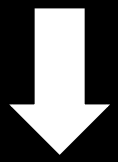
NASZE OBOWIĄZKI I UPRAWNIENIA

LexDENTAL

PRZETWARZANIE DANYCH OSOBOWYCH?



Art. 7 ust. 2 ustawy o ochronie danych osobowych:

przetwarzanie danych osobowych to wykonywanie jakichkolwiek operacji na danych osobowych, takich jak np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w sytemach informatycznych.

USTAWA
z dnia 29 sierpnia 1997 r.
o ochronie danych osobowych.

(tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926)

Art. 6. 1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

2. 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.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

KWESTIONARIUSZ OSOBOWY
KARTA PACJENTA

DANE OSOBOWE

IMIĘ I NAZWISKO _____ PESEL _____

DATA URODZENIA _____ EMAIL _____

TELEFON KOMÓRKOWY _____ TELEFON STACJONARNY _____

ADRES ZAMIESZKANIA _____

LexDENTAL

HISTORIA ZDROWIA I CHOROBY
Poradni Stomatologicznej

Nr karty .....

Data rej. .....

Dokument uprawn. do świadczeń ..... O/NFZ .....

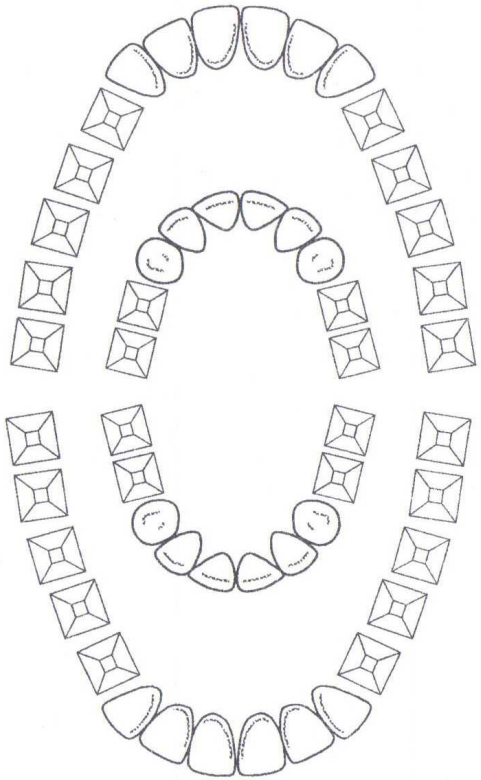
pieczątka poradni

M
Ż

Nazwisko ..... imię .....

Adres .....

Data urodz. ..... PESEL



Stan jamy ustnej

Błona śluzowa .....

.....

Przyzębie .....

.....

Higiena .....

Informacje uzupełniające (dot. stanu szkliwa, zaburzeń ortodont. i inne)

.....

Podczas leczenia na diagramie nie dokonywać żadnych zmian. Jeżeli pacjent zgłasza się po przerwie i stwierdzono nowe ubytki, wypełnić nowy diagram zębowy.

Wizyta z dnia: 11-07-2014 12:01 /
Stomatologia zachowawcza

Pacjent:
PESEL:
Pacjenta
Data wy

Rozpoznanie

z.16 Przewlekłe zapalenie tkanek okołowierzchołowych;
odczyn zapalny w zatoce szczękowej prawej

Opis wizyty

Pacjentka odbyła konsultację laryngologiczną,która wykazała stan zap.zatoki szczękowej prawej w obrębie dna zatoki bez zniszczenia struktur kostnych;brak przeciwskazan do wyk.zabiegu chirurgicznego czy lecz .kanałowego.
Ze wzgl na planowane lecz.ortodontyczne ustalono:
-ekstrakcję z.16 i 36 /ew lecz endodontyczne,
-pozostawienie z.26 jako prawidłowo przeleczonego endodontycznie

Tabela procedur

Ząb	Procedura	Materiały / Leki	Rozpoznanie
obszar szczęki	Znieczulenie komputerowe TheWand/ computer local anasthesia The Wand		
25	Wypełnienie duże / aesthetic, composite filling (large)		
24	Wypełnienie duże / aesthetic, composite filling (large)		
28	Wypełnienie małe / aesthetic, composite fillin (small)		
27	Wypełnienie duże / aesthetic, composite filling (large)		

Przepisane leki

Nie przepisano żadnych leków

Zalecenia

Nie zanotowano żadnych uwag

CZY MUSIMY UZYSKIWAĆ OD PACJENTA ZGODĘ NA PRZETWARZANIE JEGO DANYCH OSOBOWYCH?

PODSTAWY PRAWNE

Art. 23 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta
1.Pacjent ma prawo do dostępu do dokumentacji medycznej
dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych.

Art. 24
1.W celu realizacji prawa, o którym mowa w art. 23 ust. 1, podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w niniejszym rozdziale oraz zapewnić ochronę danych zawartych w tej dokumentacji.
2. **Lekarze, pielęgniarki i położne są uprawnieni do uzyskiwania i przetwarzania danych zawartych w dokumentacji medycznej, o których mowa w art. 25.**

Art. 41 Ustawy o zawodach lekarza i lekarza dentysty
Lekarz ma **obowiązek** prowadzenia indywidualnej dokumentacji medycznej pacjenta.

USTAWA
z dnia 6 listopada 2008 r.

o prawach pacjenta i Rzeczniku Praw Pacjenta

Art. 25.

Dokumentacja medyczna zawiera co najmniej:

1) oznaczenie pacjenta, pozwalające na ustalenie jego tożsamości:
   a) nazwisko i imię (imiona),
   b) datę urodzenia,
   c) oznaczenie płci,
   d) adres miejsca zamieszkania,
   e) numer PESEL, jeżeli został nadany, w przypadku noworodka – numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość,
   f) w przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody – nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania;
2) oznaczenie podmiotu udzielającego świadczeń zdrowotnych ze wskazaniem komórki organizacyjnej, w której udzielono świadczeń zdrowotnych;
3) opis stanu zdrowia pacjenta lub udzielonych mu świadczeń zdrowotnych;
4) datę sporządzenia.

Zbiór danych osobowych gromadzony w ramach dokumentacji medycznej:

- ✓**nie podlega zgłoszeniu** **do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych**
- ✓**nie mamy obowiązku uzyskiwania zgody pacjenta** **na przetwarzanie danych osobowych zawartych w dokumentacji medycznej w celach świadczenia usług medycznych.**

KWESTIONARIUSZ OSOBOWY
KARTA PACJENTA

DANE OSOBOWE

IMIĘ I NAZWISKO _____ PESEL _____

DATA URODZENIA _____ EMAIL _____

TELEFON KOMÓRKOWY _____ TELEFON STACJONARNY _____

ADRES ZAMIESZKANIA _____

LexDENTAL

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 09.10.2013 r.

Organ I instancji wywiódł, iż nazwisko i imię osoby zgłaszającej stanowią dane osobowe, gdyż wprost identyfikują osobę fizyczną, natomiast **numer telefonu otwiera możliwość ustalenia tożsamości osoby fizycznej**, a więc jest również **informacją zawierającą dane osobowe.**

USTAWA
z dnia 6 listopada 2008 r.

o prawach pacjenta i Rzeczniku Praw Pacjenta

Art. 25.

Dokumentacja medyczna zawiera co najmniej:

1) oznaczenie pacjenta, pozwalające na ustalenie jego tożsamości:
   a) nazwisko i imię (imiona),
   b) datę urodzenia,
   c) oznaczenie płci,
   d) adres miejsca zamieszkania,
   e) numer PESEL, jeżeli został nadany, w przypadku noworodka – numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość,
   f) w przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody – nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania;
2) oznaczenie podmiotu udzielającego świadczeń zdrowotnych ze wskazaniem komórki organizacyjnej, w której udzielono świadczeń zdrowotnych;
3) opis stanu zdrowia pacjenta lub udzielonych mu świadczeń zdrowotnych;
4) datę sporządzenia.

Katalog art. 25 nie obejmuje takich danych, jak **numer telefonu czy adres e-mail**, które najczęściej uzyskujemy dodatkowo od pacjentów, czy to w celu potwierdzenia wizyty czy informacji o aktualnych promocjach, akcjach profilaktycznych.

USTAWA
z dnia 29 sierpnia 1997 r.
o ochronie danych osobowych.

(tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926)

Artykuł 23

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
   1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych,
   2) zezwalają na to przepisy prawa,
   3) (7) jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia koniecznych działań przed zawarciem umowy,
   4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
   5) (8) jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych, o których mowa w art. 3 ust. 2, lub osób trzecich, którym są przekazywane te dane - a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

Artykuł 24

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:
   1) adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
   2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
   3) prawie wglądu do swoich danych oraz ich poprawiania,
   4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Zgodnie z art. 23 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r.Nr 101, poz. 926, z późn. zm.) wyrażam zgodę na przetwarzanie w/w danych osobowych przez XYZ z siedzibą w ..... w celu komunikacji z osobami korzystającymi z usług medycznych oraz na otrzymywanie za pośrednictwem telefonii komórkowej i poczty elektronicznej informacji dot. planowanych wizyt, jak również informacji o medycznej działalności XYZ.

Jednocześnie oświadczam, że zgodnie z art.24 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, ze zm.) zostałem poinformowany/a o tym, że dane zbierane są przez XYZ z siedzibą w ....., o celu zbierania danych, dobrowolności ich podania, prawie wglądu do tych danych i wnoszenia poprawek oraz o tym, że dane te nie będą udostępniane innym podmiotom.

Miejscowość i data

Czytelny podpis pacjenta

Art. 40 Ustawy o ochronie danych osobowych
Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 wyłączenia obowiązku rejestracji zbioru danych ust. 1 i 1a.


e-GIODO
E-giodo
Rejestr Zbiorów Danych Osobowych
Rejestr Administratorów Bezpieczeństwa Informacji
Serwis e-GIODO wykorzystuje sesyjne pliki Cookies. Dowiedz się więcej
Rejestr Zbiorów Danych Osobowych
Aplikacja Rejestr Zbiorów Danych Osobowych udostępnia narzędzia wspomagające administratorów danych osobowych w przygotowaniu i wysyłaniu zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Danych Osobowych.
Aplikacja ta zawiera również funkcje umożliwiające użytkownikom dostęp do prowadzonego przez GIODO ogólnokrajowego jawnego rejestru zbiorów danych osobowych, o których mowa w art. 42 ust.1 ustawy o ochronie danych osobowych.
W celu skorzystania z aplikacji należy wybrać z menu pozycję Rejestr Zbiorów Danych Osobowych.
Rejestr Administratorów Bezpieczeństwa Informacji
Aplikacja Rejestr Administratorów Bezpieczeństwa Informacji umożliwia użytkownikom publiczny dostęp do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO) ogólnokrajowego, jawnego rejestru administratorów bezpieczeństwa informacji, o których mowa w art 46c ustawy o ochronie danych osobowych.
W celu skorzystania z aplikacji należy wybrać z menu pozycję Rejestr Administratorów Bezpieczeństwa Informacji (Rejestr ABI)
Uwaga! W obecnej wersji aplikacji Rejestru ABI brak jest funkcjonalności umożliwiającej wypełnianie wniosków o powołanie lub odwołanie administratorów bezpieczeństwa informacji.
UNIA EUROPEJSKA
Projekt współfinansowany przez
Europejski Fundusz Rozwoju Regionalnego
UNIA DLA PRZEDSIĘBIORCZYCH
PROGRAM KONKURENCYJNOŚĆ
Polityka prywatności
Copyright by GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH 2006
Kancelaria@giodo.gov.pl

Czy podmioty udzielające świadczeń zdrowotnych mają **obowiązek rejestracji zbiorów danych osobowych** swoich pacjentów u Generalnego Inspektora Ochrony Danych Osobowych?

Art. 40 Ustawy o ochronie danych osobowych
Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, **z wyjątkiem przypadków**, o których mowa w art. 43 wyłączenia obowiązku rejestracji zbioru danych ust. 1 i 1a.

Art. 43 ust. 1 pkt 5 Ustawy o ochronie danych osobowych

Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych dotyczących osób korzystających z ich usług medycznych (...).

ALE

Każdy lekarz dentysta prowadzący praktykę lekarską, mimo, że nie jest zobowiązany do zgłaszania Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych osobowych pacjentów oraz ewentualnie zatrudnionych pracowników pracowników, **powinien stosować w swojej działalności przepisy ustawy o ochronie danych osobowych.**

Lekarz dentysta jako administrator danych osobowych zobowiązany jest do:

✧ opracowania i wdrożenia dokumentu **polityka bezpieczeństwa,**
✧ opracowania i wdrożenia dokumentu **instrukcja zarządzenia systemem informatycznym**, (w przypadku prowadzenia zbioru danych w systemie informatycznym),
✧ wyznaczenia administratora bezpieczeństwa informacji (fakultatywnie),
✧ dopuszczenia do przetwarzania danych wyłącznie **osoby posiadające upoważnienia,**
✧ prowadzenia **ewidencji osób upoważnionych** do przetwarzania danych.

Lekarz dentysta jako administrator danych osobowych zobowiązany jest do:

✧ opracowania i wdrożenia dokumentu **polityka bezpieczeństwa,**
✧ opracowania i wdrożenia dokumentu **instrukcja zarządzenia systemem informatycznym**, (w przypadku prowadzenia zbioru danych w systemie informatycznym),
✧ **wyznaczenia administratora bezpieczeństwa informacji (fakultatywnie),**
✧ dopuszczenia do przetwarzania danych wyłącznie **osoby posiadające upoważnienia,**
✧ prowadzenia **ewidencji osób upoważnionych** do przetwarzania danych.

Czy powołanie ABI należy zgłosić do rejestracji GIODO?


e-GIODO
E-giodo
Rejestr Zbiorów Danych Osobowych
Rejestr Administratorów Bezpieczeństwa Informacji
Serwis e-GIODO wykorzystuje sesyjne pliki Cookies. Dowiedz się więcej
Rejestr Zbiorów Danych Osobowych
Aplikacja Rejestr Zbiorów Danych Osobowych udostępnia narzędzia wspomagające administratorów danych osobowych w przygotowaniu i wysyłaniu zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Danych Osobowych.
Aplikacja ta zawiera również funkcje umożliwiające użytkownikom dostęp do prowadzonego przez GIODO ogólnokrajowego jawnego rejestru zbiorów danych osobowych, o których mowa w art. 42 ust.1 ustawy o ochronie danych osobowych.
W celu skorzystania z aplikacji należy wybrać z menu pozycję Rejestr Zbiorów Danych Osobowych.
Rejestr Administratorów Bezpieczeństwa Informacji
Aplikacja Rejestr Administratorów Bezpieczeństwa Informacji umożliwia użytkownikom publiczny dostęp do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO) ogólnokrajowego, jawnego rejestru administratorów bezpieczeństwa informacji, o których mowa w art 46c ustawy o ochronie danych osobowych.
W celu skorzystania z aplikacji należy wybrać z menu pozycję Rejestr Administratorów Bezpieczeństwa Informacji (Rejestr ABI)
Uwaga! W obecnej wersji aplikacji Rejestru ABI brak jest funkcjonalności umożliwiającej wypełnianie wniosków o powołanie lub odwołanie administratorów bezpieczeństwa informacji.
UNIA EUROPEJSKA
Projekt współfinansowany przez
Europejski Fundusz Rozwoju Regionalnego
UNIA DLA PRZEDSIĘBIORCZYCH
PROGRAM KONKURENCYJNOŚĆ
Polityka prywatności
Copyright by GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH 2006
Kancelaria@giodo.gov.pl

Jeżeli administrator danych skorzysta z przysługującego mu uprawnienia i powoła administratora bezpieczeństwa informacji, zgodnie z art. 46b ust. 1 u.o.d.o., **ma 30 dni od dnia powołania ABI na zgłoszenie ABI do rejestracji Generalnemu Inspektorowi.**

Administrator danych, który zgłosi ABI do rejestracji, **zobowiązany jest zgłaszać Generalnemu Inspektorowi każdą zmianę informacji objętych zgłoszeniem powołania ABI** w terminie 14 dni, a także jego odwołanie w terminie 30 dni, odpowiednio od dnia dokonania zmiany lub odwołania.

Lekarz dentysta jako administrator danych osobowych zobowiązany jest do:

✧ opracowania i wdrożenia dokumentu **polityka bezpieczeństwa,**
✧ opracowania i wdrożenia dokumentu **instrukcja zarządzenia systemem informatycznym**, (w przypadku prowadzenia zbioru danych w systemie informatycznym),
✧ dopuszczenia do przetwarzania danych wyłącznie **osoby posiadające upoważnienia,**
✧ prowadzenia **ewidencji osób upoważnionych** do przetwarzania danych.

http://www.dilnet.wroc.pl/pliki/prawo_lex/ochrona_danych.pdf

Polityka bezpieczeństwa powinna zawierać w szczególności :

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

Wykaz zbiorów danych przetwarzanych w praktyce lekarskiej/dentystycznej w

……

lp.	Nazwa zbioru danych (1)	Forma danych/Baza danych (2)	Zabezpieczenie informatyczne (3)	Nazwa programu służącego do przetwarzania danych osobowych	Lokalizacja/nr pokoju	Zabezpieczenia inne niż informatyczne. (4)
1						
2						
3						

Opis:
(1) nazwa zwyczajowa lub własna
(2) Windows, SQL, dokumenty papierowe
(3) np.: indywidualne hasło dostępu, wydzielona fizycznie sieć
(4) np.: kraty w oknach, alarm, drzwi antywłamaniowe, kontrola dostępu, ochrona całodobowa.

Zbiorami danych osobowych, które podlegają obowiązkowi zgłoszenia do rejestru GIODO przez podmioty wykonujące działalność leczniczą (gdy nie został powołany ABI) to m. in.:

- zbiory danych dotyczące ewidencjonowania korespondencji;
- zbiór osób upoważnionych przez pacjentów do uzyskiwania informacji i dokumentacji medycznej;
- księga skarg i wniosków;
- zbiory monitoringu wizyjnego.

UWAGA

Metadane

30 CZERWCA 2015 R. TO TERMIN ZGŁOSZENIA **DO REJESTRACJI ABI**, A NIE ZBIORÓW DANYCH.

GIODO NIE NAKŁADA KAR ZA NIEZGŁOSZENIE ZBIORU DO REJESTRACJI.

W związku z pojawiającymi się w sieci błędnymi informacjami o konieczności zgłoszenia - do 30 czerwca 2015 r. - zbiorów danych osobowych do rejestracji GIDOO i groźbie nałożenia kary do 200 tys. zł za niedotrzymanie tego terminu, GIODO raz jeszcze informuje:

:: 30 czerwca 2015 r. to ostateczny termin na zgłoszenie do rejestracji GIODO dotychczasowych administratorów bezpieczeństwa informacji (ABI), o ile administrator danych zdecyduje, by dalej pełnili oni tę funkcję,

:: jeśli administrator danych powoła ABI i zgłosi go do rejestracji GIODO, zwolniony będzie z obowiązku rejestracji zbiorów danych u Generalnego Inspektora (z wyjątkiem zbiorów zawierających dane szczególnie chronione).

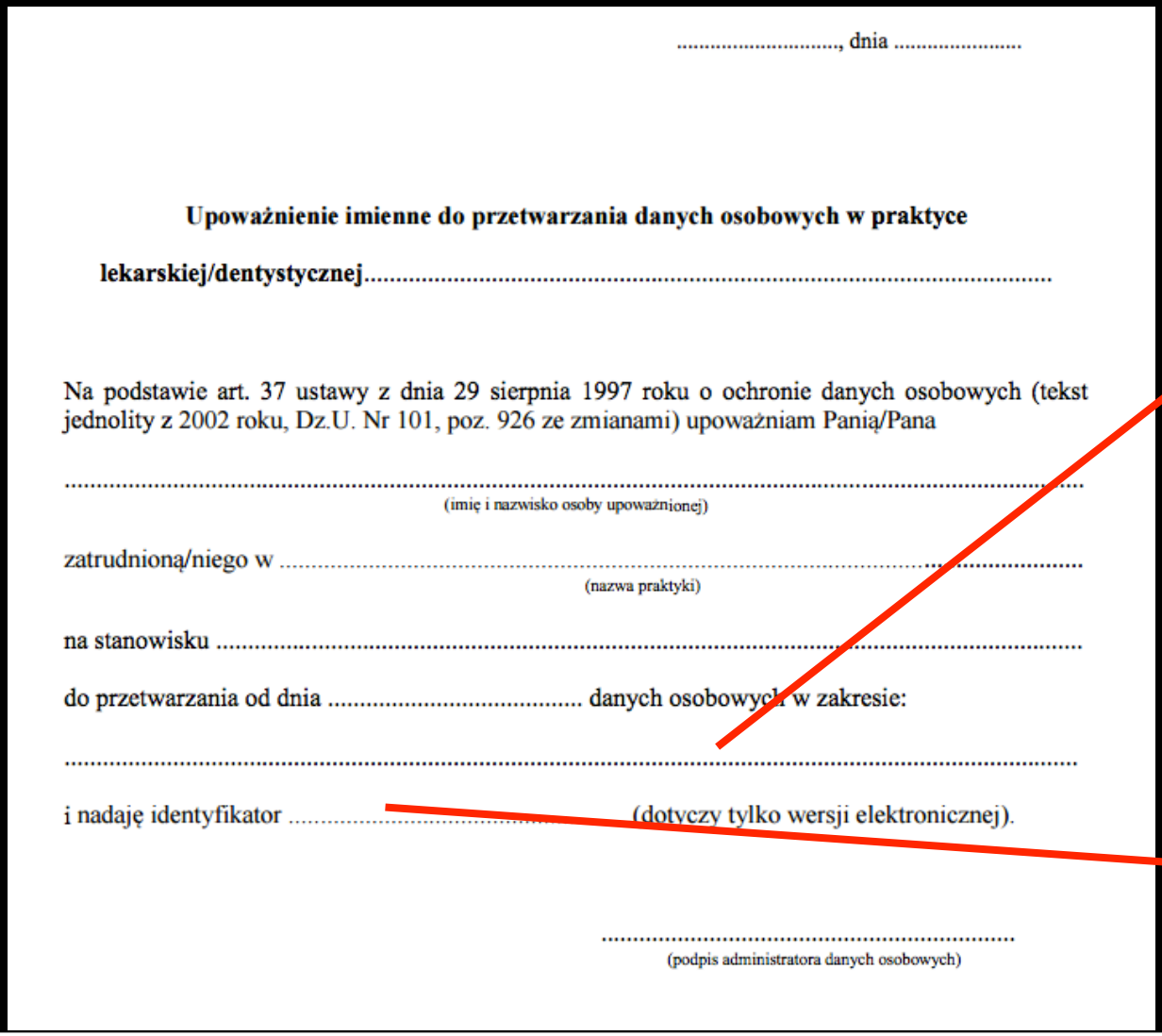
Więcej szczegółowych wyjaśnień na temat zmian, jakie od 1 stycznia 2015 r. zostały wprowadzone do ustawy o ochronie danych osobowych, jest dostępnych pod linkiem http://www.giodo.gov.pl/1520223/j/pl/.

Ponadto należy przypomnieć, że żaden przepis **nie uprawnia GIODO do nakładania kar finansowych, w tym za niezgłoszenie zbioru danych osobowych do rejestracji. Z**a niedopełnienie tego obowiązku przewidziana jest odpowiedzialność karna,jednak o rodzaju kary decyduje sąd. Nawet jeśli byłaby nią kara grzywny, to nakłada ją sąd, i to on określa jej wysokość. GIODO może nałożyć jedynie grzywnę, ale tylko w celu przymuszenia, w przypadku niewykonania wydanej przez niego decyzji.

Lekarz dentysta jako administrator danych osobowych zobowiązany jest do:

✧ opracowania i wdrożenia dokumentu **polityka bezpieczeństwa,**
✧ opracowania i wdrożenia dokumentu **instrukcja zarządzenia systemem informatycznym**, (w przypadku prowadzenia zbioru danych w systemie informatycznym),
✧ dopuszczenia do przetwarzania danych wyłącznie **osoby posiadające upoważnienia,**
✧ prowadzenia **ewidencji osób upoważnionych** do przetwarzania danych.

Art. 37. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.



....., dnia .....

Upoważnienie imienne do przetwarzania danych osobowych w praktyce

lekarskiej/dentystycznej.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity z 2002 roku, Dz.U. Nr 101, poz. 926 ze zmianami) upoważniam Panią/Pana

.....
(imię i nazwisko osoby upoważnionej)

zatrudnioną/niego w .....
(nazwa praktyki)

na stanowisku .....

do przetwarzania od dnia ..... danych osobowych w zakresie:

.....

i nadaję identyfikator ..... (dotyczy tylko wersji elektronicznej).

.....
(podpis administratora danych osobowych)

- ✓ ODCZYT
- ✓ ZAPIS
- ✓ MODYFIKACJA

- DOKUMENTACJA MEDYCZNA
- KSIĘGA PRZYJĘĆ
- ZDJĘCIA RTG

ANNA KOWALSKA

LexDENTAL

ZAŁ. B DO ROZPORZĄDZENIA MSWIA Z 29.04.2004:

W przypadku gdy do uwierzytelniania użytkowników używa się HASŁA, **składa się ono co najmniej z 8 znaków,** zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

ZAŁ.A DO ROZPORZĄDZENIA MSWIA Z 29.04.2004:

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego **zmiana następuje nie rzadziej niż co 30 dni. (*)**

Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;

b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

*

W przyjętym niedawno ogólnym rozporządzeniu Unii Europejskiej o ochronie danych osobowych, które będzie obowiązywało od 25 maja 2018 r., **nie ma już postanowień o szczegółowych rozwiązaniach i środkach bezpieczeństwa w celu ochrony danych.**

Przepis dotyczący zmiany hasła nie rzadziej niż co 30 dni będzie uchylony. To administrator danych sam zdecyduje, jak zadbać o poufność i integralność danych i po wcześniejszej analizie ryzyka określi politykę haseł.

Art. 39. 1. Administrator danych prowadzi **ewidencję osób upoważnionych do ich przetwarzania**, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej; 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych; 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Wzór Ewidencji osób upoważnionych do przetwarzania danych osobowych w praktyce

lekarskiej/dentystycznej .....

lp.	Imię i nazwisko użytkownika	Identyfikator użytkownika (dotyczy wersji elektronicznej)	Zakres uprawnień	Data nadania uprawnień	Data odebrania uprawnień	Przyczyna odebrania uprawnień	Podpis administratora danych lub ABI
1							
2							
3							

KARTA ZLECEŃ

Gabinet .....

Lekarz .....

Pacjent .....

PESEL ☐☐☐☐☐☐☐☐☐☐☐

Płeć K ☐ M ☐

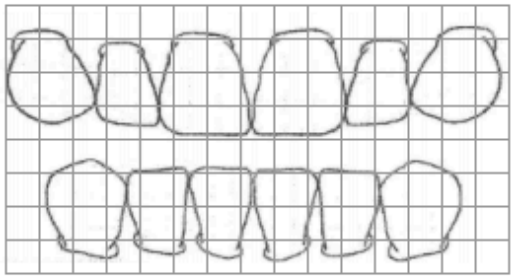
Fason zębów przednich

□ ▯ △ ○

PROJEKT PRACY

18	17	16	15	14	13	12	11	21	22	23	24	25	26	27	28
48	47	46	45	44	43	42	41	31	32	33	34	35	36	37	38

korony – O mosty – XXX



kolor bazowy ☐

Indywidualna charakteryzacja

- ☐ Mamelony
- ☐ Pęknięcia szkliwa
- ☐ Odwapnienia
- ☐ Pigmentacja bruzd

Podbudowa korony/mostu

- ☐ Stal bezniklowa
- ☐ ZrO_2
- ☐ Złoto

Stopień

- ☐ Metalowy
- ☐ Porcelanowy (Margin)

UWAGI	Termin wykonania	
	Data	Godzina

ZLECENIE WYKONANIA WYROBU NA ZAMÓWIENIE

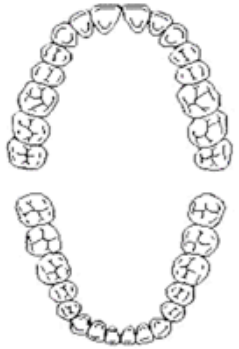
Wytwórca :	Data przyjęcia*:	Zlecający:
.....	.....	.....
.....		.....
.....	Numer*:	.....
.....	.....	Tel. .....

Nazwisko Pacjenta	Kod lub akronim	Wiek:	Płeć:	Wycisk z dnia
.....			K M	
.....				.....

Nazwa wyrobu:

.....

Zalecenia:



.....

.....

.....

Właściwości:

8 7 6 5 4 3 2 1	1 2 3 4 5 6 7 8
8 7 6 5 4 3 2 1	1 2 3 4 5 6 7 8

R L

Kolor:

Data:	Godzina:	Etap:	Akceptuję poprawność wykonania etapu. Podpis:

Termin wykonania :

Podpis Zlecającego (pieczęć):

UMOWA POWIERZENIA DANYCH

Art. 31.

1. Administrator danych może powierzyć innemu podmiotowi, **w drodze umowy zawartej na piśmie, przetwarzanie danych.**
2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.
3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.
4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

(*dane podmiotu który umowę zawiera, w szczególności: firma spółki, siedziba, adres, oznaczenie sądu rejestrowego, w którym przechowywana jest dokumentacja spółki oraz numer pod którym spółka jest wpisana do rejestru; NIP, wysokość kapitału zakładowego i kapitału wpłaconego – art. 206 lub 374 ksh. W przypadku podmiotów prowadzących działalność gospodarczą imię nazwisko adres zamieszkania osoby fizyczne, PESEL, firma pod jaką działalność jest prowadzona oraz adres głównego miejsca wykonywania działalności*).

zwana w dalszej części umowy „*Wykonawcą*"

reprezentowana przez:

_____

oraz

(*dane podmiotu który umowę zawiera, w szczególności: firma spółki, siedziba, adres, oznaczenie sądu rejestrowego, w którym przechowywana jest dokumentacja spółki oraz numer pod którym spółka jest wpisana do rejestru; NIP, wysokość kapitału zakładowego i kapitału wpłaconego – art. 206 lub 374 ksh. W przypadku podmiotów prowadzących działalność gospodarczą imię nazwisko adres zamieszkania osoby fizyczne, PESEL, firma pod jaką działalność jest prowadzona oraz adres głównego miejsca wykonywania działalności*)

zwana w dalszej części umowy „*Zleceniodawcą*"

reprezentowana przez:

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 07.06.2013 r.

Przechowywanie próbek DNA klientów Spółki jest przetwarzaniem danych osobowych, dlatego **w tym zakresie powinna być zawarta umowa powierzenia** przetwarzania danych osobowych, spełniająca wymogi określone w art. 31 ustawy.

CZYSTE BIURKO I CZYSTY EKRAN

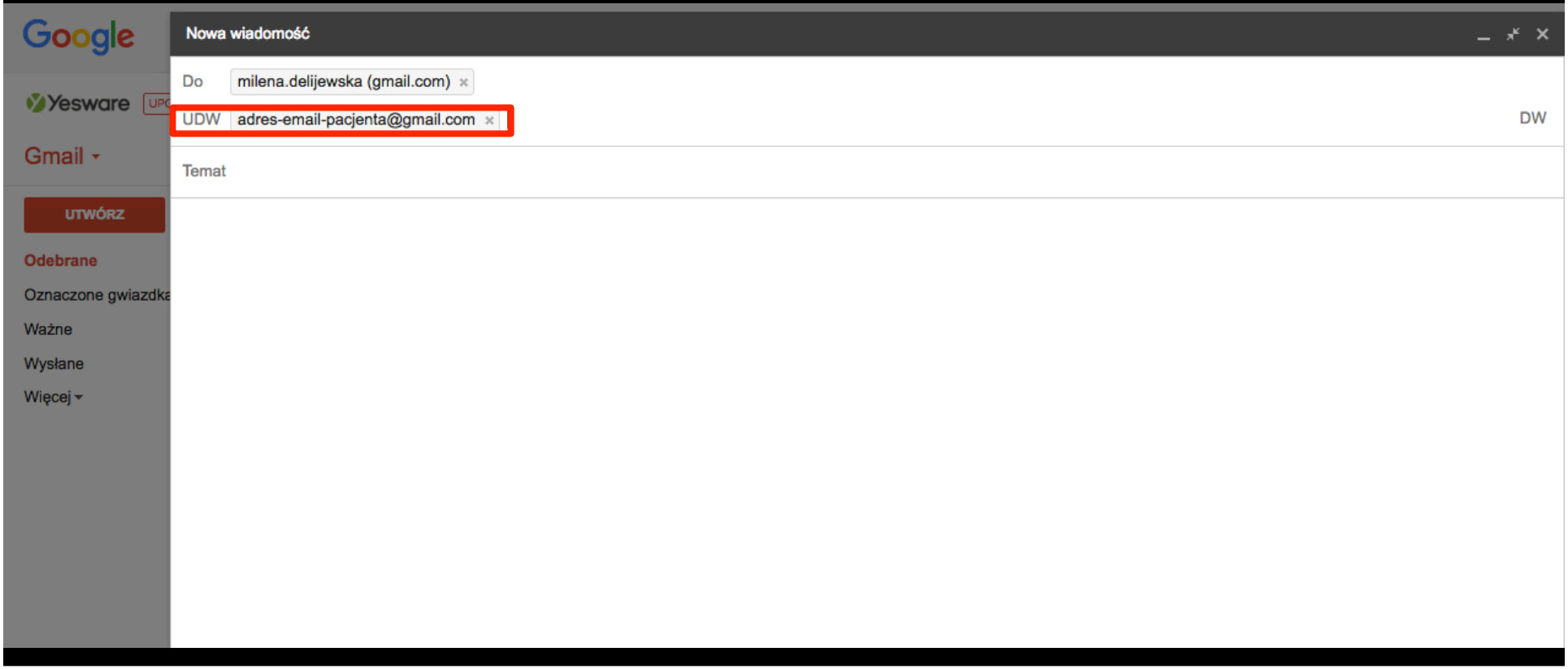
✓ Osoba postronna – np. pacjent - spoglądająca na nasze biurko lub ekran nie może być w stanie dostrzec jakichkolwiek informacji przeznaczonych dla osób upoważnionych. Nie korzystamy z karteczek z zapisanym hasłem do komputera przyklejanych do monitora.
✓Jeżeli na biurku znajdują się koperty z historiami chorób pacjentów zaplanowanych na dzisiaj, a na każdej z kopert znajduje się imię, nazwisko, pesel, adres pacjenta, to układamy je w odwrotny sposób.

✓ Ustawienie monitora powinno zapewniać brak możliwości wglądu do danych osobowych przez osoby postronne i umożliwić wgląd do wyświetlanej zawartości przez osobę pracującą z danym komputerem. Zwykle polega to na ustawieniu monitora pod odpowiednim kątem.

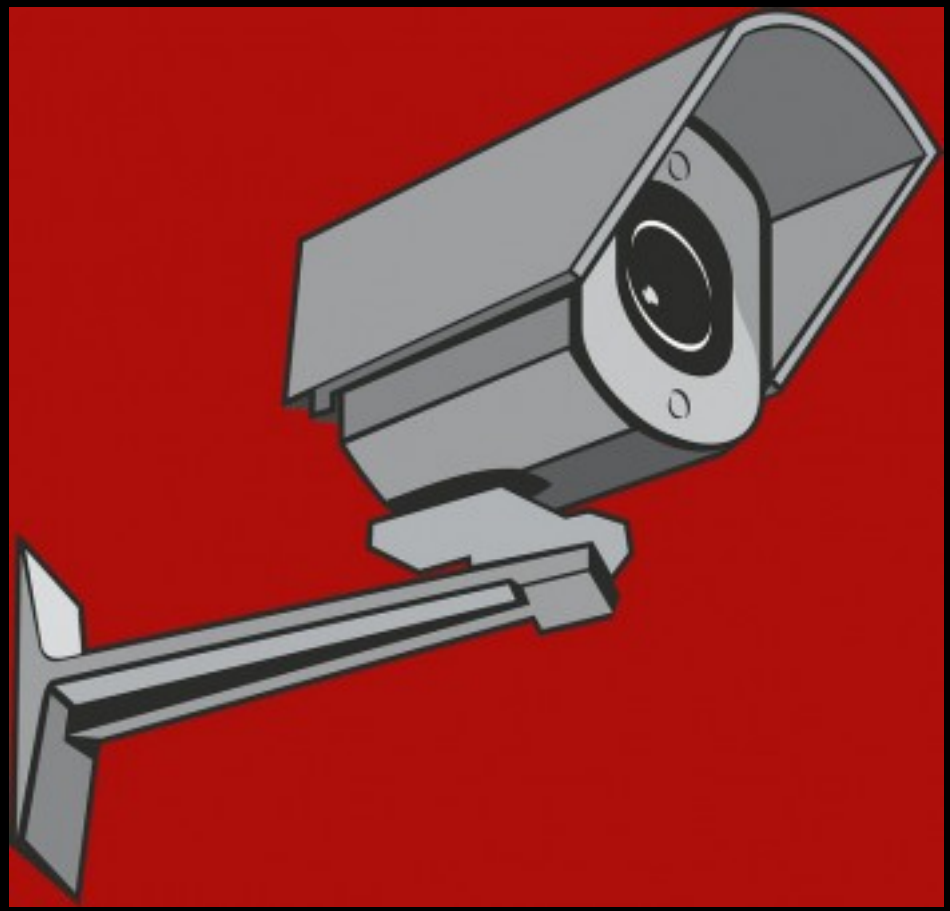
✓ Odchodząc od komputera naciskamy jednocześnie klawisze: flaga + L, dzięki temu aby wznowić pracę z komputerem wymagane będzie wprowadzenie hasła.

Dokumenty zawierające dane osobowe utylizujemy używając niszczarki

Szyfrujemy dane osobowe przesyłane poprzez e-mail albo poprzez umieszczanie danych w pliku zip z hasłem i przesłanie hasła w SMS na telefon komórkowy odbiorcy lub podanie osobiście



MONITORING WIZYJNY



MONITORING WIZYJNY

ZGODA PACJENTA?

Wyrok Naczelnego Sądu Administracyjnego z dnia 18.11.2009 r.

Wizerunki stanowią bez wątpienia dane osobowe, a ochrona danych osobowych obejmuje także ochronę wszystkich faktów dotyczących przeszłości określonego człowieka.

Art. 43 ust. 1 pkt 5 Ustawy o ochronie danych osobowych

Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych dotyczących osób korzystających z ich usług medycznych (...).

MONITORING WIZYJNY

ZGODA PRACOWNIKA?

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 06.06.2012 r.

Monitoring musi spełniać wymogi zgodności z prawem, usprawiedliwionego celu, proporcjonalności, transparentności oraz uwzględnienia przepisów o ochronie danych osobowych. Wymóg transparentności oznacza zaś, że **pracownicy powinni mieć świadomość, iż są poddawani monitoringowi**. Pracodawca winien zatem szczegółowo określić zasady monitoringu i zapoznać z nimi pracowników, którzy fakt zapoznania się powinni potwierdzić stosownym podpisanym oświadczeniem o ich akceptacji.

„Klauzula usprawiedliwionego celu“ administratora danych osobowych

Artykuł 23

1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:
   1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych,
   2) zezwalają na to przepisy prawa,
   3) (7) jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia koniecznych działań przed zawarciem umowy,
   4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
   5) (8) jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych, o których mowa w art. 3 ust. 2, lub osób trzecich, którym są przekazywane te dane - a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.


e-GIODO
Rej.ABI
Wyszukiwanie
Wyszukiwanie +
Wypełnianie wniosku
Wysyłanie/Sprawdzenie
Twoja sprawa
Nr księgi: 173420 Data zatw./aktual.: 2016-11-14 Nr zgł.: 023697/2014 Data wpł.: 2014-07-28
A,B
C
D
« wybierz właściwą zakładkę klikając na odpowiedni opis
Część A.
Nazwa zbioru danych osobowych:
Monitoring wizyjny na terenie Spółki
1. Wnioskodawca (administrator danych):
Administrator: SZPITAL WOJEWÓDZKI IM. JANA PAWŁA II W BEŁCHATOWIE
REGON: 000306503
Miejscowość: Bełchatów
Kod pocztowy: 97-400
Ulica: Czapliniecka
Nr domu: 123
Lokal:
Województwo: łódzkie
Powiat: bełchatowski (Bełchatów)
Gmina:
Poczta:
(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

[redacted]

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

- [ ] zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,

- [ ] przetwarzanie jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa

- [ ] przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

- [ ] gdy przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego - jeśli TAK, to opisz te zadania:

- [x] przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

[redacted]

Wyrok Wojewódzkiego Sądu Administracyjnego z dnia 06.06.2012 r.

Monitoring musi spełniać wymogi zgodności z prawem, usprawiedliwionego celu, proporcjonalności, transparentności oraz uwzględnienia przepisów o ochronie danych osobowych. Wymóg transparentności oznacza zaś, że **pracownicy powinni mieć świadomość, iż są poddawani monitoringowi.** Pracodawca winien zatem szczegółowo określić zasady monitoringu i zapoznać z nimi pracowników, którzy **fakt zapoznania się powinni potwierdzić stosownym podpisanym oświadczeniem o ich akceptacji.**

1. Od dnia roku pomieszczenia Kliniki , za wyjątkiem pomieszczeń sanitarnych ,znajdują się pod nadzorem audio-wizualnym.

2. Celem monitoringu jest dbałość o mienie pracodawcy, prawidłowe wykonywanie obowiązków przez pracowników, świadczenie najwyższej jakości usług; przestrzeganie przez podwykonawców ustalonego czasu i jakości pracy; rozstrzyganie spraw dotyczących roszczeniowych pacjentów.

3. Nagrania mogą być wykorzystywane jedynie w celach określonych w/wych punktach.

Wyrok Naczelnego Sądu Administracyjnego z dnia 18.11.2009 r.

Wizerunki stanowią bez wątpienia dane osobowe, a ochrona danych osobowych obejmuje także ochronę wszystkich faktów dotyczących przeszłości określonego człowieka.

WYKORZYSTANIE WIZERUNKU LEKARZA

Wśród wymienionych w Kodeksie pracy informacji o pracowniku **nie ma zdjęcia pracownika**, tak więc pracodawca, aby móc legalnie je pozyskać w celu np. mieszczania na identyfikatorach czy stronach internetowych, musi pozyskać na to zgodę pracownika. Zgodnie z art. 7 pkt. 5 ustawy o ochronie danych osobowych zgoda taka musi być dobrowolna (pracownik ma możliwość odmowy bez ryzyka poniesienia konsekwencji), nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
Zgoda może być odwołana w każdym czasie.
Najlepiej, aby zgoda udzielona była w formie pisemnej, ze względu na wartość dowodową.

OŚWIADCZENIE

Wyrażam bezterminową zgodę na wykorzystanie mojego wizerunku do celów marketingowych, reklamowych, promujących klinikę ……

CO SPRAWDZA GIODO?

Rodzaje kontroli GIODO

- **Kontrola z urzędu** - wykonywana z własnej inicjatywy GIODO w ramach wykonywania zadań kontrolnych nałożonych przez ustawę.
- **Kontrola na wniosek** - wykonywana przez GIODO na wniosek podmiotu zewnętrznego np. PIP, NIK, związki zawodowe, pracodawcy, osoba fizyczna itd.
- **Kontrola częściowa** - dotyczy zwykle poszczególnych zagadnień w procesie przetwarzania danych będących przedmiotem skargi.
- **Kontrola kompleksowa** - dotyczy wszystkich zbiorów danych osobowych prowadzonych przez kontrolowanego ADO oraz obejmuje swoim zakresem wszystkie wymogi określone w przepisach o ochronie danych osobowych, mające zastosowanie w działalności danego podmiotu.
- **Kontrola sektorowa** - może być częściowa lub kompleksowa. Jest wskazana przez GIODO w rocznym harmonogramie kontroli i dotyczy wybranej kategorii podmiotów lub zagadnień.

Rodzaje kontroli GIODO

- **Kontrola z urzędu** - wykonywana z własnej inicjatywy GIODO w ramach wykonywania zadań kontrolnych nałożonych przez ustawę.
- **Kontrola na wniosek** - wykonywana przez GIODO na wniosek podmiotu zewnętrznego np. PIP, NIK, związki zawodowe, pracodawcy, osoba fizyczna itd.
- **Kontrola częściowa** - dotyczy zwykle poszczególnych zagadnień w procesie przetwarzania danych będących przedmiotem skargi.
- **Kontrola kompleksowa** - dotyczy wszystkich zbiorów danych osobowych prowadzonych przez kontrolowanego ADO oraz obejmuje swoim zakresem wszystkie wymogi określone w przepisach o ochronie danych osobowych, mające zastosowanie w działalności danego podmiotu.
- **Kontrola sektorowa - może być częściowa lub kompleksowa. Jest wskazana przez GIODO w rocznym harmonogramie kontroli i dotyczy wybranej kategorii podmiotów lub zagadnień.**

GIODO
Generalny Inspektor Ochrony Danych Osobowych

20-LECIE PRAWA DO OCHRONY DANYCH OSOBOWYCH W POLSCE

O Urzędzie | Kontrole | Prawo | Edukacja | Współpraca | Wydarzenia | Serwis prasowy | Odpowiedzi na pytania | Kontakt

O Urzędzie

- Generalny Inspektor
- Zadania i kompetencje
- Poprzednicy
- BIP
- Biuro
- Statystyki i sprawozdania

Reforma przepisów

» O Urzędzie

Plan kontroli sektorowych

Metadane

Na rok 2017 Generalny Inspektor Ochrony Danych Osobowych (GIODO) zaplanował kontrole sektorowe następujących kategorii podmiotów w poniżej wskazanym zakresie:

1. Sklepy stacjonarne: w zakresie przetwarzania danych osobowych w związku ze stosowaniem monitoringu pozwalającego na profilowaniu klientów. Zastrzeżenia pojawiają się odnośnie do monitorowania klientów przez sklepy, które korzystają z narzędzi (w tym kamer), umożliwiających nie tylko liczenie osób odwiedzających daną placówkę, ale pozwalających również na analizę płci i wieku na podstawie twarzy wyświetlonej na monitorze używanego w tym celu urządzenia.

2. Przychodnie i poradnie lekarskie (publiczne i niepubliczne) funkcjonujące w strukturach podmiotów wykonujących działalność lecznicą (ustawa o działalności leczniczej z dnia 15 kwietnia 2011 r.)**:** w zakresie przetwarzania danych osobowych w związku z rejestracją pacjentów. Szczególną uwagę GIODO zwróci na problem konieczności podawania przez pacjentów, w obecności innych osób, danych osobowych wymaganych podczas rejestracji w placówkach służby zdrowia oraz na zastosowane środki techniczne i organizacyjne w celu ich zabezpieczenia.

Generalny Inspektor Ochrony Danych Osobowych zaplanował kontrole w ww. sektorach ze względu na coraz częściej pojawiające się zagrożenia naruszenia przepisów o ochronie danych osobowych w sygnalizowanych obszarach, w tym liczne sygnały obywateli korzystających z usług takich podmiotów.

14.12.2012 roku zawarto porozumienie między GIODO a Państwową Inspekcją Pracy.

Od tego momentu to, czy przedsiębiorcy i inne instytucje, w tym każda instytucja ochrony zdrowia, przestrzegają przepisów Kodeksu pracy oraz przepisów z zakresu ochrony danych osobowych może być sprawdzane podczas jednej kontroli prowadzonej albo przez pracowników Biura GIODO albo Państwowej Inspekcji Pracy.

ZAWIADOMIENIE O KONTROLI

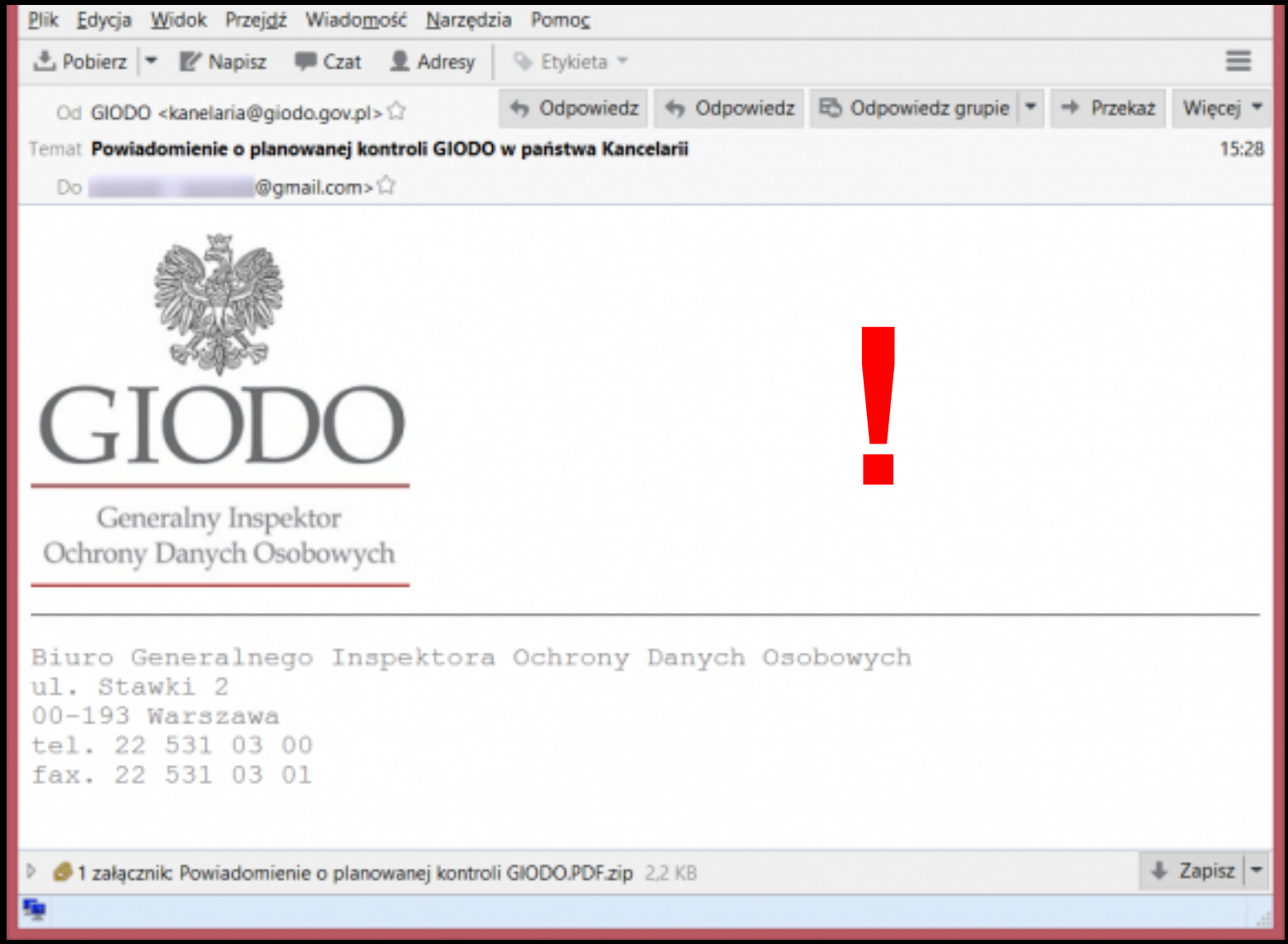
Ustawa o ochronie danych osobowych nie reguluje tej kwestii. Jednak przyjąć należy, iż administrator danych, u którego będą prowadzone czynności kontrolne, **powinien być poinformowany o terminie kontroli.** Kontrolowany podmiot ma wówczas możliwość przygotowania się do kontroli, a w szczególności sprawdzenia dokumentacji, uzupełnienia ewentualnych nieprawidłowości, które mogłyby zostać zakwestionowane przez inspektora.

CO DO ZASADY

W odniesieniu do przedsiębiorców obowiązują regulacje dotyczące zawiadomienia o kontroli. Stosownie do art. 79 ust. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej kontrolę wszczyna się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomieni o zamiarze wszczęcia kontroli.

Brak wcześniejszego zawiadomienia o kontroli nie uprawnia administratora danych do odmowy wstępu inspektorom GIODO, stanowi natomiast przesłankę do wniesienia do GIODO sprzeciwu.

CHYBA, ŻE .... okoliczności sprawy wskazują, iż kontrolowany mógłby ukryć dowody, które świadczą o popełnieniu przez niego czynu zabronionego wskazanego w ustawie.


Plik Edycja Widok Przejdź Wiadomość Narzędzia Pomoc
Pobierz Napisz Czat Adresy Etykieta
Od GIODO <kanelaria@giodo.gov.pl>
Odpowiedz Odpowiedz Odpowiedz grupie Przekaż Więcej
Temat Powiadomienie o planowanej kontroli GIODO w państwa Kancelarii
15:28
Do @gmail.com>
GIODO
Generalny Inspektor
Ochrony Danych Osobowych
!
Biuro Generalnego Inspektora Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
tel. 22 531 03 00
fax. 22 531 03 01
1 załącznik: Powiadomienie o planowanej kontroli GIODO.PDF.zip 2,2 KB
Zapisz

Kontrola GIODO może odbyć się:

- korespondencyjnie lub
- na miejscu: w obrębie pomieszczeń, w których są przetwarzane dane osobowe w godzinach od 6.00 do 22.00 przez GIODO, zastępcę GIODO, upoważnionych pracowników biura GIODO - po okazaniu imiennego upoważnienia (2 strony A4) i legitymacji służbowej

GIODO
Generalny Inspektor Ochrony Danych Osobowych

20-LECIE PRAWA DO OCHRONY DANYCH OSOBOWYCH W POLSCE

20

O Urzędzie | Kontrole | Prawo | Edukacja | Współpraca | Wydarzenia | Serwis prasowy | Odpowiedzi na pytania | Kontakt

Kontrole

- 2017 r.
- 2016 r.
- 2015 r.

Reforma przepisów

» Kontrole » 2017 r.

Plan sektorowych sprawdzeń dla GIODO

Metadane

W 2017 r. Generalny Inspektor Ochrony Danych Osobowych (GIODO) skieruje do ABI powołanych w **przychodniach i poradniach lekarskich (publicznych i niepublicznych)**, wystąpienia o dokonanie sprawdzeń, o których mowa w art. 19b ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Ich przedmiotem będzie przetwarzanie danych osobowych w związku z rejestracją pacjentów, w tym zastosowanie środków technicznych i organizacyjnych w celu zabezpieczenia takich danych.

Objęcie tego sektora sprawdzeniami przeprowadzanymi przez ABI na wniosek GIODO, a jednocześnie kontrolami inspektorów GIODO (co zostało ujęte w planie kontroli sektorowych GIODO na rok 2017), ma na celu zwiększenie liczby podmiotów, w których dokonana zostanie ocena przestrzegania przepisów o ochronie danych osobowych.

Wystąpienia o dokonanie sprawdzeń mogą być również doraźnie kierowane do ABI reprezentujących inne sektory, np. w związku z prowadzonymi przez GIODO postępowaniami czy też z powodu dużego społecznego zainteresowania określonymi problemami.

KONTROLA „KORESPONDENCYJNA“

GIODO nie musi przychodzić na kontrolę – **może skierować wystąpienie** do firmy zmierzające do zapewnienia skutecznej ochrony danych osobowych, a podmiot który je otrzyma ma obowiązek ustosunkować się do niego w terminie 30 dni od daty jego otrzymania. (Art. 19a UODO)

– ilość wystąpień GIODO w 2014 r.: 66
– ilość wystąpień GIODO w 2013 r.: 121
– ilość wystąpień GIODO w 2012 r.: 126

Termin trwania kontroli jest uzależniony m.in. od rodzaju kontroli, zakresu kontroli oraz wielkości kontrolowanego podmiotu. Termin jest ustalany przez Generalnego Inspektora, gdyż **przepisy nie przewidują czasu trwania kontroli.**

Jednakże w odniesieniu do przedsiębiorców przepisy ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej wskazują limity czasowe w obrębie danego roku kalendarzowego.

Art. 83 ust. 1. **Czas trwania wszystkich kontroli** organu kontroli u przedsiębiorcy w jednym roku kalendarzowym nie może przekraczać:
1) w odniesieniu do mikroprzedsiębiorców – **12 dni roboczych**

Zgodnie z obowiązującymi przepisami kontroli dokonuje sam Generalny Inspektor Ochrony Danych Osobowych lub zastępca GIODO (gdy taki został powołany) albo upoważnieni przez GIODO pracownicy, określani inspektorami:

W praktyce w skład zespołu kontrolnego wchodzą najczęściej:
• **dwóch prawników** będących pracownikami Departamentu Inspekcji Biura GIODO;
• **jeden informatyk** będący pracownikiem Departamentu Informatyki Biura GIODO.

OBOWIĄZKI INSPEKTORA

Zapoznanie kontrolowanego z jego prawami i obowiązkami następuje poprzez przedstawienie mu **upoważnienia do kontroli zawierającego pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach.** Osoba uprawniona do reprezentacji tego podmiotu poświadcza zapoznanie się z pouczeniem poprzez złożenie pod nim podpisu.

Inspektor ma obowiązek poinformować, w jaki sposób kontrolowany może domagać się np. wniesienia uwag, zastrzeżeń, poprawek i sprostowań do protokołu kontroli. W żadnym wypadku inspektor nie może przekraczać zakresu upoważnienia udzielonego przez Generalnego Inspektora – nie może domagać się okazania dokumentów lub podawać informacji o okolicznościach**, które nie mają związku z przedmiotem kontroli**, np. dotyczących sytuacji finansowej.


RZECZPOSPOLITA
POLSKA
Biuro Generalnego Inspektora
Ochrony Danych Osobowych
001
LEGITYMACJA SŁUŻBOWA
Inspektora
Ochrony Danych Osobowych

Załącznik
do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r.
(poz. 601)

WZÓR

.....
(pieczęć podłużna Generalnego Inspektora
Ochrony Danych Osobowych)

L.dz. . .....

Upoważnienie imienne

Na podstawie art. 12 pkt 1 i 2 w związku z art. 14 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238 oraz z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497)

upoważniam

Panią/Pana
.....
.....
(imię i nazwisko inspektora)

stanowisko służbowe ..... nr legitymacji służbowej .....
do przeprowadzenia kontroli:
.....
.....
.....
.....
.....
.....
(określenie: podmiotu objętego kontrolą albo zbioru danych, albo miejsca poddawanego kontroli)
w zakresie:
.....
.....
.....
.....
.....
.....
(określenie zakresu przedmiotowego kontroli)

Data rozpoczęcia kontroli:
.....
Przewidywany termin zakończenia kontroli:
.....

Upoważnienie jest ważne jedynie z równoczesnym okazaniem legitymacji służbowej.

.....
(miejsce i data
wystawienia upoważnienia)
pieczęć urzędowa

.....
(podpis
Generalnego Inspektora

Ochrony Danych Osobowych)

Pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach

1. Zgodnie z art. 15 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli, a w szczególności umożliwić przeprowadzenie czynności oraz spełnić żądania, o których mowa w art. 14 pkt 1-4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, polegające na:
• umożliwieniu wstępu inspektorom, w godzinach od 600 do 2200, za okazaniem niniejszego imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym jest zlokalizowany zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą o ochronie danych osobowych,
• żądaniu złożenia pisemnych lub ustnych wyjaśnień oraz wzywania i przesłuchiwania osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
• umożliwieniu wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,
• przeprowadzaniu oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.
2. Zgodnie z art. 16 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu administratorowi danych. Protokół podpisują inspektor i kontrolowany administrator danych, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi (art. 16 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych). W razie odmowy podpisania protokołu przez kontrolowanego administratora danych inspektor czyni o tym wzmiankę w protokole, a odmawiający podpisu może, w terminie 7 dni, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi (art. 16 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych).

.....
(data i czytelny podpis osoby
reprezentującej kontrolowany podmiot)

OBOWIĄZKI KONTROLOWANEGO

Kontrolowany ma obowiązek **umożliwić inspektorowi przeprowadzenie czynności kontrolnych** oraz powinien **udostępnić wszelkie żądane dokumenty i nośniki informacji** związane z zakresem kontroli. Na żądanie inspektora kontrolowany jest obowiązany **wydać kopie wskazanych dokumentów oraz tzw. zrzuty (wydruki) z ekranu komputera.** Powinien **czynnie uczestniczyć w prowadzonej kontroli**: udzielać wyjaśnień, zapewnić terminowe udzielanie informacji przez podległych pracowników i inne osoby uczestniczące w procesie przetwarzania danych, być do dyspozycji w czasie trwania kontroli – w celu zapewnienia sprawnego jej przebiegu.

CO KONTROLUJĄ INSPEKTORZY GIODO?

1. Polityka bezpieczeństwa informacji i Instrukcja zarządzania systemem informatycznym – czy są kompletne, formalnie zatwierdzone i wdrożone, zgodne z wymogami 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

2. Pracownicy - czy zostały im nadane upoważnienia do przetwarzania danych osobowych i prowadzona jest ewidencja osób upoważnionych, czy byłym pracownikom zablokowano uprawnienia.

3. Rejestracja zbiorów – czy właściwe zbiory zostały zarejestrowane w GIODO.

4. Prowadzenie właściwych wykazów zbiorów – czy prowadzony jest wykaz zbiorów danych osobowych, a w przypadku, gdy powołany został ABI dodatkowo również rejestr zgodny z Rozporządzeniem Ministra Administracji i Cyfryzacji z 11 maja 2015 r.

5. Stosowanie odpowiednich środków ochrony – technicznych i organizacyjnych, czy są wystarczające i adekwatne do występujących zagrożeń. W tym następuje sprawdzenie, czy podpisano umowy powierzenia przetwarzania danych z firmami zewnętrznymi oraz jak utylizowana jest dokumentacja medyczna.

6. Sposób zabezpieczenia systemu informatycznego: stosowanie indywidualnych haseł, ochrona przed wirusami i oprogramowaniem hakerskim, zabezpieczenie przed skutkami **awarii, kopie zapasowe.**

7. Przesłanki legalności przetwarzania danych osobowych i obowiązki informacyjne.

WYNIKI KONTROLI

Protokół powinien zostać podpisany zarówno przez inspektora przeprowadzającego kontrolę w firmie, jak i przez samego ADO.
ADO może wnieść do protokołu zastrzeżenia i uwagi.

Gdy ADO odmówi podpisania protokołu, inspektor odnotowuje ten fakt w protokole. ADO odmawiający podpisu w terminie 7 dni może przedstawić swoje stanowisko na piśmie GIODO.

Jeżeli po przeprowadzonej kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do Generalnego Inspektora o wydanie decyzji administracyjnej, o której mowa w art. 18 ustawy.

UWAGA

Metadane

30 CZERWCA 2015 R. TO TERMIN ZGŁOSZENIA **DO REJESTRACJI ABI**, A NIE ZBIORÓW DANYCH.

GIODO NIE NAKŁADA KAR ZA NIEZGŁOSZENIE ZBIORU DO REJESTRACJI.

W związku z pojawiającymi się w sieci błędnymi informacjami o konieczności zgłoszenia - do 30 czerwca 2015 r. - zbiorów danych osobowych do rejestracji GIDOO i groźbie nałożenia kary do 200 tys. zł za niedotrzymanie tego terminu, GIODO raz jeszcze informuje:

:: 30 czerwca 2015 r. to ostateczny termin na zgłoszenie do rejestracji GIODO dotychczasowych administratorów bezpieczeństwa informacji (ABI), o ile administrator danych zdecyduje, by dalej pełnili oni tę funkcję,

:: jeśli administrator danych powoła ABI i zgłosi go do rejestracji GIODO, zwolniony będzie z obowiązku rejestracji zbiorów danych u Generalnego Inspektora (z wyjątkiem zbiorów zawierających dane szczególnie chronione).

Więcej szczegółowych wyjaśnień na temat zmian, jakie od 1 stycznia 2015 r. zostały wprowadzone do ustawy o ochronie danych osobowych, jest dostępnych pod linkiem http://www.giodo.gov.pl/1520223/j/pl/.

Ponadto należy przypomnieć, że żaden przepis **nie uprawnia GIODO do nakładania kar finansowych, w tym za niezgłoszenie zbioru danych osobowych do rejestracji. Z**a niedopełnienie tego obowiązku przewidziana jest odpowiedzialność karna,jednak o rodzaju kary decyduje sąd. Nawet jeśli byłaby nią kara grzywny, to nakłada ją sąd, i to on określa jej wysokość. GIODO może nałożyć jedynie grzywnę, ale tylko w celu przymuszenia, w przypadku niewykonania wydanej przez niego decyzji.

Najczęściej wskazywane przez GIODO błędy popełniane przez ADO w placówkach medycznych:

1. Niedopełnienie obowiązku informacyjnego wobec usługobiorców (pacjentów) i pracowników (brak informacji kto jest administratorem danych, np. na drukach wypełnianych przed pacjentów czy pracowników na etapie zatrudniania w placówce).
2. Brak lub niekompletna dokumentacja ochrony danych osobowych.
3. Środki techniczne i organizacyjne zapewniające ochronę danych są niewystarczające lub w ogóle ich brak: np.

• przechowywanie dokumentacji zawierającej dane osobowe, w tym danych o stanie zdrowia, na odkrytych regałach oraz w szafach niewyposażonych w zamki, a także w pomieszczeniach, do których dostęp mają osoby trzecie;
• brak czujników przeciwpożarowych/ gaśnic;
• niewłaściwie chronione archiwa medyczne/składnice akt;
• klucze do pomieszczeń, w których przechowywana jest dokumentacja medyczna personel pozostawia po pracy w drzwiach, aby swobodnie mogły wejść do nich osoby sprzątające, czyli brak tzw. procedur postępowania z kluczami;
• brak nadanych pracownikom upoważnień do przetwarzania danych osobowych lub nadawanie uprawnień do przetwarzania danych osobom, które de facto na swoim stanowisku pracy danych tych nie przetwarzają i nie mają prawa przetwarzać (np. osoby sprzątające);
• brak ewidencji osób upoważnionych do przetwarzania danych osobowych.

Najczęściej wskazywane przez GIODO błędy popełniane przez ADO w placówkach medycznych c.d.:

4. Brak zgłoszenia zbioru danych do GIODO, jeśli zbiór taki podlega zgłoszeniu.
5. Wywoływanie pacjentów zapisanych w kolejce do lekarza po nazwisku lub wywieszanie list pacjentów na drzwiach gabinetów.
6. Brak regulacji w zakresie stosowania monitoringu wizyjnego.

Art. 18. Ustawy o ochronie danych osobowych

1. W przypadku naruszenia przepisów o ochronie danych osobowych **Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej**, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień;

2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych;

3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;

4) wstrzymanie przekazywania danych osobowych do państwa trzeciego;

5) zabezpieczenie danych lub przekazanie ich innym podmiotom;

6) usunięcie danych osobowych.