Ochrona danych pacjentów

OCHRONA DANYCH OSOBOWYCH JEST DLA LEKARZA SPRAWĄ SKOMPLIKOWANĄ. Najważniejszym krajowym aktem prawnym dotyczącym danych osobowych w placówce medycznej jest ustawa o ochronie danych osobowych (dalej u.o.d.o.). Przetwarzanie danych osobowych przez podmioty udzielające świadczeń zdrowotnych podlega regulacjom zawartym w tej ustawie. Na szczęście gabinety lekarskie nie musza zgłaszać baz danych pacjentów do GIODO.

autor:
Maciej Gibiński

Ą rolę odgrywa również ustawa o prawach pacjenta zeczniku Praw Pacjenta (wraz z właściwymi rozporzą-eniami resortowymi) – regulująca chociażby kwestie iązane z udostępnianiem i przechowywaniem doku-entacji medycznej.

ODPOWIEDZIALNOŚĆ Z TYTUŁU NIEPRZESTRZEGANIA PRZEPISÓW

rożeniem dla podmiotów leczniczych w związku liwym naruszeniem przepisów ustawy o ochronie danych osobowych jest nieodpowiednie zabezpieczenie prowadzonej dokumentacji medycznej pacjentów.

Ustawa o ochronie danych osobowych w art. 51 opisuje przestępstwo związane z naruszeniem zasad postępowania z danymi osobowymi: „Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Artykuł 51 ust. 2 u.o.d.o. natomiast brzmi: „Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku".

Sąd Najwyższy w swoim postanowieniu z dnia 21 listopada 2007 r., sygn. akt IV KK 376/07, stwierdził, że wobec obecnej treści przepisu art. 51 ust. 1 u.o.d.o. udostępnienie danych lub umożliwienie do nich dostępu jednej osobie nie wyczerpuje znamion omawianego przestępstwa.

Kolejnym zachowaniem, które jest karane przez ustawę o ochronie danych osobowych, jest przestępstwo przewidziane w art. 52 u.o.d.o., który stanowi, że kto administrując danymi, narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Zgodnie z wyrokiem Naczelnego Sądu Administracyjnego z dnia 7 maja 2008 r., sygn. akt I OSK 998/07, osoba, której dotyczą dane osobowe, nie powinna być w żaden sposób ograniczona w dostępie do tych danych i w dysponowaniu nimi. Jest to zatem uprawnienie podmiotu, którego dane osobowe są przetwarzane przez administratora danych osobowych. Z niego wynika także równoległe zwolnienie od odpowiedzialności administratora danych osobowych za niewłaściwe ich wykorzystywanie lub zabezpieczenie przez samego zainteresowanego. W związku z tym podmiot leczniczy udzielający świadczeń zdrowotnych, który zgodnie z obowiązującymi przepisami udostępnił pacjentowi jego dokumentację medyczną, nie ponosi odpowiedzialności za wykorzystanie tych danych przez samego pacjenta.

PODSTAWOWE POJĘCIA

Dane osobowe są to wszelkie informacje służące identyfikowaniu. Osoba możliwa do zidentyfikowania to taka, 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. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Doktryna prawnicza przyjmuje, że adres e-mail, umożliwiający identyfikację określonej osoby należy do danych osobowych i jako taki powinien być chroniony w zgodzie z przepisami.

Administrator danych osobowych to osoba fizyczna lub osoba prawna, bądź jednostka organizacyjna bez osobowości prawnej, która decyduje o celach i środkach wykorzystywania zgromadzonych danych osobowych. W przypadku, gdy administrator danych osobowych nie wykonuje funkcji administratora bezpieczeństwa infor-

macji, nadzorującego przestrzeganie zasad ochrony, musi powołać taką osobę wewnątrz placówki.

Administrator Bezpieczeństwa Informacji (ABI), powinien być wyznaczony przez Administratora Danych Osobowych, do którego należy sprawowanie nadzoru nad przestrzeganiem przepisów ustawy. Może nim być tylko osoba fizyczna, która: ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych, posiada odpowiednią wiedzę w zakresie ochrony danych osobowych i nie była karana za umyślne przestępstwo. ABI może powoływać swoich zastępców, którzy także powinni spełniać warunki wskazane w oświadczeniu.

Zbiór danych osobowych, którym w myśl ustawy jest „każdy zbiór posiadający strukturę danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie".

Cechą wyróżniającą zbiór danych od innego zestawu danych jest struktura, czyli uporządkowanie, które daje możliwość wyszukania konkretnych danych według określonego kryterium. Żeby jakikolwiek zestaw danych zaklasyfikować jako zbiór w rozumieniu przepisów ustawy o ochronie danych osobowych, wystarczające jest kryterium umożliwiające odnalezienie danych osobowych w zestawie. Możliwość wyszukania według jakiegokolwiek kryterium osobowego (np. imię, nazwisko, data urodzenia, PESEL) lub nieosobowego (np. data zamieszczenia danych w zbiorze) przesądza o uporządkowanym charakterze zestawu danych i tym samym umożliwia zakwalifikowanie tego zestawu jako zbioru danych osobowych. Tylko będący zbiorem danych osobowych usystematyzowany zestaw danych powinien być zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, o ile nie zachodzi żadna z przesłanek określonych w art. 43 ustawy o ochronie danych osobowych, zwalniająca administratorów danych z tego obowiązku.

Placówka medyczna, jako administrator danych, powinna dołożyć szczególnej staranności w celu ochrony interesów osób, których dane posiada, a w szczególności jest obowiązana zapewnić, aby dane te były: przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 u.d.u.).

DANE OSOBOWE W PLACÓWCE MEDYCZNEJ

Placówka medyczna posiada kilka rodzajów danych osobowych. Wśród najważniejszych należy wymienić:

FOT. CHROMA

Adres e-mail umożliwiający identyfikację określonej osoby należy do danych osobowych i jako taki powinien być chroniony w zgodzie z przepisami

Dane pracownicze zawierające imię, nazwisko, adres domowy, adres do korespondencji czy mailowy, dane o rodzinie, stanie cywilnym, liczbie dzieci i zarobkach.

Dane o współpracownikach (osobach fizycznych prowadzących własne działalności gospodarcze, które w myśl ustawy u.o.d.o. podlegają również ochronie prawnej.

DANE PACJENTÓW, ZAWARTE W DOKUMENTACJI MEDYCZNEJ.

Dokumentacja medyczna jest zbiorem danych opisujących stan zdrowia pacjenta oraz zakres udzielanych mu świadczeń. Ze względu na zawarte w niej informacje kwalifikuje się ją jako dane wrażliwe. W jej skład wchodzą wszelkiego rodzaju dokumenty zawierające informacje o: pacjencie, jego schorzeniu, udzielonych świadczeniach zdrowotnych, wykonywanych zabiegach diagnostycznych, leczniczych czy rehabilitacyjnych, zaleceniach, a także dokumenty w rodzaju: zaświadczenia, orzeczenia, opinie.

Zawiera ona dwa rodzaje danych osobowych: identyfikujące – związane z możliwością ustalenia tożsamości pacjenta i medyczne – dotyczące stanu zdrowia pacjenta, rodzajów przeprowadzonych zabiegów czy operacji oraz udzielonych świadczeń medycznych.

Co do zasady przetwarzania danych wrażliwych (za jakie uznaje się dokumentację medyczną) jest zabronione. Dopuszczalne jest jednak przetwarzanie danych wrażliwych

ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH

- Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania,
- Nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych oraz przestrzegania zasad określonych w dokumentacji (przez dokumentację rozumie się tworzenie polityki bezpieczeństwa przetwarzania danych osobowych, tworzenie instrukcji określającej sposób zarządzania i użytkowania systemów informatycznych),
- Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych. W związku z nowelizacją przepisów u.o.d.o. osoby, które aktualnie zajmują stanowisko ABI powinny zostać zgłoszone do rejestru ABI (prowadzonego przez GIODO) najpóźniej do dnia 30 czerwca 2015 roku. Do tego czasu firmy powinny wyodrębnić stanowisko ABI wewnątrz struktury organizacyjnej lub dopasować aktualny opis stanowiska osoby piastującej tę funkcję w taki sposób, aby uniezależnić ABI od dotychczasowych przełożonych, z jednoczesnym raportowaniem do kierownika danej jednostki,
- Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych.
- Przetwarzanie danych osobowych, przez które rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

w celu: ochrony stanu zdrowia, świadczenia usług medycznych, leczenia pacjentów.

Uprawnienie do przetwarzania danych wrażliwych zostało przyznane osobom wykonującym zawód medyczny oraz zajmującym się zarządzaniem udzielania usług medycznych.

ŚRODKI MAJĄCE NA CELU ZABEZPIECZENIE DANYCH OSOBOWYCH

Ustawa o ochronie danych osobowych nakłada na administratora danych osobowych obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności obowiązek zabezpieczenia danych przed ich: udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem, zniszczeniem.

Placówka medyczna jest zobowiązana do prowadzenia dokumentacji opisującej sposób przetwarzania danych.

W celu dookreślenia wymogów dotyczących zapewnienia odpowiedniego zaplecza technicznego oraz wyznaczenia zasad, jakim podlegać powinno administrowanie danymi osobowymi, wydane zostało 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 (dalej r.d.p.d.o.), Określa ono:

a) sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;

b) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

c) wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Wspomniane powyżej Rozporządzenie wprowadza trzy poziomy ochrony danych osobowych przetwarzanych w systemie informatycznym:

a) poziom podstawowy – dotyczy systemów informatycznych, w których nie przetwarza się tzw. danych osobowych wrażliwych oraz gdy żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną;

b) poziom podwyższony – dotyczy systemu informatycznego, w którym przetwarzane są tzw. dane wrażliwe, a żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną;

c) poziom wysoki – dotyczy systemu informatycznego, w którym przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.

Pod pojęciem sieci publicznej, przyjmuje się: sieć telekomunikacyjną, w której przeważająca część usług jest wykorzystywana przez użytkowników, którzy nie pozostają z dostawcą tychże usług w żadnym

ŚRODKI BEZPIECZEŃSTWA NA POZIOMIE PODSTAWOWYM

Środki bezpieczeństwa na poziomie podstawowym zgodnie z załącznikiem do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych obejmują:

- zabezpieczenie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych;

- zapewnienie, aby przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, odbywało się wyłącznie za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych;

- stosowanie w systemie informatycznym, służącym do przetwarzania danych osobowych, mechanizmów kontroli dostępu do tych danych; jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas należy zapewnić, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator, a dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia;

- stosowanie haseł zmienianych nie rzadziej niż co 30 dni i składających się co najmniej z sześciu znaków;

- zakaz przydzielania innej osobie identyfikatora użytkownika, który utracił uprawnienia do przetwarzania danych;

- zabezpieczenie systemu informatycznego służącego do przetwarzania danych osobowych w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;

- wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych; kopie zapasowe powinny być przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, a także usuwane niezwłocznie po ustaniu ich użyteczności;

- zachowywanie szczególnej ostrożności przez osoby użytkujące komputer przenośny zawierający dane osobowe podczas transportu, przechowywania i użytkowania komputera poza obszarem, w którym przetwarzane są dane osobowe; w szczególności nakaz zachowania szczególnej ostrożności obejmuje stosowanie kryptograficznych środków ochrony przetwarzanych danych osobowych;

- obowiązek pozbawiania urządzeń, dysków lub innych elektronicznych nośników informacji zawierających dane osobowe i przeznaczonych do likwidacji zapisu danych; jeżeli jest to możliwe, nośniki uszkadza się w sposób uniemożliwiający ich odczytanie;

- obowiązek pozbawiania urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe i przekazywanych podmiotowi nieuprawnionemu do przetwarzania danych zapisu danych w sposób uniemożliwiający ich odzyskanie;

- obowiązek pozbawiania urządzeń, dysków lub innych elektronicznych nośników informacji zawierających dane osobowe i przekazywanych do naprawy zapisu danych w sposób uniemożliwiający ich odzyskanie albo obowiązek nadzoru administratora danych w procesie ich naprawiania.

dodatkowym stosunku prawnym poza stosunkiem związanym ze świadczeniem usług.

Administrator danych, lub działając w jego imieniu ABI, ma obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz stosowane przez niego środki ich zabezpieczenia. Szczegółowe wymagania określa Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (dalej r.d.p.d.o.). Dokumentacja ochrony danych osobowych składa się z polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

POLITYKA BEZPIECZEŃSTWA

W przypadku gdy placówka medyczna posiada jedynie dokumentację w formie papierowej, administrator danych osobowych zobowiązany będzie do opracowania polityki bezpieczeństwa. Obowiązek opracowania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych odnosi się do placówek medycznych, które przetwarzają dane osobowe za pomocą systemów informatycznych (np. poprzez prowadzenie elektronicznego terminarza, odbierania maili itp.). Dokumentacja ochrony danych osobowych, zgodnie z przepisami, prowadzona jest w formie pisemnej. Administrator danych ma obowiązek opracować a następnie pisemnie wdrożyć dokumenty, o których mowa powyżej (politykę bezpieczeństwa oraz instrukcję przetwarzania danych osobowych). Zadaniem administratora danych jest również aktualizowanie ww. dokumentów.

Wymogi te mają na celu pomóc administratorowi danych w określeniu poprawnej dokumentacji ochrony danych osobowych. Elementy wskazane powyżej muszą być zawarte w dokumentacji, jednak administrator może dodać inne elementy określające procedury zabezpieczenia danych, dopasowując je do prowadzonej przez siebie działalności.

OBOWIĄZKI ADMINISTRATORA DANYCH

Poza wskazanymi dokumentami administrator jest zobowiązany stworzyć i prowadzić dwa dokumenty związane z ochroną danych osobowych: ewidencję osób upoważnionych do przetwarzania danych

ŚRODKI BEZPIECZEŃSTWA NA POZIOMIE PODWYŻSZONYM

Środki bezpieczeństwa na poziomie podwyższonym obejmują – oprócz środków bezpieczeństwa stosowanych na poziomie podstawowym – dodatkowo:

- obowiązek stosowania haseł do uwierzytelniania użytkowników, składających się co najmniej z ośmiu znaków i zawierających małe i wielkie litery oraz cyfry lub znaki specjalne;
- obowiązek zabezpieczania urządzeń i nośników zawierających tzw. dane osobowe wrażliwe w sposób zapewniający poufność i integralność tych danych w sytuacji ich przekazywania poza obszar, w którym przetwarzane są dane osobowe.

Na poziomie wysokim – oprócz środków bezpieczeństwa stosowanych na poziomie podstawowym i podwyższonym przepisy przewidują dodatkowo, aby:

- system informatyczny służący do przetwarzania danych osobowych był chroniony przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;
- stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Zgodnie z § 4 r.d.p.d.o. powinna zawierać:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
- opis struktury zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
- informacje na temat sposobu przepływu danych pomiędzy poszczególnymi systemami;
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z § 5 r.d.p.d.o. powinna określać:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
- stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- sposób odnotowywania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia;
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO ICH PRZETWARZANIA

Ewidencja osób upoważnionych do ich przetwarzania 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.

Informacja dla osób, których dane osobowe są przetwarzane, zawiera:

- adres siedziby i pełną nazwę, a w przypadku gdy administratorem danych jest osoba fizyczna - miejsce jej zamieszkania oraz imię i nazwisko,
- cel zbierania danych,
- prawo dostępu do treści swoich danych oraz ich poprawiania,
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

osobowych i informację dla osób, których dane są przetwarzane w placówce medycznej.

Dodatkowo administrator danych jest także obowiązany do regularnego przeprowadzania szkoleń oraz zapewnienia kontroli nad procesem przetwarzania danych osobowych.

ZGŁOSZENIE ZBIORÓW DANYCH DO REJESTRU GIODO

Obecnie zbiory danych obejmujące dokumentację medyczną nie podlegają obowiązkowi zgłoszenia Generalnemu Inspektorowi Ochrony Danych Osobowych. Zamiast tego, to ABI w spółce będzie zobowiązany prowadzić taki rejestr, stosownie go opisując.

Rejestr zbiorów danych osobowych powinien zawierać co najmniej: oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku powierzenia przetwarzania danych podmiotowi (umowa o powierzeniu danych osobowych) – oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania; cel przetwarzania danych; opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych; sposób zbierania oraz udostępniania danych; informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane; opis środków technicznych i organizacyjnych zastosowanych w celach zabezpieczania danych osobowych; informację o sposobie wypełnienia warunków technicznych i organizacyjnych, wprowadzonych celem zabezpieczenia danych osobowych; informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Jako przykładowe zbiory danych osobowych, tworzone przez ABI można wskazać:

a) rejestr skarg i wniosków,

b) listę osób upoważnionych do wglądu w dokumentację medyczną,

c) listę osób upoważnionych do odbioru dokumentacji medycznej.

Przed nowelizacją przepisów w roku 2014 brak zgłoszenia zbiorów danych oznaczał, że nie wolno z nich korzystać w placówce medycznej. Obecnie wydaje się, że brak stworzenia odpowiedniego rejestru dla zbioru danych osobowych, również może oznaczać bezprawne jego tworzenie i korzystanie.

ZESTAWIENIE PRZYGOTOWAŁ
MACIEJ GIBIŃSKI, DOKTOR PRAWA

Ukończył studia magisterskie na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego na kierunku Prawo oraz Studia doktoranckie na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego. Jest znanym i cenionym mówcą na wielu konferencjach z zakresu prawa medycznego oraz autorem wielu publikacji i i książek z zakresu prawa medycznego. Od 2009 roku prowadzi firmę Centrum Doradcze Prawa Medycznego.