KODEKS DOBRYCH PRAKTYK OCHRONY DANYCH OSOBOWYCH	Załącznik nr 1 do Polityki Bezpieczeństwa
	Wersja I obowiązująca od 15.03.2019r.

FENIX

PSYCHOTERAPIA UZALEŻNIEŃ SP. Z O.O.

UL. PAWŁA POŚPIECHA 1A

44-300 WODZISŁAW ŚLĄSKI

	IMIĘ I NAZWISKO	DATA	PODPIS
ZATWIERDZIŁ:			

1. DANE OSOBOWE

Danymi osobowymi są wszystkie informacje dotyczące osoby fizycznej, na podstawie których można tą osobę zidentyfikować, lub rozszerzyć informację o osobie już zidentyfikowanej. Dane osobowe to między innymi:

- dane pracowników
- dane pacjentów
- dane osób upoważnionych przez pacjentów
- kolejki oczekujących
- zapis monitoringu

Nadzór nad prawidłowym przetwarzaniem danych osobowych w organizacji pełni Administrator Danych Osobowych (ADO) sam lub przy współpracy z Inspektorem Ochrony Danych (IOD).
Do zadań IOD należy m.in.:

- utrzymywanie, aktualizacja niezbędnej dokumentacji;
- opiniowanie w sprawie spraw dotyczących danych osobowych;
- szkolenia pracowników;
- kontrola zabezpieczeń danych osobowych;
- informacja w przypadku zmiany przepisów.

W przypadku wątpliwości czy pytań dotyczących danych osobowych każdy pracownik może zwrócić się z zapytaniem bezpośrednio do ADO lub IOD.

2. ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Na przetwarzanie danych osobowych pacjentów w celu ochrony stanu zdrowia, świadczenia usług medycznych, leczenia przez osoby trudniące się zawodowo leczeniem, świadczenia innych usług medycznych oraz zarządzania udzielaniem usług medycznych nie jest wymagana pisemna zgoda pacjenta. Podanie danych osobowych jest wymogiem ustawowym.

3. UDOSTĘPNIANIE DANYCH

Udostępnianie danych reguluje P-02/PB „Procedura udostępniania danych osobowych”.

Aby uzyskać kserokopię dokumentacji medycznej należy złożyć stosowny wniosek (dostępny w rejestracji). Termin oczekiwania na kserokopię dokumentacji medycznej wynosi do 7 dni roboczych.
Dokumentacja medyczna udostępniana jest osobiście pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie pisemnie upoważnionej przez pacjenta na podstawie upoważnienia przechowywanego w kartotece pacjenta lub na podstawie jednorazowego upoważnienia do odbioru określonej dokumentacji medycznej.

4. MONITOROWANIE PRACOWNIKÓW W SYSTEMACH INFORMATYCZNYCH

W związku z zapewnieniem prawidłowego przestrzegania zasad pracy na danych osobowych, Administrator Danych Osobowych może monitorować działania użytkowników w systemach informatycznych poprzez gromadzenie informacji o:

- fakcie logowania i czasie trwania sesji użytkownika, oraz miejscu i sposobie jej nawiązania;
- dostępie do zasobów i danych oraz sposobie ich wykorzystywania, w szczególności kopiowania i przesyłania poza Organizację;
- sposobie wykorzystywania systemów, wykorzystywanych aplikacji, plików oraz poczty email;
- dostępnie do zasobów sieci publicznej;
- czasie pracy i czasie wykorzystania poszczególnych systemów i aplikacji;
- plikach zgromadzonych na komputerach użytkowników;
- wydrukach.

Monitorowanie nie naraża użytkownika na utratę prywatności dlatego zabronione jest np:

- wykonywanie okresowych zrzutów ekranu użytkownika;
- podgląd ekranu użytkownika bez jego wiedzy i zgody;
- analiza ruchu sieciowego w celu uzyskania danych użytkownika (np. loginów/haseł).

5. KORESPONDENCJA MAILOWA

Jeśli przedmiotem korespondencji są jakiekolwiek dane osobowe, które nie mogą być publicznie dostępne, nie należy ich umieszczać w treści wiadomości, a w załączniku do wiadomości, który należy zabezpieczyć hasłem. Hasło należy przekazać inną drogą niż mail (telefonicznie, smsem, osobiście). Pliki można szyfrować za pomocą programu 7 Zip File Manager, który wymagany jest również do odczytu załącznika opatrzonego hasłem.
W przypadku wysyłania wiadomości do wielu odbiorów, którzy się nie znają (np. w przypadku wysyłania informacji do potencjalnych wykonawców w postępowaniu przetargowym) ich adresy mailowe należy umieścić w polu UDW: wiadomości (ukryte do wiadomości). Nie używamy w takich wiadomościach pola DO: .
W przypadku, gdy użytkownik, niezależnie od nadawcy, **NIE SPODZIEWA SIĘ** otrzymać wiadomości email zawierającej dodatkowe dokumenty w załączniku lub w postaci pliku do pobrania, powinien powstrzymać się od otwarcia takiej wiadomości i skomunikować się z nadawcą w celu weryfikacji otrzymanego maila.

6. UDZIELANIE INFORMACJI PRZEZ TELEFON

Nie należy udzielać telefonicznie informacji o danych osobowych instytucjom, podmiotom zewnętrznym (np. bankom) oraz osobom trzecim.

7.ZASADY OCHRONY FIZYCZNEJ

1. Wszystkie dane osobowe w formie papierowej po zakończonej pracy muszą być przechowywane w zamykanych szafkach, klucze do szaf należy zabezpieczyć przed dostępem osób nieupoważnionych.
2. Ekrany monitorów stanowisk dostępu do danych osobowych muszą zostać wyłączone po 10 minutach nieaktywności pracownika. W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych muszą zostać ustawione w sposób uniemożliwiający tym osobom wgląd do danych.
3. W obszarach przetwarzania danych osobowych nie można pozostawiać osób nieuprawnionych bez nadzoru.
4. Po opuszczeniu pomieszczenia przez ostatnią osobę upoważnioną należy zamknąć je na klucz i zabrać klucz ze sobą.
5. Dokumenty zawierające dane osobowe po ustaniu przydatności muszą być niszczone w sposób mechaniczny za pomocą niszczarek do papieru.

8. PRACA W SYSTEMIE INFORMATYCZNYM

Każda osoba posiada swój login i hasło do komputera i jest zobowiązana do tego, aby nie ujawniać haseł innym osobom. Pracownik odpowiada za zachowanie poufności swojego hasła, zatem nieuprawnione jest:

- zapisywanie haseł;
- korzystanie z funkcji zapamiętywania haseł;
- przekazywanie haseł innym osobom.

Jeśli do uwierzytelnienia wymagane jest hasło, musi się ono składać min. z 8 znaków oraz zawierać małą i dużą literę oraz cyfrę lub znak specjalny.
Odchodząc od komputera za każdym razem należy go zablokować poprzez naciśnięcie kombinacji klawiszy **Ctrl + Alt + Del** wybierając opcję „zablokuj ten komputer" lub **Windows + L**. Po zakończeniu pracy należy wylogować się z wszystkich programów i aplikacji oraz wyłączyć komputer.

9. ZASADY KORZYSTANIA Z OPROGRAMOWANIA

Organizacja przyjmuje następujące zasady korzystania z oprogramowania:

1. Pracownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi i nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę / Zleceniodawcę na swoje własne potrzeby ani na potrzeby osób trzecich;
2. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez ASI. Pracownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę / Zleceniodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z prywatnych płyt CD,

pendrive, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe;
3. Pracownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez ASI;
4. W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca / Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

10. Zasady korzystania z Internetu

Organizacja przyjmuje następujące zasady korzystania z Internetu:
1. Pracownicy mają prawo korzystać z Internetu w celu wykonywania obowiązków służbowych.
2. Przy korzystaniu z Internetu, Pracownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich. Pracownicy nie mają prawa korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym Pracodawcy / Zleceniodawcy, ściągać z Internetu jakichkolwiek plików muzycznych lub wideo.
3. W zakresie dozwolonym przepisami prawa, Pracodawca/Zleceniodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Pracownika z Internetu pod kątem wyżej opisanych zasad. Ponadto, w uzasadnionym zakresie, Pracodawca/Zleceniodawca zastrzega sobie prawo kontroli czasu spędzanego przez Pracownika w Internecie.
4. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

11. Obowiązki pracownika

1. Każdy pracownik zobowiązany jest zachować w poufności sposoby zabezpieczenia oraz dane osobowe, z którymi styka się w związku z pełnieniem obowiązków służbowych;
2. Pracownik jest zobowiązany przetwarzać dane tylko w zakresie niezbędnym do realizacji zadań służbowych – zgodnie z nadanym upoważnieniem. Zabronione jest np. pozyskiwanie szerszego zakresu danych niż wynika to z wewnętrznych przepisów Organizacji, przekazywanie danych służbowych osobom (także innym pracownikom), które nie posiadają analogicznego upoważnienia;
3. Obowiązkiem pracownika jest informowanie Inspektora Ochrony Danych o dostrzeżonych naruszeniach bezpieczeństwa przetwarzanych danych lub wystąpieniu sytuacji, które mogą do takiego naruszenia doprowadzić;
4. Obowiązkiem pracownika jest zgłaszanie Informatykowi incydentów związanych z naruszeniem bezpieczeństwa, bądź też niewłaściwym funkcjonowaniem systemu informatycznego.

12. Postępowanie w przypadku wystąpienia naruszenia

1. Każdy pracownik Organizacji w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora Danych Osobowych lub Inspektora Ochrony Danych;
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    - niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    - niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
    - nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych naruszeń bezpieczeństwa danych osobowych należą:
    - zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
    - zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
    - umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia zagrożenia, IOD prowadzi postępowanie wyjaśniające w toku, którego:
    - ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
    - inicjuje ewentualne działania dyscyplinarne;

- rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
- dokumentuje prowadzone postępowania.

5. W przypadku stwierdzenia naruszenia, IOD prowadzi postępowanie wyjaśniające w toku, którego:
    - ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
    - zabezpiecza ewentualne dowody;
    - ustala osoby odpowiedzialne za naruszenie;
    - podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
    - inicjuje działania dyscyplinarne;
    - wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
    - dokumentuje prowadzone postępowania.

13. POSTĘPOWANIE W PRZYPADKU PRZYJĘCIA NOWEGO PRACOWNIKA

1. W momencie rozpoczęcia współpracy z nową osobą (pracownikiem, zleceniobiorcą, praktykantem, stażystą) osoba odpowiedzialna za przygotowanie umowy jest zobowiązana przekazać tej osobie do podpisu upoważnienie do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym **Załącznik nr 4** do Polityki Bezpieczeństwa .
2. Jeśli nowozatrudniona osoba ma mieć dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe – informacja przekazywana jest do ASI, a ten tworzy konto w systemie i nadaje osobie uprawnienia zgodnie z upoważnieniem.
3. ADO prowadzi ewidencję wszystkich osób upoważnionych do przetwarzania danych osobowych.
4. Zmiana uprawnień odbywa się na podstawie pisemnego wniosku przełożonego.
5. Odebranie uprawnień dokonywane jest na podstawie pisemnego wniosku przełożonego. Odebranie uprawnień polega na zablokowaniu konta użytkownika we wszystkich systemach, do których użytkownik miał dostęp. ADO odnotowuje tę zmianę w ewidencji upoważnionych do przetwarzania danych osobowych. Identyfikator osoby nie może być przydzielany ponownie żadnej innej osobie.
6. Dostęp do wszystkich systemów przetwarzających dane osobowe wymaga uwierzytelnienia. Jeśli do uwierzytelnienia wymagane jest hasło, musi się ono składać min. z 8 znaków oraz zawierać małą i dużą literę oraz cyfrę lub znak specjalny. Pierwsze hasło podawane jest użytkownikowi ustnie przez ASI, po pierwszym logowaniu wymagana jest zmiana hasła. Hasła do systemów są zmieniane raz na 30 dni – zmiana ta jest wymuszona systemowo.

14. PRZEPISY KARNE

Pracownik Organizacji odpowiedzialny jest za wywiązywanie się z zakresu obowiązków oraz ponosi odpowiedzialność za potencjalne szkody wyrządzone pracodawcy. Pracownik przyjmuje do wiadomości następujące kary (wynikające z przepisów prawa):

- **Art. 266 Kodeksu karnego –** *Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*
- **Art. 267 Kodeksu karnego –** *Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Tej samej karze podlega, kto informację uzyskaną w sposób określony powyżej ujawnia innej osobie.*
- **Art. 268 Kodeksu karnego –** *Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli czyn dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. Kto, dopuszczając się czynu, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

- **Art. 269a Kodeksu karnego –** *Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
- **Art. 269b Kodeksu karnego –** *Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.*