającej wykładni. Każda z okoliczności usprawiedliwiających przetwarzanie danych wrażliwych ma charakter autonomiczny i niezależny.

Art. 27 ust. 2 stanowi: „Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli:

- 1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,
- 2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
- 3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
- 4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,
- 5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
- 6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
- 7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
- 8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,
- 9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,
- 10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym”.

Art. 27 ust. 2 pkt 7 u.o.d.o. stanowi, że przetwarzanie danych medycznych (dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym) jest dopuszczalne jeżeli: **„przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych”**.

Przy przetwarzaniu danych medycznych, a więc przy ich przekazywaniu czy innym udostępnianiu należy zaznaczać, iż chodzi o tego rodzaju dane - bądź wprost, bądź nawet przez adnotację „poufne”. Takie zachowanie odpowiada nałożonemu na administratora obowiązkowi dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą (art. 26 ust. 1 u.o.d.o.).

Dla przetwarzania danych wrażliwych, w tym danych medycznych przyjęte zostały (w ust. 2) częściowo odmienne w stosunku do ogólnych - podanych w art. 23 ustawy – „kryteria legalizacyjne”, kryteria zaostrzone. W zakresie jednak, w którym brak szczególnego uregulowania, znajdują zastosowanie zasady ogólne, w szczególności wyrażone w art. 23 i 26 u.o.d.o.

Dane medyczne to m.in. powiązane z określonymi osobami informacje na temat ich stanu zdrowia, prowadzonych badań medycznych czy terapii. Osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych mogą przetwarzać takie dane, o ile stworzone są pełne gwarancje ochrony danych osobowych; pod tym samym warunkiem dopuszczalne jest przetwarzanie danych w celu zarządzania udzielaniem usług medycznych.

Przetwarzanie danych medycznych jest możliwe jeżeli prowadzone jest w celu ochrony stanu zdrowia, leczenia i świadczenia usług medycznych. Przez **pojęcie ochrony stanu zdrowia, leczenia i świadczenia usług medycznych** rozumieć należy także działania profilaktyczne, diagnostyczne, rehabilitacyjne (w tym kuracyjne); tak więc dopuszczalne jest przetwarzanie danych o stanie zdrowia pacjenta również przez te podmioty medyczne, które uczestniczą w kierowaniu pacjenta na leczenie uzdrowiskowe. Z kolei osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych to "personel medyczny", który tworzą nie tylko sami lekarze, ale również personel pomocniczy (pielęgniarki, laboranci), rehabilitanci; bardziej dyskusyjne jest, czy podobnie odnieść się należy do osób zawodowo wykonujących usługi zaliczane do medycyny niekonwencjonalnej, bioenergoterapeutów itd. Nadto można, naszym zdaniem, zasadnie bronić poglądu, iż osobami zawodowo świadczącymi usługi medyczne są również aptekarze.

Do kręgu uprawnionych ustawa zalicza też **osoby, które "zarządzają udzielaniem usług medycznych"**. Chodzi tu głównie o personel administracyjny zatrudniony w sektorze szeroko rozumianych usług medycznych, wykonujący rozmaite funkcje sekretarskie, funkcje związane z ewidencją pacjentów, prowadzeniem statystyki, archiwizacją dokumentów medycznych itp. Natomiast usługi medyczne nie rozciągają się na sektor ubezpieczeń na zdrowie czy życie.

Warunkiem powołania się na analizowane upoważnienie **jest stworzenie pełnych gwarancji ochrony danych osobowych**. Dotyczy to, w pierwszym rzędzie, przestrzegania tajemnicy lekarskiej i tajemnicy nałożonej poprzez prawo lub umowę na inne osoby pracujące w sektorze szeroko rozumianych usług medycznych. Uwzględnić należy przy tym **stosowanie odpowiednich zabezpieczeń informatycznych uniemożliwiających dostęp do danych osobom nieupoważnionym**.

1) Udostępnianie danych medycznych:

Szczególnym przypadkiem przetwarzania danych medycznych jest ich udostępnianie. Zgodnie z art. 29 u.o.d.o. udostępnianie danych medycznych w celu ich włączenia do zbioru, a także w celu stworzenia zbioru, oraz w innym celu przez podmiot prywatny odbywa się na podstawie przesłanek legalizujących z art. 27 u.o.d.o. Natomiast w przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

Zgodnie z art. 30 u.o.d.o. administrator danych odmawia udostępnienia danych osobowych ze zbioru danych podmiotom i osobom innym niż wymienione w art. 29 ust. 1, jeżeli spowodowałyby to: ujawnienie wiadomości stanowiących tajemnicę państwową, zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego, zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa, istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

W rozumieniu art. 7 ustawy zbiorem danych jest:

- zestaw danych o charakterze osobowym,
- posiadający własną strukturę,

- w którym dane są dostępne według określonych kryteriów.

Nie jest natomiast istotne to, czy zestaw ten jest scentralizowany czy rozproszony, jednolity albo podzielony funkcjonalnie. Takie podejście uniemożliwia lub przynajmniej utrudnia unikanie poddania się reżimom ustawy o ochronie danych osobowych poprzez dekoncentrację zasobów informatycznych.

Pojęcie zbioru danych obejmuje swym zakresem, zarówno zbiory zautomatyzowane, jak i niezautomatyzowane (manualne, tradycyjne). Poza zakresem działania przepisów pozostawione są natomiast takie akta, które nie posiadają żadnego strukturalnego układu danych osobowych.

Jeśli chodzi o zbiory zautomatyzowane, to będą nimi - jak zaznacza A. Kaczmarek (*Obowiązki administratora danych oraz administratora bezpieczeństwa informacji wynikające z przepisów ustawy o ochronie danych osobowych (w:) Prawa i obowiązki administratora bezpieczeństwa informacji w świetle przepisów ustawy o ochronie danych osobowych*, red. A. Bierć, Warszawa 2000, s. 22) - m.in. bazy danych tworzone przez profesjonalne systemy zarządzania bazami danych, jak i pliki zawierające dane, których strukturę definiuje programista indywidualnie na potrzeby danego systemu. Jak podkreśla przy tym ten autor, kryterium dostępności danych zawartych w zbiorze informatycznym "nie należy oceniać biorąc pod uwagę postać zapisu tych danych na nośniku komputerowym, gdzie są przechowywane, ale przede wszystkim przetwarzający je system komputerowy". Poza tym, "w systemie informatycznym ważne jest to, aby sposób zapisu danych na nośniku komputerowym oraz wbudowane w system procedury ich przetwarzania umożliwiały prawidłowe zestawienie ich struktury wtedy, kiedy to jest potrzebne w czasie ich przetwarzania. Z punktu widzenia ustawy nie jest istotne to, czy dane osobowe zapisane w zbiorze znajdują się fizycznie w jednym pliku danych, rozumianym jako obszar danych na nośniku komputerowym identyfikowany przez system operacyjny komputera, czy w kilkudziesięciu."

2) Wymogi co do jakości przetwarzanych danych:

Do wymogów jakości przetwarzanych danych odnosi się art. 26 u.o.d.o. Przepis ten nakazuje administratorowi danych przetwarzającemu dane osobowe dołożyć szczególnej staranności, w celu ochrony osób których dane dotyczą. Szczególna staranność to staranność wyjątkowa, specjalna, nieprzeciętna, a więc większa od tej, która jest normalnie oczekiwana w obrocie.

Art. 26 u.o.d.o. wskazuje cztery podstawowe zasady jakości przetwarzania danych:

- 1)zasada legalności
- 2)zasada celowości,
- 3)zasada poprawności i adekwatności danych,
- 4)zasada ograniczenia czasowego przechowywania danych.

W myśl zasady legalności dane muszą być przetwarzane zgodnie z prawem. W stosunku do danych medycznych oznacza to konieczność zachowania przesłanek z art. 27 ust. 2 u.o.d.o., ale również obowiązek przestrzegania innych norm prawnych (np. przepisów k.p.k.).

Zgodnie z zasadą celowości dane mogą być zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. (od tej zasady art.26 ust.2 wprowadza wyjątki, które nie odnoszą się do danych medycznych).

Zasada poprawności i adekwatności danych statuuje obowiązek administratora danych polegający na zapewnieniu, by dane medyczne były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Zebrane dane powinny być zgodne z prawdą, kompletne i aktualne. Dane medyczne przetwarzane przez administratora danych nie powinny wykroczać swym rodzajem i treścią poza potrzeby wynikające z celu ich przetwarzania.

Z zasady ograniczenia czasowego przechowywania danych wynika obowiązek przechowywania w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Po osiągnięciu celu przetwarzania danych, dane powinny być usunięte, ewentualnie poddane anonimizacji.

3) Prawa podmiotu danych:

Ustawa o ochronie danych osobowych ustanawia wiele uprawnień szczególnych składających się na prawo do ochrony danych medycznych:

- prawo do informacji o danych medycznych (art. 24 i 25 u.o.d.o.)
- prawo do dostępu do danych medycznych (art. 32 ust.1-5, 33 i 34 u.o.d.o.)
- prawo sprostowania, uzupełnienia, uaktualnienia, wstrzymania przetwarzania danych medycznych
- prawo do wniesienia żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej, jeżeli treść rozstrzygnięcia jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

4) Postępowanie rejestracyjne:

Obowiązek dokonania przez administratora danych rejestracji zbiorów danych u Generalnego Inspektora Ochrony Danych Osobowych ma na celu ochronę tych danych. Administrator jest zobowiązany zarejestrować zbiór przed rozpoczęciem przetwarzania danych, a niespełnienie tego warunku oznacza konieczność zaprzestania przetwarzania danych po uzyskaniu nakazu Generalnego Inspektora Ochrony Danych Osobowych. Wyjątki od obowiązku przewiduje art. 43 u.o.d.o. np. wobec zbiorów zawierających dane dotyczące osób korzystających z usług medycznych administratora danych. Generalny Inspektor Ochrony Danych Osobowych uznał, iż nie podlegają obowiązkowi rejestracji zbiory danych osobowych prowadzone przez zakłady opieki zdrowotnej.

5) Ochrona danych medycznych za pomocą innych przepisów prawa polskiego:

- a) Ustawa z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej. (Dz. U. z dnia 14 października 1991 r.) w art. 18 i 19a.
- b) Kodeks cywilny w art. 23, 23 i 448.
- c) Kodeks karny w art. 266, 267, 268.
- d) Kodeks postępowania karnego w art. 237, 239, 241.
- e) Ustawa z dnia 5 grudnia 1996 r. o zawodzie lekarza w art. 31 i 40. Przepisy te są szczególnego rodzaju *leges speciales* w stosunku do ustawy o ochronie danych osobowych – są to przepisy przewidujące dalej idącą ochronę w rozumieniu art. 5 u.o.d.o.
 - Kodeks postępowania cywilnego art. 261 § 2 i 248 § 2,
 - Kodeks postępowania karnego art. 180.

III. BEZPIECZEŃSTWO DANYCH MEDYCZNYCH

Do obowiązku zabezpieczenia zbiorów danych medycznych odnoszą się przepisy **rozdziału 5 u.o.d.o.** oraz **rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych** (Dz. U. 2004 r. Nr 100 poz. 1024).

Zgodnie z **art. 36 u.o.d.o.** administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Aby skutecznie zapewnić tę ochronę, administrator powinien zabezpieczyć dane medyczne przed ich:

- udostępnieniem osobom nieupoważnionym,

- zabranieniem przez osobę nieuprawnioną,
- przetwarzaniem z naruszeniem ustawy,
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zadania te realizowane powinny być poprzez zastosowanie odpowiednich, skutecznych środków technicznych i organizacyjnych. Ustawodawca nie przesądza, jakie to mają być środki. Mogą być one różnego rodzaju, od rozwiązań architektoniczno-budowlanych, poprzez systemy alarmowe i służby ochrony, aż po środki technicznego i czysto informatycznego charakteru (chip-karty, kody dostępu, systemy kodujące i przeciwdziałające hackingowi). Powinna zachodzić adekwatność między zagrożeniem dla zbioru i rodzajem danych, które zawiera, a skalą i rodzajem zastosowanych środków. W przypadku danych medycznych-sensytywnych należy zastosować środki „wyższego rzędu”, bardziej skuteczne.

Przepis ust. 2 nakłada na administratora danych obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środki wskazane w ust. 1. Obowiązek ten dotyczy wszystkich administratorów danych również przetwarzających dane metodami tradycyjnymi.

Należy dodać, że obowiązki które wskazuje art. 36 nie tylko na administratorze danych, ale także – wówczas gdy administrator powierza innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych, na osobie, która na zlecenie administratora przetwarza takie dane (art. 31 u.o.d.o.).

Na podstawie ust. 3 administrator danych jest zobowiązany do wyznaczenia administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony określonych w ust. 1. Obowiązek ten jest wyłączony jeśli administrator danych sam wykonuje te czynności.

Na podstawie **art. 37 u.o.d.o.** nakłada na administratora danych obowiązek polegający na dopuszczeniu do przetwarzania danych wyłącznie osób posiadających nadane przez niego upoważnienie.

Zwrot „osoby posiadające upoważnienie nadane przez administratora danych” wskazuje, że powinno to być upoważnienie specjalne, odrębne, a nie wywodzone tylko z treści umowy o pracę czy z zakresu obowiązków pracowniczych.

Zgodnie z **art. 38** administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Na podstawie **art. 39 ust. 1** administrator danych zobowiązany jest do prowadzenia ewidencji osób upoważnionych do ich przetwarzania, która powinna zawierać:

- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Art. 39 ust. 2 ustanawia obowiązek ciążyący na osobach, które zostały upoważnione do przetwarzania danych, polegający na zachowaniu w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Rozporządzenie nakłada na administratora danych obowiązek stworzenia i wdrożenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Przepisy Rozporządzenia określają także jej zakres i sposób prowadzenia tej dokumentacji.

Na dokumentację, o której mowa powyżej składa się polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Ponadto rozporządzenie nakłada na administratora danych obowiązek stworzenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz określa wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Zgodnie z § 7 ust. 1. dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten powinien zapewnić odnotowanie:

- daty pierwszego wprowadzenia danych do systemu;
- identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
- źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczyć;
- informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
- sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

Ust. 2 stanowi, że odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

Konieczność dostosowania systemu informatycznego do wymogów określonych w załączniku do Rozporządzenia oznacza wymóg przystosowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych do warunków technicznych i organizacyjnych określonych w Rozporządzeniu z uwzględnieniem zastosowania właściwych środków bezpieczeństwa w zależności od poziomu bezpieczeństwa przetwarzanych danych osobowych.

Zgodnie z § 6 uwzględniając kategorie przetwarzanych danych oraz zagrożenia Rozporządzenie wprowadza trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: podstawowy, podwyższony, albo wysoki.

Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

W pkt. C załącznika do ww Rozporządzenia zostały uregulowane środki bezpieczeństwa na poziomie wysokim:

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych

a siecią publiczną;

b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.

IV. PODPIS ELEKTRONICZNY.

Podpis elektroniczny jest pełnoprawną sygnaturą. Zgodnie z brzmieniem art. 78 ust. 2 kodeksu cywilnego: „Oświadczenie woli złożone w postaci elektronicznej, opatrzone bezpiecznym podpisem elektronicznym, weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu, jest równoważne formie pisemnej”.

W Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. 2001 r. Nr 130 poz. 1450) określono: warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych, zasady nadzoru nad podmiotami świadczącymi te usługi.

Zgodnie z definicją zawartą w art. 3 pkt. 1 ustawy za **podpis elektroniczny** uznaje się dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Istnieją dwa rodzaje podpisów elektronicznych: zwykły i bezpieczny.

Na podstawie art. 3 pkt. 2 ustawy **bezpieczny podpis elektroniczny** to podpis elektroniczny, który:

- a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,
- b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
- c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakkolwiek późniejsza zmiana tych danych jest rozpoznawalna,

Tak zdefiniowany podpis elektroniczny daje wystarczającą pewność, że nie mógł zostać utworzony przez nikogo innego niż osoba, o której tożsamości świadczy. Osoba ta ma wyłączną kontrolę nad urządzeniem do składania podpisu, które to urządzenie spełnia szereg wymagań bezpieczeństwa. Ponadto, złożenie podpisu elektronicznego daje wystarczającą pewność integralności danych, do których został dołączony. Ta ostatnia cecha w zasadniczy sposób odróżnia podpis elektroniczny od tradycyjnego - bezpieczny podpis elektroniczny jest przekształceniem na danych, co oznacza, że za każdym razem jest inny. Jakkolwiek zmiana danych, które zostały podpisane, skutkuje całkowitą zmianą wartości podpisu elektronicznego. Oznacza to, że taki podpis już nie jest elektronicznym odpowiednikiem podpisu złożonego na papierze - w przeciwieństwie do niego nie jest związany ze swoim nośnikiem. Bezpečny podpis elektroniczny chroni całość dokumentu - nie ma potrzeby parafować każdej jego strony i nie ma już oryginału i jego kopii, ponieważ każdy dokument, który został opatrzony ważnym bezpiecznym podpisem elektronicznym nie może już zostać zmieniony, a zatem jest oryginalny.

Aby złożyć podpis elektroniczny trzeba być osobą fizyczną, do tego posiadającą urządzenie służące do składania podpisu elektronicznego. Osoba ta musi jednak działać we własnym imieniu albo w imieniu innej osoby fizycznej, prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej. Każda taka osoba posiada niepowtarzalne i przyporządkowane sobie dane, które są wykorzystywane przez tę osobę do składania podpisu elektronicznego. Te same dane służą do weryfikacji podpisu elektronicznego. Są one wykorzystywane do identyfikacji osoby składającej podpis elektroniczny.

Podpis ten musi być poświadczony przez odpowiedni certyfikat. Możemy mówić o dwóch rodzajach certyfikatu: kwalifikowanym oraz niekwalifikowanym.

Art. 5 ust.1 stanowi, że bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu. Bezpieczny podpis elektroniczny złożony w okresie zawieszenia kwalifikowanego certyfikatu wykorzystywanego do jego weryfikacji wywołuje skutki prawne z chwilą uchylecia tego zawieszenia.

Na podstawie ust. 2 dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej.

Na podstawie art. 5 tylko bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu ma moc prawną i został on zrównany pod względem prawnym z podpisem odręcznym.

Techniki, które umożliwiają stworzenie bezpiecznego podpisu elektronicznego pozwalają także na wiarygodne potwierdzenie jego ważności. Dane służące stwierdzeniu ważności podpisu można publikować w postaci certyfikatów. Zgodnie z definicją zawartą w art. 3 pkt 10 ustawy **certyfikat** to elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.

Na podstawie art. 3 pkt. 12 **certyfikat kwalifikowany** to zaświadczenie w postaci elektronicznej wydawane przez kwalifikowany podmiot świadczący usługi certyfikacyjne, umożliwiające identyfikację osoby, która złożyła dany podpis elektroniczny (elektroniczny dowód tożsamości do podpisów elektronicznych).

Certyfikaty są więc zróżnicowane, w zależności od poziomu bezpieczeństwa, jaki oferują. Wiąże się to ze sposobem, w jaki Ośrodki Certyfikujące dokonują identyfikacji użytkownika.

Poza zebraniem danych, które umożliwiają weryfikację podpisu elektronicznego certyfikaty spełniają jeszcze jedną niezwykle istotną funkcję: wiążą dane weryfikujące podpis z tożsamością osoby, która go utworzyła. Ta właśnie funkcja nadaje wartość dowodową podpisowi, ponieważ można go związać z osobą fizyczną. Umożliwia zastosowanie elektronicznych form do czynności prawnych wykonywanych przez osoby fizyczne oraz nowe poważne zastosowania Internetu.

Zgodnie z Ustawą, za związek tożsamości osoby fizycznej z danymi służącymi do weryfikacji podpisu elektronicznego oraz za dostępność i integralność certyfikatów

odpowiada podmiot świadczący usługi certyfikacyjne, którym może być zgodnie z art. 3 pkt. 14 przedsiębiorca w rozumieniu przepisów prawa o działalności gospodarczej, Narodowy Bank Polski albo organ władzy publicznej. Podmiot ten musi zapewnić bezpieczeństwo i wiarygodność tych usług.

W myśl art. 6 ust. 1. wspomnianej ustawy bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny.

Nie można odnieść tej samej zasady do certyfikatu, którego termin ważności już upłynął.

Nie można tego stosować również od dnia unieważnienia certyfikatu oraz w okresie jego zawieszenia, chyba że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu lub przed jego unieważnieniem albo zawieszeniem.

Ponadto zastrzega się, iż nie można powoływać się, że podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.

Również nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego. Jego prawa są potwierdzone ustawowo.

Zastosowanie do danych medycznych. Wraz z rozwojem zdalnych usług medycznych, np. zdalnej diagnostyki czy zdalnej analizy rośnie znaczenie ochrony danych przesyłanych za pośrednictwem publicznych sieci teleinformatycznych. Usługa certyfikacji umożliwia bezpieczny i uwierzytelniony transfer informacji, oznaczanie czasem -ustalenie wiarygodnej chronologii napływających informacji; usługa archiwizacji - bezpieczne przechowywanie kart chorobowych pacjentów.

Zalety podpisu elektronicznego w stosunku do podpisu tradycyjnego:

- 1) możliwość natychmiastowej i obiektywnej identyfikacji podpisanej osoby,
- 2) sfalszowanie podpisu elektronicznego jest o wiele trudniejsze niż własnoręcznego,
- 3) podpis elektroniczny chroni całość dokumentu, nie ma potrzeby parafować każdej jego strony,
- 4) nie ma oryginału i jego kopii gdyż żaden dokument, który został opatrzony podpisem elektronicznym nie może już zostać zmieniony, jest więc oryginałem,
- 5) dane skierowane do danego odbiorcy mogą zostać zaszyfrowane, w taki sposób, że tylko odbiorca dla którego zostały przeznaczone może je rozszyfrować,
- 6) podpis elektroniczny jest powiązany z dokumentem, do którego został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana danych jest rozpoznawalna.

Podpis elektroniczny, zwłaszcza w swej bezpiecznej postaci, ma szereg cech, których nie posiada zwykły podpis. Jedną z nich jest to, że w przeciwieństwie do podpisu tradycyjnego, jego ważność i prawdziwość nie zależy od nośnika, a jedynie od danych służących do weryfikacji i zawartych w certyfikacie, co powoduje, że osoba, która utworzyła podpis może być zidentyfikowana w sposób natychmiastowy, automatyczny i obiektywny. Drugą, że pozwala stwierdzić integralność danych, do których się odnosi. Trzecią, że dzięki

nowoczesnym technikom opartym na współczesnej kryptografii, wdrożonym w bezpiecznych urządzeniach do tworzenia podpisu, podrobienie takiego podpisu jest o wiele trudniejsze niż podpisu własnoręcznego, a właściwie niemożliwe.