Dokumentacja bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.

Specyfikacja projektowa

Autor: Wiesław Jan Palczewski
Data ostatniej zmiany: 19 lutego 2022
Streszczenie: Opracowanie omawia sposób przygotowania i zakresu dokumentacji opisującej politykę bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. [1], 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. Nr 100 poz. 1024, [2]). Dokument jest zgodny z informacjami i wymogami zawartymi w portalu Generalny Inspektor Ochrony Danych Osobowych [3]

Podstawowe informacje o dokumencie

Autor:	Wiesław Jan Palczewski
Status:	roboczy
Tytuł:	Dokumentacja bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.
Podtytuł:	Specyfikacja projektowa
Projekt:	MEDUCASE
Utworzenie:	1 października 2015 roku
Ostatnie zmiany:	19 lutego 2022
Wersja:	1.3
Liczba stron:	72+2
Plik źródłowy:	giodo_v2.tex

Zastrzeżenia

1. Wszystkie nazwy handlowe i towarów występujące w niniejszym dokumencie są znakami towarowymi zastrzeżonymi odnośnych właścicieli.
2. Niniejszy dokument nie stanowi oferty w znaczeniu prawa handlowego.
3. Treść poniższego dokumentu nie może być wykorzystywana poza firmą MEDUCASE Sp. z o.o.

Strona kontroli dokumentu:

L.p.	Opis niezgodności	Niezgodność z	Zalecenia	Opis realizacji
Wymagane zmiany do wersji 1.2				
1.	nieaktualne nazwiska osób funkcyjnych	ze stanem osobowym w firmie	uaktualnić dokumentację	dopisać nazwiska Pana mec. Tomasza Leśniaka i mgr inż. Marcina Roczka z firmy Rekonstrukcja Zdrowia Sp. z o.o. ul. Wrocławska 46-48, 45-701 Opole

Tabela 1: Wymagane zmiany

Spis treści

Wstęp

Zgodnie z Ustawą [2] dokumentacja przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych dzieli się na:

- politykę bezpieczeństwa,
- instrukcję zarządzania systemem informatycznym.

Polityka bezpieczeństwa zawiera w szczególności:

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

Instrukcja zawiera w szczególności:

1. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5. sposób, miejsce i okres przechowywania:
    - elektronicznych nośników informacji zawierających dane osobowe,
    - kopii zapasowych, o których mowa w pkt 4,

6. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
7. sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia;
8. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

→ ***UWAGA:***
W systemie teleinformatycznym meducase *obowiązuje niniejszy dokument o nazwie: „*Dokumentacja bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.*" obejmujący* ***łącznie*** *procedury ochrony danych osobowych określonych w Polityce Bezpieczeństwa oraz w Instrukcji Zarządzania Systemem Informatycznym.*

Poziomy bezpieczeństwa

W SYSTEMIE TELEINFORMATYCZNYM MEDUCASE stosujemy **wysoki** poziom bezpieczeństwa, gdyż przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

W treści instrukcji zawarte są ogólne informacje o ZINTEGROWANYM INTERNETOWYM SYSTEMIE PORTALI MEDUCASE i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, o zastosowanych rozwiązaniach technicznych, jak również o procedurach eksploatacji i zasadach użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Administrator danych, do przetwarzania danych wykorzystuje nie jeden, lecz kilka systemów informatycznych Systemy są bardzo podobne i bazują na jednolitej technologii programistycznej. Instrukcja zarządzania obejmuje i dotyczy każdego z użytkowanych systemów.

W instrukcji wskazane są systemy informatyczne, ich lokalizacje, stosowane metody dostępu (bezpośrednio z komputera, na którym system jest zainstalowany, w lokalnej sieci komputerowej, czy też poprzez sieć telekomunikacyjną Internet). Instrukcja obejmuje zagadnienia dotyczące zapewnienia bezpieczeństwa informacji, a w szczególności elementy wymienione w §5 rozporządzenia, na które składają się:

- 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,
  - kopii zapasowych, o których mowa w pkt. 4,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,
- sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Szczegółowe wymagania i zalecenia dotyczące zagadnień, jakie powinny być zawarte w instrukcji przedstawiono poniżej.

1. Daty kluczowe

Istotne dla SYSTEMU TELEINFORMATYCZNEGO MEDUCASE daty są następujące:

1. 15.04.2011 r. – rejestracja w międzynarodowym systemie informacji o wydawnictwach ciągłych CZASOPISMA PrzypadkiMedyczne.pl w Bibliotece Narodowej - ISSN 2083-0033
2. 28.06.2015 r. – zawiązanie spółki z ograniczoną odpowiedzialnością, Repertorrium A numer 3884/2015
3. 21.08.2015 r. – rozpoczęcie prac nad oprogramowaniem portalu WWW.PrzypadkiMedyczne.pl
4. 19.10.2015 r. – Postanowienie Sądu Rejonowego dla Wrocławia-Fabryczna o wpisaniu do Krajowego Rejestru Sadowego: Rejestru Przedsiębiorców pod numerem KRS 0000581184 MEDUCASE Spółki z ograniczoną odpowiedzialnością, sygn. sprawy: WR.VI NS-REJ.KRS/027600/15/133
5. 21.10.2015 r. – rozpoczęcie prac nad dokumentacją bezpieczeństwa informacji w firmie MEDUCASE SP. Z O.O.
6. 25.11.2015 r. – zawarcie umowy o świadczenie usług księgowych z biurem Rachunkowym „*Konstans*"
7. 27.11.2015 r. – wpisanie zbioru danych osobowych o nazwie: „Zbiór danych użytkowników serwisów" do Rejestru Zbiorów Danych Osobowych w GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH (rejestracja zbiorów danych osobowych)
8. 1.12.2015 r. – Porozumienie pomiędzy PayU S.A. a COMVIDEO Krystyna Palczewska odnośnie cesji umowy Nr 70534 z dnia 14.02.2012 r. na rzecz MEDUCASE SP. Z O.O.
9. 5.05.2016 r. – postanowienie sądu Sygn. akt I Ns Rej. Pr. 59/16, Rej Pr 3057 o zmianie wydawcy czasopisma „PrzypadkiMedyczne.pl". Dotychczasowy wydawca: Krystyna Palczewska COMVIDEO, nowy wydawca: MEDUCASE SP. Z O.O.

10. 10.05.2016 r. – uruchomienie portalu CZASOPISMO PrzypadkiMedyczne.pl u nowego providera z wykorzystaniem nowego oprogramowania
11. 29.03.2020 r. – opracowanie wersji drugiej *Dokumentacji bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.*
12. 1.01.2022 r. – opracowanie wersji trzeciej *Dokumentacji bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.*

2. Definicje

Najczęściej pojawiające się pojęcia oraz ich oficjalne definicje:

Administrator danych osobowych — organ, jednostka organizacyjna, podmiot lub osoba decydująca (samodzielnie) o celach i środkach przetwarzania danych osobowych (art. 7 pkt 4). Jest to podmiot praw i obowiązków, który sprawuje władztwo nad przetwarzaniem danych osobowych przez zaciąganie zobowiązań i rozporządzanie prawami. Nie ma przy tym znaczenia fakt, czy podmiot ten jest w posiadaniu przetwarzanych danych lub sam je przetwarza. W systemie SYSTEMIE TELEINFORMATYCZNYM MEDUCASE administatorem **ADO** jest firma MEDUCASE SP. Z O.O..

Dane osobowe — to, wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Zbiór danych osobowych — to, zgodnie z art. 7 pkt 1 ustawy o ochronie danych osobowych [2], „*każdy posiadający strukturę zestaw 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 zatem struktura, czyli takie 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.

Instytucja powierzania przetwarzania danych — określona została w art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [2]. Zgodnie

z dyspozycją tego przepisu powierzenie przetwarzania danych osobowych przez administratora danych jest dopuszczalne na podstawie pisemnej umowy z podmiotem przetwarzającym — wykonawcą, zwanym również procesorem [4].

W przypadku gdy działania te będą dotyczyły, choćby w pośredni sposób, przetwarzania danych osobowych zebranych przez administratora danych, dochodzić będzie do tzw. powierzenia przetwarzania danych osobowych.

Obowiązek informacyjny — obowiązek informacyjny określony w art. 33 ustawy [2] ma na celu zapewnienie osobom, których dane osobowe są przetwarzane w zbiorach, dostępu do informacji o okolicznościach przetwarzania ich danych. Obowiązek ten spoczywa na administratorze danych, który powinien poinformować o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna — o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Zgoda na przetwarzanie danych osobowych — Przez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

MEDUCASE Sp. z o.o., przy okazji zawierania umowy równocześnie pozyskuje zgodę na przetwarzanie danych osobowych kontrahenta. Jest to wyodrębnione oświadczenie, którego treścią jest zgoda na przetwarzanie danych osobowych, od oświadczenia wyrażającego chęć związania się postanowieniami umowy. Nie utożsamia się woli zawarcia umowy ze złożeniem oświadczenia woli, na podstawie którego osoba, której dane dotyczą, zgadza się na wykorzystywanie jej danych osobowych do innych celów.

Publikacja danych osobowych — w przypadku przetwarzania danych tzw. wrażliwych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych, zgoda na publikację danych osobowych musi być pozyskana na piśmie. Publikowane wszelkiego rodzaju rankingi, zestawienia wyników konkursów obejmujące na ogół nick uczestników w tym rozumieniu nie są kwalifikowane

jako przetwarzanie danych wrażliwych i w związku z tym nie jest wymagana dodatkowa zgoda na ich publikację.

Udostępnianie danych osobowych — art. 23 Ustawy. Zgodnie z tym przepisem, podmiot udostępniający dane osobowe, będzie mógł to uczynić m.in.:

- na podstawie zgody osoby, której dane dotyczą (art. 23 ust. 1 pkt 1 Ustawy),
- w celu realizacji umowy, której stroną jest osoba, której dane dotyczą (art. 23 ust. 1 pkt 3 Ustawy), lub
- dla wypełnienia prawnie usprawiedliwionych celów przez siebie realizowanych np. marketing bezpośredni własnych produktów lub usług (art. 23 ust. 1 pkt 5 Ustawy).

Co ważne, udostępnienie danych osobowych w oparciu o art. 23 ust. 1 pkt 5 Ustawy będzie mogło nastąpić, jeśli będzie ono niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez podmiot udostępniający dane albo podmiot, który ma je otrzymać. Dodatkowo trzeba zaznaczyć, że udostępnienie danych na podstawie cytowanego przepisu nie może naruszać praw i wolności osób, których udostępniane dane dotyczą. W SYSTEMIE TELEINFORMATYCZNYM MEDUCASE dane osobowe nie są udostępniane.

Zabezpieczenia danych osobowych — Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz ww. środki (art. 36 ustawy). Administrator danych (ADMINISTRATOR DANYCH OSOBOWYCH):

- wyznacza pełnomocnika ds. danych osobowych[1], nadzorującego przestrzeganie zasad ochrony, chyba że sam wykonuje te czynności,
- upoważnia inne osoby do przetwarzania danych[2],
- zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane,
- prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

[1] W SYSTEMIE TELEINFORMATYCZNYM MEDUCASE nie jest wyznaczany **A**dministrator **B**ezpieczeństwa **I**nformacji (**ABI**)

[2] W SYSTEMIE TELEINFORMATYCZNYM MEDUCASE wyznaczany jest **A**dministrator **S**ystemu **I**nformatycznego (**ASI**)

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.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Środki bezpieczeństwa, sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych, podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne określa Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych [1, 5].

Fakturownia — to program do faktur. Fakturownia zapewnia bezpieczeństwo na najwyższym poziomie. W portalu stosowane są najwyższej klasy zabezpieczenia używane w bankach i innych instytucjach finansowych. Zapewniając bezpieczny dostęp do konta oferowane jest szyfrowanie za pomocą protokołu SSL [6] https://fakturownia.pl/.

CPM — czasopismo PrzypadkiMedyczne.pl

ABI — administrator bezpieczeństwa informacji (nie wyznaczany w systemie teleinformatycznym meducase).

ASI — administrator systemu informatycznego (jego obowiązki opisane są w roz. D).

PADO — pełnomocnik administratora danych osobowych (jego obowiązki opisane są w roz. C).

poufność — zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,

integralność — zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

dostępność — zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,

rozliczalność — zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

autentyczność — zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),

niezaprzeczalność — brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,

niezawodność — zapewnienie spójności oraz zamierzonych zachowań i skutków.

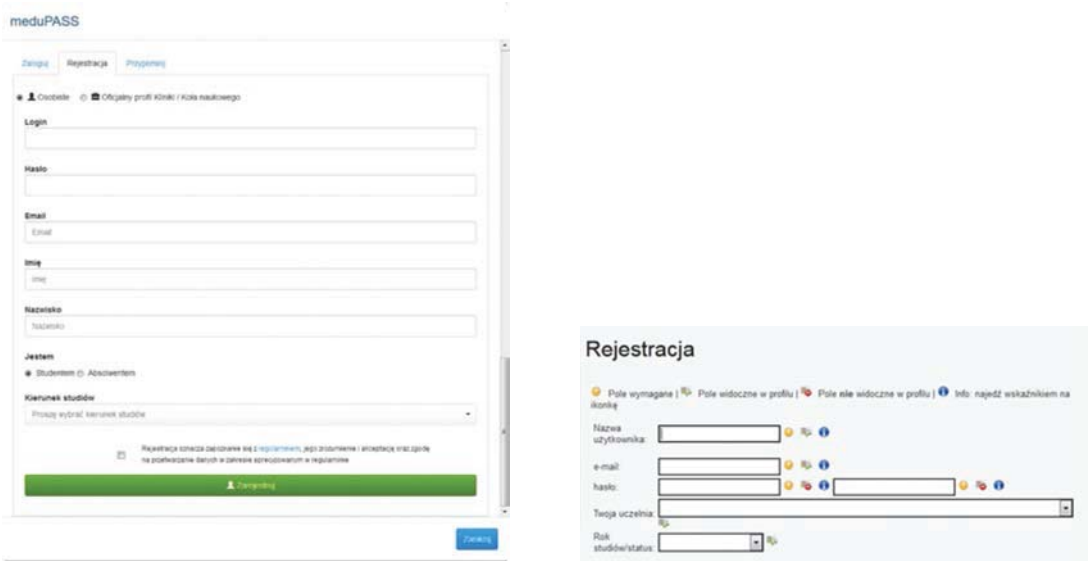
3. Charakterystyka systemu, zakres

MEDUCASE Sp. z o.o. jest animatorem, autorem, właścicielem i współwłaścicielem następujących portali (stron internetowych):

1. Przypadki Medyczne, https://PrzypadkiMedyczne.pl. Portal zawiera w sobie następujące moduły:
   - publikacje wraz z systemem JMS CZASOPISMO PrzypadkiMedyczne.pl
   - quizy, testy i konkursy
   - LEK-endium
   - konferencje naukowe
2. Kazusy Prawne, https://kazusyprawne.pl/
3. Ogólnopolskie forum studentów medycyny i lekarzy https://medfor.me/
4. Portal edukacyjny https://www.mdcse.com/index.php/en/
5. Portal poświęcony kongresowi ESPES'2017 http://espes2017.pl

4. Procedury nadawania uprawnień

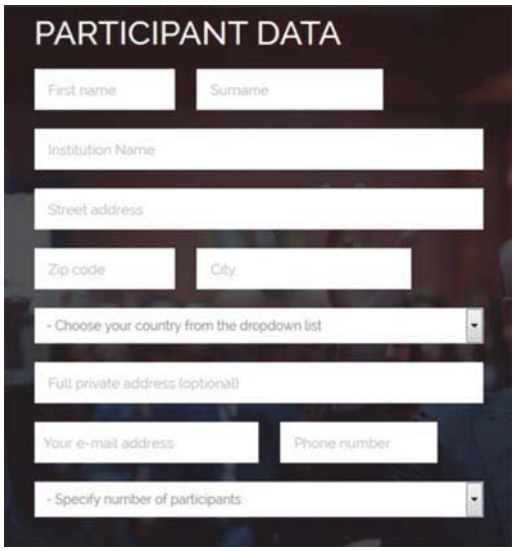
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności respektują przepisy i zasady zdefiniowane w § 5 pkt 1 rozporządzenia [2]. W eksploatowanych systemach użytkownicy sami tworzą swoje profile. Dane jakie są pobierane podczas rejestracji ilustrują rys. 4.1.



(a) http://PrzypadkiMedyczne.pl (b) http://KazusyPrawne.pl

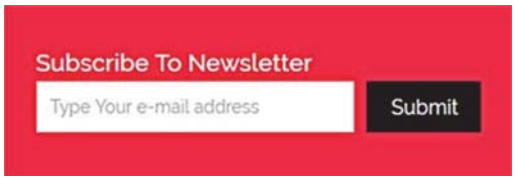
Rys. 4.1: Okno z wymaganymi polami danych podczas rejestracji do portalu

(a) http://medfor.me/register/

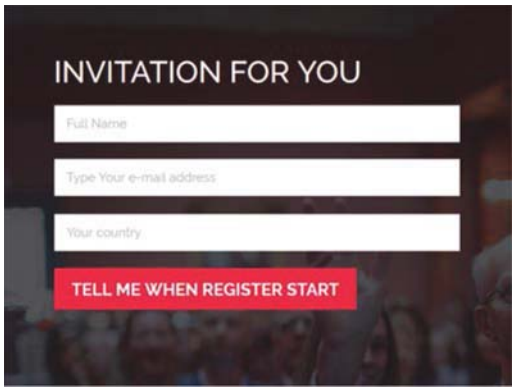


(b) http://www.espes2017.pl/pl/registration — formularz rejestracyjny

Rys. 4.2: Okno z wymaganymi polami danych podczas rejestracji do portalu



(a) http://www.espes2017.pl/pl/kontakt — zapis do Newsletter



(b) http://espes2017.pl — formularz potrzeby informowania

Rys. 4.3: Okno z wymaganymi polami danych podczas rejestracji do portalu

Osobami odpowiedzialnymi za realizację procedur rejestrowania i wyrejestrowywania użytkowników w SYSTEMIE TELEINFORMATYCZNYM MEDUCASE są:

1. prezes MEDUCASE Sp. z o.o.
2. ADMINISTRATOR Systemu Informatycznego
3. PEŁNOMOCNIK ADMINISTRATORA DANYCH OSOBOWYCH

Uprawnienia dla użytkowników uprzywilejowanych nadaje tylko i wyłącznie prezes MEDUCASE Sp. z o.o., realizatorem jest on sam lub w jego imieniu ADMINISTRATOR Systemu Informatycznego.

Użytkownicy podczas rejestracji wyrażają dobrowolną zgodę na przetwarzanie danych osobowych w obrębie korzystania z konkretnego portalu — lista 4.
Treść oświadczenia, odpowiednia dla wybranego portalu brzmi:

UWAGA:

Oświadczam, że zgodnie z Ustawą z dnia 29.08.1997r. o ochronie danych osobowych (Dz. U. Nr 101, poz. 926), wyrażam zgodę na przetwarzanie moich danych osobowych przez Administratora danych Stowarzyszenie „MEDUCASE" z siedzibą: 54-617 Wrocław, ul. Karpacka 18A, w celach związanych z administrowaniem, korzystaniem i rejestracją w bazie użytkowników portalu pod nazwą:

→
- *czasopismo PrzypadkiMedyczne.pl* http://przypadkimedyczne.pl
- *Ogólnopolskie Forum Studentów Medycyny i Lekarzy* http://medfor.me
- *portal prawny KazusyPrawne.pl* http://kazusyprawne.pl
- *portal kongresowy chirurgów dziecięcych* http://espes2017.pl

Jednocześnie wyrażam zgodę na otrzymywanie informacji promujących portal i dotyczących usług oferowanych przez portal zgodnie z regulaminem usług świadczonych drogą elektroniczną.

PRZEPISY: Zgodnie z art. 23 ust. 1 pkt 1 ustawy, administrator danych jest uprawniony do wykorzystywania danych osobowych, jeśli osoba, której dane dotyczą wyrazi na to zgodę. Ustawa o ochronie danych osobowych precyzuje pojęcie zgody. Zgodą (art. 7 pkt 5 ustawy) jest oświadczenie woli pochodzące od osoby, której dane dotyczą, którego treścią jest zgoda na przetwarzanie danych tego, kto składa to oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być w każdym czasie odwołana.

Tworzenie konta w portalu PrzypadkiMedyczne.pl

Jak wynika to z formularza (rys. 4.1a) każdy nowy użytkownik do systemu autorskiej aplikacji portalu internetowego przesyła dane:

1. przyciskiem typu radio wybiera, czy jest to konto osobiste, czy kliniki/koła naukowego
2. podaje proponowany login, czyli nazwę użytkownika
3. precyzuje hasło. Zgodnie z polityką bezpieczeństwa musi się ono składać z minimum 6 znaków [1]
4. adres e-mail
5. imię
6. nazwisko
7. przyciskiem typu radio wybiera, czy jest studentem, czy absolwentem. **Student** z listy rozwijanej wybiera kierunek studiów, miasto uczelni i planowany rok ukończenia studiów. **Absolwent** z listy rozwijanej wybiera zawód i miasto pracy.
8. akceptuje zasady rejestracji, regulamin i wyraża zgodę na przetwarzanie danych zaznaczając check box
9. przyciska przycisk *Zarejestruj*

Tworzenie konta na pozostałych portalach

Na pozostałych portalach/stronach www funkcjonują podobne formularze i procedury. Ilustrują to screeny, rys. 4.1b, 4.2b, 4.2a, 4.3b oraz 4.3b.

5. Metody i środki uwierzytelnienia

W systemach teleinformatycznych rozróżnia się w zakresie bezpieczeństwa teleinformatycznego dwa pojęcia:

Autoryzacja — zadecydowanie, czy podmiot może uzyskać dostęp do zasobów czy nie w oparciu o mechanizmy, prawa i uprawnienia, którymi dysponuje dany system.

Uwierzytelnienie (*autentykacja*) –- sprawdzenie tożsamości podmiotu ubiegającego się o dostęp do zasobów w systemie, w sposób przewidziany dla tego systemu. Podstawowy problem bezpieczeństwa to zdolność identyfikowania, że bycie dokładnie tym, za kogo/co się podaje. Formą weryfikacji tożsamości, czyli poświadczania tożsamości jest **hasło**.
Rozróżnia się uwierzytelnianie: jednokierunkowe (dane uwierzytelniające to identyfikator użytkownika i hasło), dwukierunkowe (sekwencja klient wobec serwera, następnie lub równocześnie serwer wobec klienta) oraz uwierzytelnienie z udziałem zaufanej trzeciej strony (zaufana strona może być „lokalna" lub może to być publiczny urząd certyfikujący, możliwość wielokrotnego wykorzystania certyfikatu).

⟶ ***UWAGA:***
W systemie systemie teleinformatycznym meducase *w zakresie uwierzytelniania stosowane są metody oraz procedury zarządzania zgodne z § 5 pkt 2 rozporządzenia [2]. Użytkownik poświadcza swą tożsamość poprzez wiedzę użytkownika — login i hasło w jednokierunkowym lub dwukierunkowym uwierzytelnianiu.*

W SYSTEMIE TELEINFORMATYCZNYM MEDUCASE wyróżnia się trzy zasadnicze grupy użytkowników:

1. użytkownicy funkcyjni (administratorzy, superwaizorzy (od ang. *supervisor*)
2. użytkownik zwykły (uczestnik portalu, autor artykułu, uczestnik forum, uczestnik konkursu)

3. partycypant newslettera

Dla każdej grupy użytkowników wprowadzono inne zasady systemu uwierzytelniania.

Zasady tworzenia haseł

Czego nie powinno się robić wybierając hasła:

- stosować hasła krótsze niż 6 znaków;
- stosować znanych słów, imienia, nazwiska, numeru telefonu, daty urodzenia, numeru rejestracyjnego samochodu;
- uzależniać hasła nowego od starego;
- zapisywać hasła w łatwo dostępnym miejscu (klawiatura, monitor, szuflada);
- udostępniać komuś swojego hasła.

Jak wybierać hasło:

- wybierać kombinacje różnych znaków;
- stosować długie i mało znane słowa i frazy, np. „DataWybuchu2WojnySwiatowej1Wrzesnia1939” **lub** „*D@t@Wybuchu2WojnySwi@towej1Wrzesni@1939*”;
- wybierać losowe znaki na hasła;
- zmieniać hasła możliwie często i w sposób przypadkowy;
- zmienić hasło zawsze gdy istnieje podejrzenie poznania hasła przez kogoś .

Czym się kierować?

- przyjąć własny algorytm generowania haseł: ulubione utwory, wybrane litery ze znanych utworów lub cytatów książek ...;
- generować hasła znanymi programami do tego celu.

Użytkownicy funkcyjni

W tej grupie zasada jest prosta: użytkownik realizuje procedurę rejestracji — definiuje swój identyfikator (login), często może to być adres indywidualny e-mail oraz hasło ustalane wg zdefiniowanych reguł w danym portalu. ADMINISTRATOR DANYCH OSOBOWYCH a właściwie główny reprezentant firmy (prezes) sam nadaje odpowiednie uprawnienia i spełniane role w systemie.

Zasady regulaminowe wymagają określonej częstotliwości i metody zmiany hasła — użytkownik sam musi o tym pamiętać. Przy określaniu częstotliwości zmiany haseł uwzględnia się, iż zgodnie z pkt IV ppk 2 załącznika do rozporządzenia, hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się co najmniej z 6 znaków, jeżeli w systemie nie są przetwarzane dane, o których mowa w art. 27 ustawy lub 8 znaków, jeżeli takie dane są przetwarzane (pkt VII załącznika).

6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu (§ 5 pkt 3 rozporządzenia)

Zasady postępowania użytkowników są następujące:

1. rozpoczęcie pracy
   W celu uruchamiania systemu informatycznego, a w szczególności podczas procesu uwierzytelniania się (logowania się do systemu) podać należy login i hasło. Dane te udostępnia ADMINISTRATOR DANYCH OSOBOWYCH kierując się zasadami opisanymi w roz. 5 oraz zawartymi w tab. 6.1.

2. zawieszenie pracy
   W sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy lub w okolicznościach, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba system, po 10 minutowym czasie bezczynności użytkownika włącza się wygaszacz ekranu chroniony hasłem.

3. zakończenie pracy

→ ***UWAGA:***
Użytkownik powinien być poinstruowany o konieczności wykonania operacji wyrejestrowania się z systemu informatycznego przed wyłączeniem stacji komputerowej oraz o czynnościach, jakie w tym celu powinien wykonać.

USTAWIENIE	SW
konsola odzyskiwania: zezwalaj na automatyczne logowanie administracyjne	wyłączone
logowanie interakcyjne: liczba poprzednich zalogowań do buforu (w przypadku niedostępności kontrolera domeny)	0
logowanie interakcyjne: monituj użytkownika o zmianę hasła przed jego wygaśnięciem	14 dni
logowanie interakcyjne: nie wymagaj naciśnięcia CTRL + ALT + DEL	wyłączone
logowanie interakcyjne: nie wyświetlaj nazwy ostatniego użytkownika	włączone
logowanie interakcyjne: tekst komunikatu dla użytkowników próbujących się zalogować	*Przestrzegaj zasad opisanych w Dokumentacji bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.! oraz zasad odnoszących się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. [1]*
logowanie interakcyjne: tytuł komunikatu dla użytkowników próbujących się zalogować	*Logujesz się do* systemu teleinformatycznego meducase.
logowanie interakcyjne: wyświetlaj informacje o użytkowniku, gdy sesja jest zablokowana	Nie wyświetlaj informacji o użytkowniku
nie przetwarzaj starszej listy uruchamiania	włączone
nie przetwarzaj listy jednokrotnego uruchamiania	wyłączone
ukryj punkt wejścia do szybkiego przełączania użytkowników	włączone

Tabela 6.1: Ustawienie zasad logowania na lokalnych hostach

W sytuacji podejrzenia naruszenia bezpieczeństwa systemu np. w przypadku:

1. braku możliwości zalogowania się użytkownika na jego konto;
2. stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe.

Użytkownik zobowiązany jest natychmiast zgłosić incydent do ADMINISTRATOR DANYCH OSOBOWYCH.

7. Procedury tworzenia kopii zapasowych

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzenia)

Providerzy chroniąc nasze dane oferują:

1. firma **HostForLIFE Inc.**
   Polityka tworzenia kopii zapasowych realizowana jest w taki sposób, że każda zawartość serwera (w tym pliki klienta i pliki systemu Windows) są archiwizowane w oddzielnym systemie tworzenia kopii zapasowych każdej nocy. W przypadku braku pliku można go łatwo odzyskać. W przypadku braku plików systemu Windows lub uszkodzenia dysku można po prostu zainstalować nowy dysk i wykonać pełną renowację. Wszystko zostanie odzyskane w ciągu zaledwie 2-3 godzin.
2. firma **nazwa.pl sp. z o.o.**

   Wszystkie dane na serwerach nazwa.pl zabezpieczone są dodatkowymi kopiami bezpieczeństwa sporządzanymi na wypadek awarii systemów dyskowych. Uaktualnianie kopii odbywa się **co 24 godziny** dedykowanym łączem 10 Gbps. Dane przechowywane są na niezależnych nośnikach zlokalizowanych w zewnętrznym Centrum Danych oddalonym o kilka kilometrów od Data Center.
3. firma **H88 S.A.**

   Backupy wykonywane są automatycznie każdej nocy i przechowywane przez 7 dni w oddzielnej lokalizacji, jest to kopia przyrostowa. W każdej chwili można dokonać przywrócenia plików zgodnie z instrukcją umieszczoną w Centrum Pomocy: https://pomoc.hekko.pl/10,odzyskanie_danych.

   Kopia taka zawiera wszystkie dane, tj. pliki oraz pocztę. W przypadku chęci przywrócenia kopii zapasowej bazy można ją przywrócić zgodnie z datą, do 7 dni wstecz https://www.hekko.pl/centrum_danych.html.

8. Sposób, miejsce i okres przechowywania

Elektroniczne nośniki informacji zawierające dane osobowe

PEŁNOMOCNIK ADMINISTRATORA DANYCH OSOBOWYCH wykonuje kopie bezpieczeństwa (serwerów www oraz baz danych) na lokalnym hoście w biurze firmy. Wszelkie kopie są przegrywane na płyty DVD i przechowywane w miejscu zabezpieczonym przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem - w sejfie firmy. Kopie awaryjne bezzwłocznie są usuwane po ustaniu ich użyteczności, po wykonaniu dwóch następnych kopii bezpieczeństwa.

Kopie zapasowe, o których mowa w §5 pkt. 4 rozporządzenia

Oprogramowanie portali wymienionych w zestawieniu 1 str. 8 bazy danych oraz dane osobowe znajdują się na serwerach zewnętrznych:

1. Przypadki Medyczne, wersja polska — http://PrzypadkiMedyczne.pl zaś anglojęzyczna wersja — http://mdcase.net umieszczono pod adresem providera http://hostforlife.eu:

   Nazwa i adres firmy:
   ***HostForLIFE**, Inc.*
   12-14 Mansion House Place
   London, EC4N 8BJ
   United Kingdom

   Na serwerze pod adresami opisano:

   - http://hostforlife.eu/Privacy oraz http://hostforlife.eu/Overview — polityka prywatności;
   - http://hostforlife.eu/European-Hosting-Data-Center — polityka bezpieczeństwa;

- http://hostforlife.eu/Terms — regulamin;
- http://hostforlife.eu/ASPNET-Shared-European-Hosting-Plans — zastosowane technologie.

2. Kazusy Prawne — http://kazusyprawne.pl/, Wizytówka spółki — http://www.mdcse.com/index.php/en/ oraz Ogólnopolskie forum studentów medycyny i lekarzy — http://medfor.me/ umieszczono pod adresem providera http://nazwa.pl:

→ *Nazwa i adres firmy:*
nazwa.pl sp. z o.o.
Cystersów 20a
31-553 Kraków
Polska

Na serwerze pod adresami opisano:

- https://www.nazwa.pl/fileadmin/nazwa/Regulaminy/Pl_prywatnosci.pdf — polityka prywatności;
- https://www.nazwa.pl/fileadmin/nazwa/Regulaminy/Regulamin_uslugi_serwera.pdf — regulamin usługi serwera;
- https://www.nazwa.pl/fileadmin/nazwa/Regulaminy/Regulamin_uslugi_strona_www.pdf — regulamin usługi strona www.

3. Portal poświęcony kongresowi ESPES'2017 — http://espes2017.pl umieszczono pod adresem providera https://www.hekko.pl/:

→ *Nazwa i adres firmy:*
HEKKO.PL
H88 S.A. z siedzibą w Poznaniu
ul. Abpa A. Baraniaka 88
61-131 Poznań
Polska

Na serwerze pod adresami opisano:

- https://www.hekko.pl/polityka_prywatnosci.html — polityka prywatności;
- https://www.hekko.pl/regulamin_hosting_www.html — regulamin świadczenia usługi hostingu WWW;
- https://www.hekko.pl/regulaminy.html — regulaminy świadczenia usług.

9. Sposób zabezpieczenia systemu

Sposób zabezpieczenia systemu informatycznego przed wirusami (pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia))

Ochrona oprogramowania antywirusowego na zdalnych serwerach

Serwery zewnętrzne podlegają zabezpieczeniu teleinformatycznemu wskazanym w rozdz. 8. W zakresie ochrony antywirusowej są to aplikacje:

1. serwer firmy HostForLIFE Inc. http://hostforlife.eu/Default.aspx świadczy usługę w środowisku ASP.NET Core 1.0 Hosting w środowisku Windows Server 2016. Dane zabezpiecza: Firewall Security, Instant Daily Backup.
2. serwer firmy nazwa.pl sp. z o.o. http://nazwa.pl/. Pocztę przychodzącą skanuje oprogramowanie o nazwie ClamAV.
3. serwer firmy H88 S.A. https://www.hekko.pl/ zabezpieczają certyfikaty SSL oraz ... Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Procedura aktualizacji oprogramowania antywirusowego na lokalnych hostach

Rekomendowane minimalne funkcje oprogramowania antywirusowego:

- ochrona w czasie rzeczywistym;

- automatyczna aktualizacja definicji i sygnatur;
- zaplanowane codzienne skanowanie systemu Windows 7 pod kątem złośliwego oprogramowania i wirusów.

Ochrona antywirusowa wymaga aktualizacji przebiegającej na dwóch poziomach:

1. upgrade wersji oprogramowania;
2. aktualizacja bazy wzorców (sygnatur) wirusów.

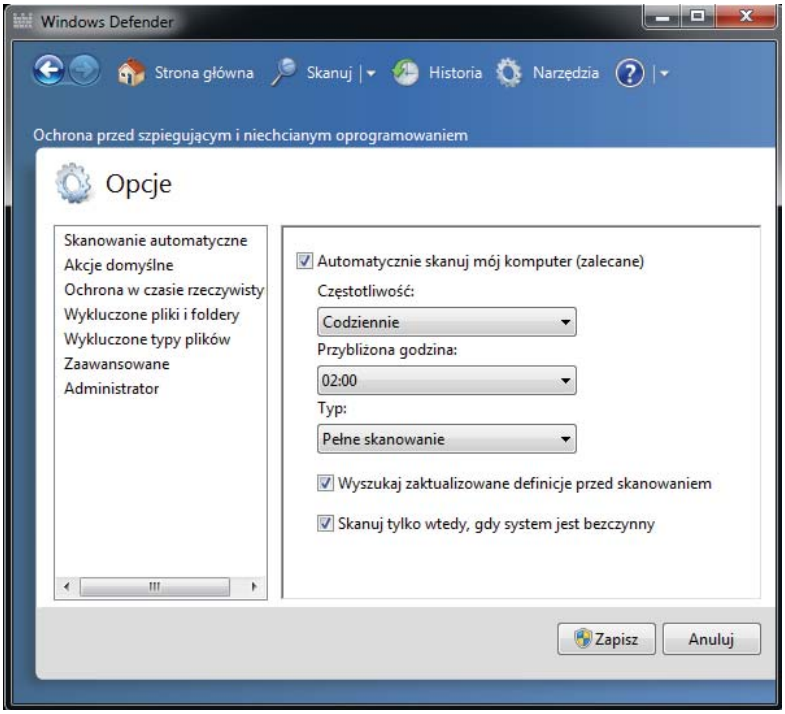
Defender

Usługa Windows Defender jest oprogramowaniem antyszpiegowskim dołączonym do systemu Windows 7 i uruchamianym automatycznie po włączeniu systemu. Używanie oprogramowania antyszpiegowskiego może pomóc w zapewnieniu ochrony komputera przed programami szpiegującymi i innymi potencjalnie niechcianymi aplikacjami. Program szpiegujący może zostać zainstalowany na komputerze bez wiedzy użytkownika podczas każdego połączenia z Internetem, a ponadto komputer może zostać nim zainfekowany podczas instalowania niektórych programów przy użyciu nośników wymiennych. Usługa Windows Defender oferuje dwa sposoby ochrony komputera przed zainfekowaniem programami szpiegującymi:

- Ochrona w czasie rzeczywistym. Usługa Windows Defender alarmuje użytkownika w przypadku próby zainstalowania lub uruchomienia programu szpiegującego na komputerze. Użytkownik jest powiadamiany również wówczas, gdy programy próbują zmieniać ważne ustawienia systemu Windows.
- Opcje skanowania. Przy użyciu usługi Windows Defender można skanować komputer w poszukiwaniu programów szpiegujących, które mogły zostać zainstalowane na komputerze. Można także ustalać harmonogram regularnego skanowania oraz automatycznie usuwać dowolne elementy wykryte podczas skanowania.

Aby zweryfikować ustawienia lub ustawić rekomendowane ustawienia Windows Defender należy:

1. kliknąć przycisk Start, wpisać w oknie „*Wyszukaj programy i pliki*": **Windows Defender**, a następnie kliknij polecenie **Windows Defender**.
2. następnie należy wybrać pozycję **Narzędzia**, następnie **Opcje** i ustawić rekomendowane ustawienia (przedstawione na rys. 9.1) i kliknąć przycisk **OK**. Do potwierdzenia wyboru może być wymagane podanie hasła administratora.



Rys. 9.1: Widok okna ustawień rekomendowanych dla usługi Windows Defender

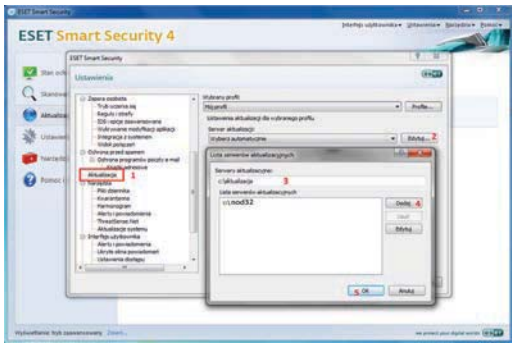
ESET NOD32

Samo jądro (motor) programu bardzo rzadko jest aktualizowany. Zawsze, nawet starsze wersje oprogramowania współpracują z zaczytywanymi wzorcami wirusów, a właśnie ich aktualizacja jest najistotniejsza, nie wersja programu. Jeśli jednak producent publikuje nową wersję, sygnalizując o wprowadzeniu nowych funkcji, o skuteczniejszym działaniu programu, ADMIN program aktualizuje, oraz:

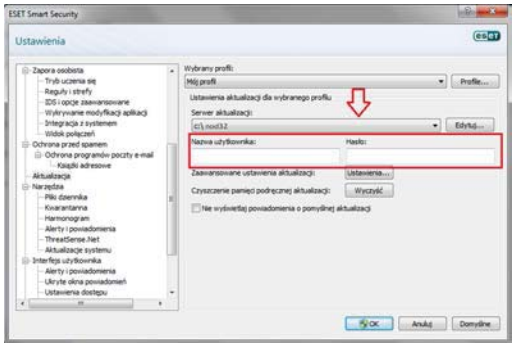
1. zaznajamia się z nową wersją programu, analizuje nowe funkcje, wymagania systemowe;
2. ze strony producenta (http://www.eset.pl/Pobierz/pelne) pobiera aktualną (sprawdzoną, bezpieczną) wersję oprogramowania i zapisuje ją na zarejestrowany pendrive;
3. przenosi pobrane oprogramowanie z pendrive do tymczasowego katalogu np. na dysku D:\,
4. w bieżącym systemie odinstalowuje istniejącą (dotychczasową) wersję programu;
5. instaluje aktualną wersję programu NOD32.

Aktualizacja sygnatur wirusów

Sygnatury wirusów można zaktualizować automatycznie korzystając z sieci Internet lub bez podłączenia komputera do sieci, stosując podawane przez producenta aktualne procedury.



(a) ustawienie katalogu aktualizacji



(b) źródło lokalnej aktualizacji

Rys. 9.2: Ustawienia aktualizacji w programie NOD32

10. Udostępnienia danych odbiorcom

Dane osobowe w SYSTEMIE TELEINFORMATYCZNYM MEDUCASE nie są udostępniane poza ten system. Dane te są wykorzystywane tylko w ramach funkcjonujących w systemie aplikacji. W wypadku szczególnym dane te mogą być udostępnione i wówczas „[...] administrator danych nie musi informować osoby, której dane dotyczą, o udostępnieniu jej danych podmiotom, które nie zostały zaliczone do kategorii odbiorców danych (sąd, komornik, prokuratura, ...), ani odnotowywać faktu udostępnienia danych tym podmiotom" [7].

11. Procedury wykonywania przeglądów i konserwacji

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji

Konserwacja sprzętu i danych informatycznych spoczywa głównie na firmach hostingujących. Wybrane zostały podmioty gwarantujące blisko 100% bezpieczeństwo. Po stronie hostów lokalnych istnieje znikoma możliwość uszkodzenia, utracenia lub modyfikacji danych. Ocena ta wynika z:

- minimalnej ilości osób mających dostęp do danych na serwerach zewnętrznych;
- stałej aktualizacji systemów operacyjnych i antywirusowych na trzech hostach lokalnych;
- stałej dbałości o sprawność lokalnego sprzętu komputerowego.

Literatura

[1] Sejm RP Min. Spraw Wewnętrznych i Administracji. 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, Dz.U. 2004 nr 100 poz. 1024. [online], April 2004.

[2] Sejm RP Min. Spraw Wewnętrznych i Administracji. Internetowy System Aktów Prawnych, Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. 2014, poz. 1182 ze zm.). [online], December 1997.

[3] Urząd Ochrony Danych Osobowych. xx. [online], 2015.

[4] Dyrektywia 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Dziennik Urzędowy L 281 , 23/11/1995 P. 0031 - 0050. [online], October 1995.

[5] U S T A W A z dnia 10 maja 2018 r. o ochronie danych osobowych. [online], May 2018.

[6] Fakturownia. [online], September 2015.

[7] Barta J., Markiewicz R., and Fajgielski P. *Ochrona danych osobowych. Komentarz*. Wolters Kluwer, 2011.

Spis rysunków

Spis tabel

Dodatki

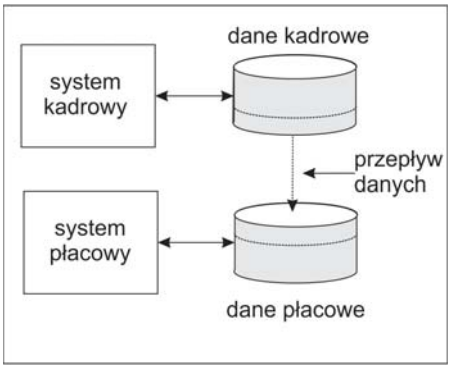
Zał. nr 1 Wykaz pomieszczeń

Wykaz pomieszczeń w których przetwarzane są dane osobowe				
L.p.	**Lokalizacja adres**	**Precyzyjne określenie pomieszczenia**	**Dział/osoba użytkująca pomieszczenie**	**Zabezpieczenie pomieszczenia**
1.	ul. Karpacka 18A; 54-617 Wrocław	przyziemie, pomieszczenie biurowe dedykowane na działalność	Wiesław Palczewski — pełnomocnik ADO	od zewnątrz: podwójne drzwi witrynowe z sygnalizacją alarmową otwarcia, w pomieszczeniu system alarmowy
2.	ul. Na Polance 22/17; 51-109 Wrocław	mieszkanie prywatne prezesa spółki	Mateusz Palczewski — prezes	drzwi wyposażone w zamek patentowy GERDA

Tabela 1: Wykaz pomieszczeń w których przetwarzane są dane osobowe

Zał. nr 2 Wykaz zbiorów danych osobowych

Polityka bezpieczeństwa identyfikuje zbiory danych osobowych oraz systemy informatyczne używane do ich przetwarzania.



Rys. 1: Model współpracy systemów informatycznych ze zbiorami danych — dwa oddzielne systemy (moduły programowe) przetwarzają dane zawarte w dwóch zbiorach pomiędzy którymi występuje przepływ danych

1. Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane są dane osobowe

   Nazwa systemu (dokładniej solucji): ZINTEGROWANY INTERNETOWY SYSTEM PORTALI MEDUCASE,
   opis: aplikacja internetowa udostępniająca treści zintegrowanym portalom, składająca się z 3 systemów:

   - baza danych
   - część serwerowa – API
   - część kliencka

2. Jak dane wprowadzane są do systemu?

   PrzypadkiMedyczne to złożona aplikacja internetowa przechowująca wiele informacji. Najważniejsze z nich zostały opisane poniżej (pełny zbiór wymagań został opisany w specyfikacji projektu):

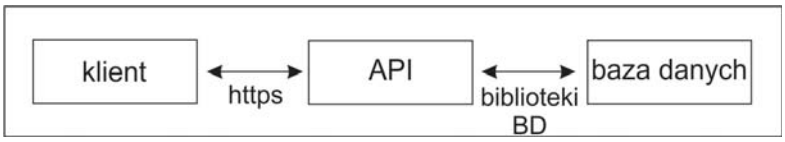
   - Użytkownicy/konta/role
   - Artykuły
   - Komentarze
   - Artykuły czasopisma
   - Newsletter

Wykaz zbiorów danych osobowych					
L.p.	**Nazwa zbioru danych osobowych**	**Cel przetwarzania**	**Nazwa systemu, ewidencji lub aplikacji, w której przetwarzane sa dane osobowe**	**Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania miedzy nimi**	**Sposób przepływu danych pomiędzy poszczególnymi systemami**
1.	zbiór danych pracowników i współpracowników	realizacja obowiązków związanych z zatrudnieniem pracowników, podpisywaniem umów z innymi podmiotami	**a)** program o nazwie *Rewizor GT* **b)** program o nazwie *Super Księga Podatkowa* (SKP) **c)** program o nazwie *Płatnik* (ZUS) **d)** kartoteka z umowami	imię, nazwisko, adres, NIP, Regon	dane z papierowej dokumentacji (kartoteki) sa „ręcznie" wprowadzane do użytkowanych programów
2.	zbiór danych użytkowników serwisów	umożliwienie funkcjonowania serwisów specjalistyczno-edukacyjnych: 1. http://przypadkimedyczne.pl 2. http://medfor.me 3. http://kazusyprawne.pl 4. http://espes2017.pl	**a)** użytkownicy zarejestrowani za pośrednictwem serwisu „przypadkimedyczne.pl" **b)** użytkownicy zarejestrowani za pośrednictwem serwisu „medfor.me" **c)** użytkownicy zarejestrowani za pośrednictwem serwisu „kazusyprawne.pl"	imię, nazwisko, login, adres zamieszkania, adres poczty email, zawód, wykształcenie, miejsce pracy, login/identyfikator	xxxxx

Tabela 2: Wykaz zbiorów danych osobowych

- Subskrypcje
- Bandery
- Filtry
- I18n
- L10n
- Quizy
- Testy
- Wyszukiwarka
- Menu
- Dostęp Premium
- PMki, KzP

3. czy są tworzone kartoteki drukowane, czy system umożliwia taki eksport?
   Brak funkcjonalności
4. Sposób przepływu danych pomiędzy systemami
   Przepływ danych między systemami przedstawiony na schemacie poniżej:



5. czy jest przepływ danych (czy np. jest przewidywany) pomiędzy systemami składowymi
   Przepływ danych został opisany w punkcie 4. Dowolny klient, który otrzyma uprawnienia może mieć dostęp do określonych części aplikacji (w zależności od przypisanej roli).
6. Krótki opis struktury zbiorów danych (parę zdań) np. czy są sql_owe tabele ze zbiorami danych osobowych, jak się nazywają
   Magazyn danych oparty o silnik MSSQL. Dane osobowe są magazynowane w tabelach o strukturze charakterystycznej dla technologii .NET Identity, a także rozszerzone o dodatkowe tabele. Poniżej informacje dotyczące tabel zawierające dane nt. kont użytkowników aplikacji PM:

Listing 1: PM_auth_schema.sql

```
CREATE TABLE [dbo].[AspNetRoles](
    [Id] [nvarchar](128) NOT NULL,
    [Name] [nvarchar](256) NOT NULL,
CONSTRAINT [PK_dbo.AspNetRoles] PRIMARY KEY CLUSTERED
(
    [Id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]

CREATE TABLE [dbo].[AspNetUserClaims](
    [Id] [int] IDENTITY(1,1) NOT NULL,
    [UserId] [nvarchar](128) NOT NULL,
    [ClaimType] [nvarchar](max) NULL,
    [ClaimValue] [nvarchar](max) NULL,
CONSTRAINT [PK_dbo.AspNetUserClaims] PRIMARY KEY CLUSTERED
(
    [Id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

CREATE TABLE [dbo].[AspNetUserLogins](
    [LoginProvider] [nvarchar](128) NOT NULL,
    [ProviderKey] [nvarchar](128) NOT NULL,
    [UserId] [nvarchar](128) NOT NULL,
CONSTRAINT [PK_dbo.AspNetUserLogins] PRIMARY KEY CLUSTERED
(
    [LoginProvider] ASC,
    [ProviderKey] ASC,
    [UserId] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]

CREATE TABLE [dbo].[AspNetUserRoles](
    [UserId] [nvarchar](128) NOT NULL,
    [RoleId] [nvarchar](128) NOT NULL,
CONSTRAINT [PK_dbo.AspNetUserRoles] PRIMARY KEY CLUSTERED
(
    [UserId] ASC,
    [RoleId] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]

CREATE TABLE [dbo].[AspNetUsers](
    [Id] [nvarchar](128) NOT NULL,
    [Email] [nvarchar](256) NULL,
    [EmailConfirmed] [bit] NOT NULL,
    [PasswordHash] [nvarchar](max) NULL,
    [SecurityStamp] [nvarchar](max) NULL,
    [PhoneNumber] [nvarchar](max) NULL,
    [PhoneNumberConfirmed] [bit] NOT NULL,
    [TwoFactorEnabled] [bit] NOT NULL,
    [LockoutEndDateUtc] [datetime] NULL,
    [LockoutEnabled] [bit] NOT NULL,
    [AccessFailedCount] [int] NOT NULL,
    [UserName] [nvarchar](256) NOT NULL,
```

```
    [ClinicAccount_Id] [int] NULL,
    [IndividualAccount_Id] [int] NULL,
    [Image] [nvarchar](max) NULL,
    [Newsletter] [bit] NOT NULL DEFAULT ((0)),
    [Language] [nvarchar](max) NULL,
CONSTRAINT [PK_dbo.AspNetUsers] PRIMARY KEY CLUSTERED
(
    [Id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

CREATE TABLE [dbo].[ClinicAccounts](
    [Id] [int] IDENTITY(1,1) NOT NULL,
    [ClinicFullName] [nvarchar](max) NULL,
    [Manager] [nvarchar](max) NULL,
    [Authros] [nvarchar](max) NULL,
    [ClinicCity] [nvarchar](max) NULL,
    [Www] [nvarchar](max) NULL,
    [Phone] [nvarchar](max) NULL,
    [ClinicCreated] [int] NULL,
CONSTRAINT [PK_dbo.ClinicAccounts] PRIMARY KEY CLUSTERED
(
    [Id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

CREATE TABLE [dbo].[GraduateAccounts](
    [Id] [int] IDENTITY(1,1) NOT NULL,
    [PWZ] [int] NOT NULL,
    [WorkCity] [nvarchar](max) NULL,
    [ProfessionId] [int] NULL,
    [GraduationYear] [int] NOT NULL DEFAULT ((0)),
CONSTRAINT [PK_dbo.GraduateAccounts] PRIMARY KEY CLUSTERED
(
    [Id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

CREATE TABLE [dbo].[IndividualAccounts](
    [Id] [int] IDENTITY(1,1) NOT NULL,
    [IsStudent] [bit] NOT NULL,
    [AboutMe] [nvarchar](max) NULL,
    [GraduateId] [int] NULL,
    [StudentId] [int] NULL,
CONSTRAINT [PK_dbo.IndividualAccounts] PRIMARY KEY CLUSTERED
(
    [Id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

CREATE TABLE [dbo].[StudentAccounts](
    [Id] [int] IDENTITY(1,1) NOT NULL,
    [SchoolCity] [nvarchar](max) NULL,
    [GraduationPlannedYear] [int] NOT NULL,
    [FacultyId] [int] NULL,
CONSTRAINT [PK_dbo.StudentAccounts] PRIMARY KEY CLUSTERED
(
    [Id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
```

) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]

Zał. nr 3 Upoważnienie do przetwarzania danych

Załącznik nr 3 do Polityki Bezpieczeństwa

Upoważnienie do przetwarzania danych osobowych

Data nadania upoważnienia: .... 25.11.2015 r. ....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Pana Mateusza Palczewskiego
   o numerze PESEL 87022613917
   zatrudnionego na stanowisku prezes firmy
   w Meducase Sp. z o.o.

   do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
   (*należy określić zbiory zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa*)
   – cała baza danych
2. Identyfikator/Login: **mpalczewski**
3. Okres trwania upoważnienia: do 2020 r.

   MEDUCASE sp. z o. o.
   ul. Karpacka 18A, 54-617 Wrocław, Polska
   www.mdcse.com | contact@mdcse.com
   REGON: 362777567 NIP: 8943067789 KRS: 0000581184

   Wystawił: .....
   (*podpis w imieniu Administratora Danych Osobowych*)
4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

25.11.2015 r. Mateusz Palczewski

Data i podpis osoby upoważnionej: .....

Załącznik nr 3 do Polityki Bezpieczeństwa

Upoważnienie do przetwarzania danych osobowych

Data nadania upoważnienia: .... 25.11.2015 r. ....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Pana Mateusza Stolarza
   o numerze PESEL .....
   zatrudnionego na stanowisku viceprezes Spółki
   w Meducase Sp. z o.o.

   do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
   (*należy określić zbiory zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa*)

   – .....

   – .....

2. Identyfikator/Login:
3. Okres trwania upoważnienia: do 2020 r.

MEDUCASE sp. z o. o.
ul. Karpacka 18A, 54-617 Wrocław, Polska
www.mdcse.com | contact@mdcse.com
REGON: 362777567 NIP: 8943067789 KRS: 0000581184

Wystawił: .....
(*podpis w imieniu Administratora Danych Osobowych*)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Załącznik nr 3 do Polityki Bezpieczeństwa

Upoważnienie do przetwarzania danych osobowych

Data nadania upoważnienia: .... 25.11.2015 r. ....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Pana Tomasza Leśniaka
   o numerze PESEL 79100814451
   zatrudnionego na stanowisku prokurent
   w Meducase Sp. z o.o.

   do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
   (*należy określić zbiory zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa*)

   – cała baza danych

2. Identyfikator/Login:
3. Okres trwania upoważnienia: do 2020 r.

MEDUCASE sp. z o. o.
ul. Karpacka 18A, 54-617 Wrocław, Polska
www.mdcse.com | contact@mdcse.com
REGON: 362777567 NIP: 8943067789 KRS: 0000581184

Wystawił: .....
(*podpis w imieniu Administratora Danych Osobowych*)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: 25.11.2015r. .....

Załącznik nr 3 do Polityki Bezpieczeństwa

Upoważnienie do przetwarzania danych osobowych

Data nadania upoważnienia: .... 25.11.2015 r. ....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Pana Wiesława Palczewskiego
   o numerze PESEL 52070105794
   zatrudnionego na stanowisku viceprezes firmy
   w Meducase Sp. z o.o.

   do dostępu do następujących zbiorów danych osobowych w celu ich przetwarzania:
   (*należy określić zbiory zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa*)

   – do wszystkich zbiorów danych

2. Identyfikator/Login:
3. Okres trwania upoważnienia: do 2020 r.

MEDUCASE sp. z o. o.
ul. Karpacka 18A, 54-617 Wrocław, Polska
www.mdcse.com | contact@mdcse.com
REGON: 362777567 NIP: 8943067789 KRS: 0000581184

Wystawił: .....
(*podpis w imieniu Administratora Danych Osobowych*)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: 25.11.2015 .....

Zał. nr 4 Oświadczenie

Załącznik nr 4 do Polityki Bezpieczeństwa — Oświadczenie

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Meducase Sp. z o.o.
Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.
Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 z poźn.zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

09.08.2016

Mateusz Palczewski
MEDUCASE sp. z o. o.
Prezes zarządu

. . . . . .

(*data i podpis osoby oświadczającej*)
Mateusz Palczewski

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Meducase Sp. z o.o.
Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.
Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 z poźn.zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

Wiesław Palczewski
MEDUCASE sp. z o. o.
Wiceprezes zarządu

25.11.2015 r. .....

(*data i podpis osoby oświadczającej*)
Wiesław Palczewski

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Meducase Sp. z o.o.
Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.
Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 z poźn.zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

25.11.2015r. Leśniak

.....

(*data i podpis osoby oświadczającej*)
Tomasz Leśniak

OŚWIADCZENIE

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Meducase Sp. z o.o.
Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.
Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 z poźn.zm.), w tym z zasadami odpowiedzialności karnej określonymi w rozdziale 8 wyżej wymienionej ustawy.

. . . . . .
(*data i podpis osoby oświadczającej*)
Mateusz Stolarz

Zał. nr 5 Upoważnienie

Wrocław, 26.11.2015 r.

Załącznik nr 5 do Polityki Bezpieczeństwa

Upoważnienie dla Pełnomocnika ds. danych osobowych

UPOWAŻNIENIE DLA PEŁNOMOCNIKA DS. DANYCH OSOBOWYCH W MEDUCASE SP. Z O.O.

Ja, niżej podpisany Mateusz Palczewski jako osoba wykonująca funkcję Administratora Danych Osobowych niniejszym upoważniam do sprawowania funkcji Pełnomocnika ds. danych osobowych Pana dr Wiesława Palczewskiego posługującego się numerem PESEL: 52070105794.
Do obowiązków Pełnomocnika ds. danych osobowych będzie należało wdrożenie i nadzór nad prawidłową realizacją Polityki Bezpieczeństwa obowiązującej w jednostce organizacyjnej, w szczególności:

1. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
2. Zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym lub zabraniem przez osobę nieuprawnioną.
3. Zabezpieczenie danych przed ich przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki techniczne służące ich zabezpieczeniu.
5. Wyznaczanie Administratora Systemu Informatycznego (ASI).
6. Nadawanie upoważnienia do przetwarzania danych osobowych.

Mateusz Palczewski

Mateusz Palczewski
MEDUCASE sp. z o.o.
Prezes zarządu

.....

(*podpis w imieniu Administratora Danych Osobowych*)

Ja, niżej podpisany, zobowiązuję się do pełnienia obowiązków Pełnomocnika ds. danych osobowych w oparciu o przepisy wewnętrzne obowiązujące w jednostce organizacyjnej, ustawę o ochronie danych osobowych oraz rozporządzenie wydane na podstawie art. 39a do wyżej wymienionej ustawy.

25.11.2015

.....

(*podpis osoby przyjmującej funkcję Pełnomocnika ds. danych osobowych*)

Zał. nr 6 Ewidencja osób upoważnionych do przetwarzania danych osobowych

Tabela 3: Ewidencja osób upoważnionych do przetwarzania danych osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych						
L.p.	Imię i nazwisko	Stanowisko / komórka organizacyjna	Zakres	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator / Login w danym systemie informatycznym
1.	Mateusz Palczewski	prezes MEDUCASE Sp. z o.o., główny reprezentant ADMINISTRATORA DANYCH OSOBOWYCH	wszystkie bazy i dane	25.11.2015	do odwołania	eMCe71
2.	Marcin Roczek	programista MEDUCASE Sp. z o.o., ADMINISTRATOR Systemu Informatycznego	wszystkie bazy i dane (pełen dostęp)	25.11.2015	do odwołania	strzyzyk
3.	Wiesław Palczewski	vice-prezes MEDUCASE Sp. z o.o., PEŁNOMOCNIK ADMINISTRATORA DANYCH OSOBOWYCH	wszystkie bazy i dane www.espes2017.pl, dostęp na żądanie do pozostałych zasobów;	25.11.2015	do odwołania	Wiesław Palczewski
4.	Tomasz Leśniak	vice-prezes MEDUCASE Sp. z o.o., koordynator spraw prawnych	wszystkie bazy i dane (bez możliwości zmian konfiguracyjnych i bez możliwości usunięcia głównego administratora)	25.11.2015	do odwołania	lex
5.	Mateusz Malik	koordynator konkursu „Rentgen w oczach”, redaktor MedFor.me MEDUCASE Sp. z o.o.	dane użytkowników	25.11.2015	do odwołania	newman

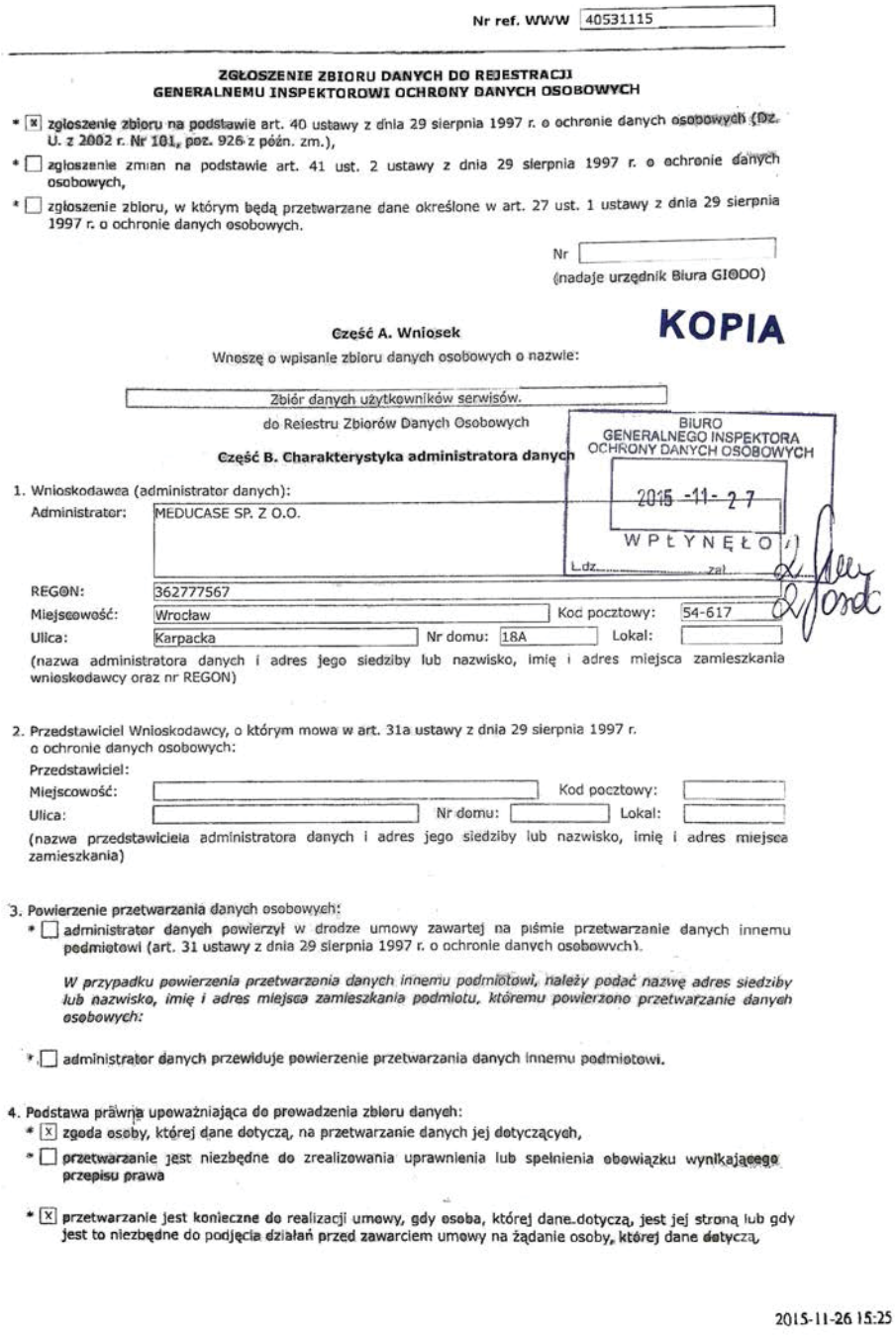
kontynuacja na następnej stronie

Tabela 3 – ciąg dalszy tabeli ze strony poprzedniej

L.p.	Imię i nazwisko	Stanowisko / komórka organizacyjna	Zakres	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator / Login w danym systemie informatycznym
6.	Łukasz Czyż	administrator (bez możliwości zmian konfiguracyjnych i bez możliwości usunięcia konta głównego administratora) KazusyPrawne.pl	dane użytkowników	25.11.2015	do odwołania	Alter Ego

Źródło: określenie, do jakich zbiorów dana osoba ma dostęp, zgodnie z załącznikiem Nr2 - rozdz. 11 do Polityki Bezpieczeństwa

Zał. nr 7 Zgłoszenie zbioru danych do rejestracji GIODO



Nr ref. WWW 40531115

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

* [x] zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
* [ ] zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
* [ ] zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Nr
(nadaje urzędnik Biura GIODO)

KOPIA

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

Zbiór danych użytkowników serwisów.

do Rejestru Zbiorów Danych Osobowych

BIURO GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH
2015 -11- 27
WPŁYNĘŁO
L.dz. zał.

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych):

Administrator: MEDUCASE SP. Z O.O.

REGON: 362777567

Miejscowość: Wrocław Kod pocztowy: 54-617

Ulica: Karpacka Nr domu: 18A Lokal:

(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel Wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:

Przedstawiciel:

Miejscowość: Kod pocztowy:

Ulica: Nr domu: Lokal:

(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:

* [ ] administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych).

W przypadku powierzenia przetwarzania danych innemu podmiotowi, należy podać nazwę adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:

* [ ] administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:

* [x] zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,
* [ ] przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego przepisu prawa
* [x] 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,

2015-11-26 15:25

Polityka Bezpieczeństwa w „MEDUCASE”

Część I – Wstęp

§ 1

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 z późn. zm.), zwanej dalej „ustawą” oraz z § 3 ust. 1 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. z 2004 r. Nr 100, poz. 1024), zwanego dalej „rozporządzeniem”, ustanawia się „Politykę Bezpieczeństwa”.

§ 2

Ilekroć w niniejszym dokumencie jest mowa o jednostce organizacyjnej, należy przez to rozumieć Meducase Sp. z o.o., posługującą się numerem REGON: 362777567 oraz NIP: 8943067789, wpisaną do KRS pod numerem: 581184, jako Administratora Danych Osobowych.

Część II – Zasady przetwarzania i ochrony danych osobowych

§ 1

Każda osoba, mająca dostęp do danych osobowych przetwarzanych w jednostce organizacyjnej jest zobowiązana do zapoznania się z niniejszym dokumentem.

§ 2

Wymagany przez rozporządzenie wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe (zwany dalej „obszarem przetwarzania") stanowi załącznik nr 1 do niniejszego dokumentu.

§ 3

Wymagany przez rozporządzenie 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 oraz sposób przepływu danych pomiędzy poszczególnymi systemami, stanowi załącznik nr 2 do niniejszego dokumentu.

§ 4

Osoby, które przetwarzają w jednostce organizacyjnej dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (załącznik nr 3 do niniejszego dokumentu, roz. 11) oraz podpisać oświadczenie o zachowaniu poufności tych danych (załącznik nr 4 do niniejszego dokumentu, roz. 11).

§ 5

Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych posiada swój identyfikator oraz hasło, pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło, określone zostały w części II § 2 Instrukcji Zarządzania Systemem Informatycznym.

§ 6

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w § 4 (załącznik nr 3 do niniejszego dokumentu), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności (załącznik nr 4 do niniejszego dokumentu), chyba że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.

§ 7

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 31 ustawy.

§ 8

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności właściwie umotywowany wniosek podmiotu uprawnionego.

§ 9

Dokumenty zawierające dane osobowe przechowywane w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w szafach zamykanych na klucz.

W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się poprzez pocięcie w niszczarce.

§ 10

Zasady przetwarzania danych osobowych w systemie informatycznym określone są w „*Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Meducase Sp. z o.o.*"

§ 11

Nadzór nad przetwarzaniem danych osobowych w jednostce organizacyjnej sprawuje prezes zarządu, który może wyznaczyć pełnomocnika ds. danych osobowych do którego zadań będzie należało bezpośrednie nadzorowanie stanu realizacji procedur związanych z ochroną danych osobowych, a w razie potrzeby także bezpośrednia realizacja procedur w imieniu prezesa zarządu. Upoważnienie dla pełnomocnika ds. danych osobowych stanowi załącznik nr 5 do niniejszego dokumentu. W przypadku wyznaczenia Pełnomocnika ds. danych osobowych należy do niego odnosić obowiązki przewidziane w paragrafach następujących dla osoby nadzorującej przetwarzanie danych.

§ 12

Osoba nadzorująca przetwarzanie danych prowadzi wykaz zbiorów danych osobowych przetwarzanych w jednostce organizacyjnej (załącznik nr 2 do niniejszego dokumentu) oraz, kiedy jest to wymagane przez przepisy, zgłasza zbiory do rejestracji do GIODO. W ramach nadzoru nad przetwarzaniem danych, osoba ta sprawdza w szczególności cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia danych osobowych. Upoważnienie do przetwarzania danych osobowych (załącznik nr 3 do niniejszego dokumentu) nadaje osoba nadzorująca przetwarzanie danych, która jest także zobowiązana do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w jednostce organizacyjnej.

§ 13

Osoba nadzorująca przetwarzanie danych prowadzi również następujące wykazy:

a) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych (załącznik nr 6 do niniejszego dokumentu)

b) wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania (załącznik nr 1 do niniejszego dokumentu)

c) wykaz podmiotów i osób, którym udostępniono dane (załączniki nr 7 i nr 9 do niniejszego dokumentu)

d) wykaz podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy (załącznik nr 8 do niniejszego dokumentu)

§ 14

Osoby upoważnione do przetwarzania danych mają obowiązek:

a) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem

b) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym

c) zabezpieczać je przed zniszczeniem

§ 15

W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, osoba wyznaczona przez osobę nadzorującą przetwarzanie danych przygotowuje odpowiedź w ciągu 30 dni.

§ 16

W przypadku zbierania danych osobowych od osoby, której one dotyczą, jest ona informowana w przystępnej dla niej formie o:

a) adresie siedziby i pełnej nazwie,

b) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

c) prawie dostępu do treści swoich danych oraz ich poprawiania,

d) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Część III – Postanowienia końcowe

§ 1

Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 49-54a ustawy o ochronie danych osobowych.

§ 2

W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych 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.

§ 3

Niniejszy dokument wchodzi w życie z dniem 26 listopada 2015 roku.

Mateusz Palczewski - Mateusz Palczews
MEDUCASE sp. z o.
Prezes zarządu

(*podpis w imieniu spółki*)

Ciasteczka

1. Serwis nie zbiera w sposób automatyczny żadnych informacji, z wyjątkiem informacji zawartych w plikach cookies.
2. Pliki cookies (tzw. „ciasteczka") stanowią dane informatyczne, w szczególności pliki tekstowe, które przechowywane są w urządzeniu końcowym Użytkownika Serwisu i przeznaczone są do korzystania ze stron internetowych Serwisu. Cookies zazwyczaj zawierają nazwę strony internetowej, z której pochodzą, czas przechowywania ich na urządzeniu końcowym oraz unikalny numer.
3. Podmiotem zamieszczającym na urządzeniu końcowym Użytkownika Serwisu pliki cookies oraz uzyskującym do nich dostęp jest operator Serwisu.
4. Pliki cookies wykorzystywane są w celu:
   (a) dostosowania zawartości stron internetowych Serwisu do preferencji Użytkownika oraz optymalizacji korzystania ze stron internetowych; w szczególności pliki te pozwalają rozpoznać urządzenie Użytkownika Serwisu i odpowiednio wyświetlić stronę internetową, dostosowaną do jego indywidualnych potrzeb;
   (b) tworzenia statystyk, które pomagają zrozumieć, w jaki sposób Użytkownicy Serwisu korzystają ze stron internetowych, co umożliwia ulepszanie ich struktury i zawartości;
   (c) utrzymanie sesji Użytkownika Serwisu (po zalogowaniu), dzięki której Użytkownik nie musi na każdej podstronie Serwisu ponownie wpisywać loginu i hasła;
5. W ramach Serwisu stosowane są następujące rodzaje plików cookies:

(a) „niezbędne" pliki cookies, umożliwiające korzystanie z usług dostępnych w ramach Serwisu, np. uwierzytelniające pliki cookies wykorzystywane do usług wymagających uwierzytelniania w ramach Serwisu;

(b) pliki cookies służące do zapewnienia bezpieczeństwa, np. wykorzystywane do wykrywania nadużyć w zakresie uwierzytelniania w ramach Serwisu;

(c) „wydajnościowe" pliki cookies, umożliwiające zbieranie informacji o sposobie korzystania ze stron internetowych Serwisu;

(d) „funkcjonalne" pliki cookies, umożliwiające „zapamiętanie" wybranych przez Użytkownika ustawień i personalizację interfejsu Użytkownika, np. w zakresie wybranego języka lub regionu, z którego pochodzi Użytkownik, rozmiaru czcionki, wyglądu strony internetowej itp.;

6. „reklamowe" pliki cookies, umożliwiające dostarczanie Użytkownikom treści reklamowych bardziej dostosowanych do ich zainteresowań.

7. W wielu przypadkach oprogramowanie służące do przeglądania stron internetowych (przeglądarka internetowa) domyślnie dopuszcza przechowywanie plików cookies w urządzeniu końcowym Użytkownika. Użytkownicy Serwisu mogą dokonać w każdym czasie zmiany ustawień dotyczących plików cookies. Ustawienia te mogą zostać zmienione w szczególności w taki sposób, aby blokować automatyczną obsługę plików cookies w ustawieniach przeglądarki internetowej bądź informować o ich każdorazowym zamieszczeniu w urządzeniu Użytkownika Serwisu. Szczegółowe informacje o możliwości i sposobach obsługi plików cookies dostępne są w ustawieniach oprogramowania (przeglądarki internetowej).

8. Operator Serwisu informuje, że ograniczenia stosowania plików cookies mogą wpłynąć na niektóre funkcjonalności dostępne na stronach internetowych Serwisu.

9. Pliki cookies zamieszczane w urządzeniu końcowym Użytkownika Serwisu i wykorzystywane mogą być również przez współpracujących z operatorem Serwisu reklamodawców oraz partnerów.

10. Więcej informacji na temat plików cookies znajdziesz pod adresem http://wszystkooociasteczkach.pl/ lub w sekcji „Pomoc" w menu przeglądarki internetowej.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w „MEDUCASE"

I – Część ogólna

§ 1

Zgodnie z art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 z późn. zm.) oraz z § 3 ust. 1 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. z 2004 r. Nr 100, poz. 1024), ustanawia się „Dokumentację bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.".

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:

a) ustawie — należy przez to rozumieć ustawę, o której mowa w § 1 niniejszej części

b) rozporządzeniu — należy przez to rozumieć rozporządzenie, o którym mowa w § 1 niniejszej części

c) jednostce organizacyjnej — należy przez to rozumieć Meducase Sp. z o.o., posługującą się numerem KRS: 581184, jako Administratora Danych Osobowych (ADO) reprezentowanego przez zarząd.

d) ASI – należy przez to rozumieć Administratora Systemu Informatycznego w rozumieniu § 3 niniejszej części

e) Instrukcji — należy przez to rozumieć niniejszy dokument

f) Polityce Bezpieczeństwa — należy przez to rozumieć przyjęty do stosowania w jednostce organizacyjnej dokument zatytułowany: „*Polityka Bezpieczeństwa w Meducase Sp. z o.o.*"

g) użytkowniku – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym w drodze upoważnienia, o jakim mowa w części II § 4 Polityki Bezpieczeństwa.

h) systemie informatycznym — należy przez to rozumieć system informatyczny, w którym przetwarzane są dane osobowe w jednostce organizacyjnej

§ 3

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO wyznaczany jest przez ADMINISTRATORA DANYCH OSOBOWYCH drogą pisemnego upoważnienia. Wzór upoważnienia ADMINISTRATORA SYSTEMU INFORMATYCZNEGO stanowi załącznik nr 1 do niniejszego dokumentu. ADMINISTRATOR SYSTEMU INFORMATYCZNEGO jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 do Polityki Bezpieczeństwa.

§ 4

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu. Do obowiązków ADMINISTRATORA SYSTEMU INFORMATYCZNEGO należy także kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego (patrz treść II § 6 niniejszego dokumentu). Obowiązkiem ADMINISTRATORA SYSTEMU INFORMATYCZNEGO jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

§ 5

Zgodnie z rozporządzeniem, uwzględniając fakt, że użytkowany w jednostce organizacyjnej system informatyczny służący do przetwarzania danych osobowych jest połączony z siecią Internet, wprowadza się wysoki poziom bezpieczeństwa.

II – Część szczegółowa

§ 1

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym określa się w sposób następujący:

a) użytkownik zamierzający przetwarzać dane osobowe, po uzyskaniu upoważnienia stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa, oraz podpisaniu oświadczenia stanowiącego załącznik nr 4 do Polityki Bezpieczeństwa, składa ustnie wniosek do ADMINISTRATORA SYSTEMU INFORMATYCZNEGO o nadanie identyfikatora i hasła w celu umożliwienia wykonywania przetwarzania danych osobowych w systemie informatycznym, ADMINISTRATOR SYSTEMU INFORMATYCZNEGO zobowiązany jest niezwłocznie przydzielić użytkownikowi identyfikator i hasło. Podanie użytkownikowi hasła nie może nastąpić w sposób umożliwiający zapoznanie się z nim osobom trzecim.

b) w przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia, stano-

wiącego załącznik nr 3 do Polityki Bezpieczeństwa, ADMINISTRATOR SYSTEMU INFORMATYCZNEGO zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.

§ 2

Stosuje się następujące metody oraz środki uwierzytelniania, a także procedury związane z ich zarządzaniem i użytkowaniem:

a) hasło składa się, z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne

b) osobą odpowiedzialną za przydział identyfikatora i pierwszego hasła jest ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

c) użytkownik, po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła, jest również zobowiązany do zmiany hasła, co każde 30 dni

d) użytkownik jest zobowiązany do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich

§ 3

Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu:

a) w celu zalogowania do systemu informatycznego, użytkownik podaje swój identyfikator oraz hasło

b) system jest skonfigurowany w taki sposób, aby po okresie 30 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu identyfikatora i hasła

c) po zakończeniu pracy użytkownik jest zobowiązany do wylogowania się, a następnie do wyłączenia komputera

§ 4

Stosuje się następujące procedury tworzenia oraz przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

a) raz na 3 miesiące ADMINISTRATOR SYSTEMU INFORMATYCZNEGO wykonuje kopię pełną

b) wykonane kopie zapasowe przechowuje się na pamięci przenośnej (pendrive), odpowiednio zabezpieczonej przestrzeni na wydzielonych serwerach lub na nośnikach CD/DVD, nośniki zawierające kopie zapasowe są przechowywane

w szafie zamykanej na klucz, do której dostęp posiada wyłącznie ADMINISTRATOR SYSTEMU INFORMATYCZNEGO lub w sytuacji wyjątkowej, osoba przez niego wyznaczona. Kopie zapasowe przechowywane są w pomieszczeniu osoby pełniącej funkcję ADMINISTRATORA SYSTEMU INFORMATYCZNEGO.

§ 5

Elektroniczne nośniki informacji zawierające dane osobowe przechowywane są w szafach zamykanych na klucz, do których dostęp ma jedynie ADMINISTRATOR SYSTEMU INFORMATYCZNEGO oraz, w sytuacjach wyjątkowych, osoba przez niego wyznaczona, dane są przechowywane przez okres, w którym istnieją przesłanki do ich przetwarzania, po ustaniu przesłanek do przetwarzania, dane muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie. Dane przechowywane są w pomieszczeniu osoby pełniącej funkcję ADMINISTRATORA SYSTEMU INFORMATYCZNEGO. Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe, przechowywany jest w obszarze przetwarzania danych osobowych, w pomieszczeniach zabezpieczonych zgodnie z załącznikiem nr 1 do Polityki Bezpieczeństwa.

§ 6

System informatyczny zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania, o jakim mowa w lit. a niniejszego paragrafu:

a) oprogramowaniem antywirusowym stosowanym w jednostce organizacyjnej jest: ESET;

b) użytkownikom nie wolno otwierać na komputerach, na których odbywa się przetwarzanie danych osobowych, plików pochodzących z niewiadomego źródła bez zgody ADMINISTRATORA SYSTEMU INFORMATYCZNEGO;

c) za wdrożenie i korzystanie z oprogramowania antywirusowego, określonego w lit. a oraz oprogramowania firewall, odpowiada ADMINISTRATOR SYSTEMU INFORMATYCZNEGO.

§ 7

Odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (z wyłączeniem osób, których dane dotyczą, osób posiadających upoważnienie do przetwarzania danych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem), odbywa się poprzez zapisanie tej informacji w utworzonym na dysku twardym komputera pliku dotyczącym danej osoby, zgodnie z systemem zapisywania informacji opisanym, w § 12 niniejszej części.

§ 8

Stosuje się następujące procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

a) ADMINISTRATOR SYSTEMU INFORMATYCZNEGO raz na 3 miesiące wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z niniejszej Instrukcji;

b) w przypadku stwierdzenia przez ADMINISTRATORA SYSTEMU INFORMATYCZNEGO nieprawidłowości w działaniu elementów systemu opisanych w lit. a niniejszego paragrafu podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania;

c) jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ADMINISTRATORA SYSTEMU INFORMATYCZNEGO lub w sytuacji wyjątkowej — osoby przez niego wyznaczonej.

§ 9

System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie:

a) systemu kopii bezpieczeństwa;

b) zabezpieczeń oferowanych przez systemy hostingujące;

c) listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami

§ 10

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych, w tym dodatkowo zabezpiecza hasłem pliki lub foldery zawierające dane osobowe.

§ 11

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ADMINISTRATORA SYSTEMU INFORMATYCZNEGO.

§ 12

Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych osobowych (z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie) zapewnia odnotowanie:

a) daty pierwszego wprowadzenia danych do systemu (automatycznie)

b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu (automatycznie)

c) źródła danych (jedynie w przypadku zbierania danych nie od osoby, której dotyczą)

d) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych

e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych

§ 13

Dla każdej osoby, której dane osobowe są przetwarzane system informatyczny, zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 12 lit. a-e.

§ 14

Stosuje się następującą procedurę w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego:

a) w przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń przez osoby nieuprawnione jest on zobowiązany niezwłocznie poinformować o tym fakcie ADMINISTRATORA SYSTEMU INFORMATYCZNEGO

b) ADMINISTRATOR SYSTEMU INFORMATYCZNEGO jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości

§ 15

Usuwanie danych osobowych utrwalonych na nośnikach elektronicznych następuje poprzez powierzenie tych nośników w celu usunięcia zapisanych na nich danych

wyspecjalizowanej w tej dziedzinie firmie informatycznej, lub poprzez nadpisanie usuwanych informacji przez ADMINISTRATORA SYSTEMU INFORMATYCZNEGO w taki sposób, by nie istniała możliwość ich ponownego odczytania. W celu usunięcia danych zapisanych na elektronicznych nośnikach ADMINISTRATOR SYSTEMU INFORMATYCZNEGO może dokonać ich fizycznego uszkodzenia w taki sposób, by nie istniała możliwość odtworzenia zapisanych na nich danych.

III – Postanowienia końcowe

§ 1

W sprawach nieuregulowanych niniejszą Instrukcją, znajdują zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133 poz. 883 z późn. zm.) 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. z 2004 r. Nr 100, poz. 1024).

§ 2

Niniejszy dokument wchodzi w życie z dniem 26 listopada 2015 roku.

Mateusz Palczewski

Mateusz Palczews
MEDUCASE sp. z o.
Prezes zarządu

(*podpis w imieniu spółki*)

B. Privacy Policy

Introduction

Purpose

The purpose of this MEDUCASE Privacy Policy („Privacy Policy") is to describe how MEDUCASE collects, uses and shares information about you through the MEDUCASE website (at www.mdcse.com) (the „Website"), the MEDUCASE mobile applications („Mobile Apps") and MEDUCASE's other online interfaces (collectively referred to herein as the "Services"). Please read this notice carefully to understand what we do. If you do not understand any aspects of our Privacy Policy, please feel free to contact us online at wp@mdcse.com or as described at the end of this Policy. Our Privacy Policy explains:

- Information We Collect and Why We Collect It
- How We Use and Share Your Information
- Access to Your Information and Choices
- Security of Your Information
- Poland Privacy Rights
- International Privacy Practices
- Changes to Our Privacy Policy
- Questions and How Contact Us

Scope; Third Party Sites

This Privacy Policy applies only to information we collect at and through the Services. Our Services may also contain links to third party sites that are not

owned or controlled by MEDUCASE. Please be aware that we are not responsible for the privacy practices of such other sites. We encourage you to be aware when you leave our Services and to read the privacy statements of each and every website, mobile application and online service that collects personal information.

Terms of Use. Please note that your use of our Services is also subject to our Terms and Conditions of Use.

Information we collect and why we collect it

Information You Provide To Us. You can provide information to us through the Services through various means, including

- When you register on the Website or Mobile App, or otherwise create an online account
- When you register or sign in to the Services using your account from another service (such as LinkedIn)
- On your account information page
- When you provide feedback via an online feedback form or contact us form
- When you request information through the Services
- When you access the Services, including the Mobile Apps through your smart phone or mobile device

The information we collect from you and via your connected social media accounts, includes personal information, such as

- Name
- Address
- Date of Birth
- Education History
- Hometown
- Work History

We also collect additional information from your connected social media accounts, including your user groups, interests, „likes", user photos, relationship details, your user status, and certain profile information about your friends. No Information From Children Under Age 13. If you are under the age of 13, please do not

attempt to register with us through the Services or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under the age of 13, we will promptly delete that information. If you believe we might have any information from a child under the age of 13, please contact us at wp@mdcse.com. Information We Collect Automatically. We collect certain information automatically as you use our Services, such as:

- IP address
- Browser type
- Computer or device type
- Unique device identifiers
- Operating system version
- Platform type
- Device ID
- The website from where you navigated to our Website
- Time and date of using our Services
- The name of your Internet service provider (ISP)
- The pages on our Website that you view
- Location / Geolocation information
- Cookies
- Local shared objects (flash cookies)
- Browser language

Cookies

When you visit our Website we send one or more "cookies" to your computer or other device. A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the website again, the cookie allows that site to recognize your browser. Cookies may store unique identifiers, user preferences and other information. The Services use both session cookies and permanent cookies.You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. We use cookies to improve the quality of our service, including for storing user preferences, tracking user trends and providing relevant advertising to you. Pixel Tags.

We may use „pixel tags," also known as „web beacons," which are small graphic files that allow us to monitor the use of our websites. A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking activity on websites, or when emails are opened or accessed, and is often used in combination with cookies. A pixel tag can collect information such as the IP (Internet Protocol) address of the computer that downloaded the page on which the tag appears; the URL of the page on which the pixel tag appears; the time the page containing the pixel tag was viewed; the type of browser that fetched the pixel tag; and the identification number of any cookie on the computer previously placed by that server.

How we use and share your information

To Provide Products, Services, and Information. As described above, we collect information from you so that we can provide the services available to you through the Services, as well as to provide the information that you request from us. We use your personal information to provide features, functionality, discover people like you, discover similar interests of other users, deliver relevant advertisements, offers and coupons, and to contact you about our products, services, and new offerings. We may provide information to third party service providers that help us deliver the information, products and services provided via the Services.

Your assigned username (not your email address) might be displayed to other users alongside the content you upload, including pictures, videos, comments, likes and other information you provide.

We may use third parties to help host our Services, send out email updates about the Services, provide marketing and advertising services, either through the Services or through third party ad networks, remove repetitive information from our user lists, and process payments. These service providers will have access to your personal information in order to provide these services, but when this occurs we implement reasonable contractual and technical protections to limit their use of that information to provide the above-mentioned services. We use demographic information to better understand our customers, and improve our products and services.

Advertising and Marketing

We may use how you browse the Services, how you use interactive features in the Services, and your profile information to show you content, advertising or other

information via the Services from MEDUCASE or through our advertising partners and third party ad networks that are more relevant to your interests. We may use cookies and other information to provide relevant interest-based advertising to you. Interest-based ads are ads presented to you based on your browsing behavior and expressed interests in order to provide you with ads more tailored to your interests. We belong to ad networks that may use your browsing history or collect personal information about your online activities over time across participating websites to show you interest-based advertisements on those websites. You can opt-out of receiving interest-based ads from us by sending an email to mp@mdcse.com with the subject line „Opt Out". Please note that if you choose to opt out, you will continue to see ads on our Services, but they will not be based on how you browse. Some websites, including our Website, belong to ad networks that use your browsing history across websites to choose which ads to display on their sites; the displayed ads may include advertising for MEDUCASE. To learn more, and to opt out of seeing interest-based advertisements on these sites, visit the Network Advertising Initiative and the Digital Advertising Alliance websites (www.mdcse.com and www.espes2017.pl). Websites may also offer their own opt-out methods for interest-based advertising.

C. Obowiązki Pełnomocnika Administratora Danych Osobowych (PADO)

W systemie teleinformatycznym MEDUCASE funkcjonują:

administrator danych osobowych — firma MEDUCASE Sp. z o.o.

pełnomocnik administratora danych osobowych — obowiązki pełni dr inż. Wiesław Palczewski

administrator Systemu Informatycznego — obowiązki pełni dr inż. Wiesław Palczewski oraz mgr inż. Marcin Roczek

Szczegółowy zakres obowiązków PADO

1. Odpowiada za przestrzeganie Ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji;
2. Monitoruje a w razie zmiany obowiązujących przepisów prawa z zakresu ochrony danych osobowych dostosowuje do nich Politykę Bezpieczeństwa;
3. Sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób;
4. Określa strategię zabezpieczania systemów informatycznych (procedury bezpieczeństwa i standardy zabezpieczeń);
5. Sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
6. Sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
7. Identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych;

8. Określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe;
9. Odpowiada za instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;
10. Sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, w których przetwarzane są dane osobowe;
11. Sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe;
12. Prowadzi ewidencję systemów informatycznych, w których przetwarzane są dane osobowe;
13. Prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych;
14. Prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych;
15. Prowadzi rejestr zbiorów danych osobowych (przetwarzanych metodą tradycyjną lub w systemach informatycznych);
16. Prowadzi profilaktykę antywirusową w zakresie eksploatowanego sprzętu;
17. Określa indywidualne obowiązki i odpowiedzialność osób zatrudnionych przy przetwarzaniu danych osobowych;
18. Zapoznaje osoby zatrudnione przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie;
19. Wdraża i nadzoruje przestrzeganie zapisów w „Dokumentacji bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.”;
20. Stwarza warunki organizacyjno-techniczne umożliwiające spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych;
21. Wspólnie z osobami upoważnionymi odpowiada za poprawność merytoryczną danych gromadzonych w systemach informacyjnych;
22. Zgłasza każdą zmianę informacji zawartych w zbiorze danych Generalnemu Inspektorowi Ochrony Danych Osobowych;
23. Przeciwdziała próbom naruszenia bezpieczeństwa informacji;
24. Zarządza licencjami i procedurami ich dotyczącymi.

D. Obowiązki Administratora Systemu Informatycznego (ASI)

Opis funkcji

Pojęcie „*Administrator Systemu Informatycznego*" (**ASI**) nie występuje w Ustawie o Ochronie Danych Osobowych z dnia 29 sierpnia 1997 r. (Dz.U. 1997, Nr 133, poz. 883 z późn. zmian.) [2], lecz w dokumentach z zakresu ochrony i przetwarzania danych osobowych w firmie pt. „*Dokumentacja bezpieczeństwa informacji w firmie MEDUCASE Sp. z o.o.*" — tak.

Do zadań ADMINISTRATORA SYSTEMU INFORMATYCZNEGO należy nadzorowanie pracy serwerów, dodawanie, ewentualna edycja danych, i kasowanie kont ich użytkowników, dbanie o bezpieczeństwo systemu i opcjonalnie samych danych, nadzorowanie, wykrywanie i eliminowanie nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych, dbanie o porządek (dotyczy w szczególności forów internetowych) itp. Chociaż ADMINISTRATOR SYSTEMU INFORMATYCZNEGO nie występuje w Ustawie o ochronie danych osobowych, to jest wpisany w Politykę Bezpieczeństwa jako osoba pełniąca nadzór i opiekę nad systemami przetwarzającymi dane osobowe.

Szczegółowy zakres obowiązków ASI

1. Sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób w zakresie obsługiwanego przez siebie sprzętu;
2. Określa strategię zabezpieczania systemów informatycznych (procedury bezpieczeństwa i standardy zabezpieczeń);
3. Sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe w zakresie obsługiwanego przez siebie sprzętu;

4. Identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych;
5. Określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe;
6. Odpowiada za instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;
7. Sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, w których przetwarzane są dane osobowe;
8. Monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych;
9. Sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych;
10. Decyduje o przyznaniu danemu użytkownikowi identyfikatora oraz prawa dostępu do informacji chronionych w danym systemie przetwarzania;
11. Prowadzi profilaktykę antywirusową;
12. Stwarza warunki organizacyjno-techniczne umożliwiające spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych;
13. Wspólnie z osobami upoważnionymi odpowiada za poprawność merytoryczną danych gromadzonych w systemach informacyjnych;
14. Monitoruje i zapewnia ciągłość działania systemu informatycznego oraz baz danych;
15. Optymalizuje wydajność systemu informatycznego baz danych;
16. Zarządza kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie;
17. Przeciwdziała próbom naruszenia bezpieczeństwa informacji;
18. Przyznaje ściśle określone prawa dostępu do informacji w danym systemie.