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. **??**) oraz podpisać oświadczenie o zachowaniu poufności tych danych (załącznik nr 4 do niniejszego dokumentu, roz. **??**).

§ 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.

. . . . . .

(*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://wszystkoociasteczkach.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, sta-

nowiącego 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.

(*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.