Polityka danych osobowych

Towarzystwo Psychopedagogiczne

POLITYKA DANYCH OSOBOWYCH W GABINECIE

§ 1

O DOKUMENCIE

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

§ 2

O ZAŁĄCZNIKACH

Polityka zawiera:

a) opis zasad ochrony danych obowiązujących w gabinetach specjalistów

b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

§ 3

ODPOWIEDZIALNOŚĆ

Specjalista jest odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki. Specjalista zapewnia ponadto zgodność postępowania współpracowników specjalisty z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez specjalistę w niezbędnym zakresie, np. w ramach współpracy z biurem rachunkowym, działem administracyjnym lub podobną jednostką.

§ 4

SŁOWNICZEK

Polityka – oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

RODO – oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s.1).

Dane – oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

Dane szczególnych kategorii – oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne – oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci – oznaczają dane osób poniżej 16. roku życia.

Osoba – oznacza osobę, której dane dotyczą w szczególności klient/pacjent Specjalisty, o ile co innego nie wynika wyraźnie z kontekstu.

Podmiot przetwarzający – oznacza organizację lub osobę, której specjalista powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość itp.).

Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Eksport danych – oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

IOD *lub* ***Inspektor*** – oznacza Inspektora Ochrony Danych Osobowych.

RCPD *lub* ***Rejestr*** – oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

§ 5

REGUŁY OCHRONY DANYCH

1. Ochrona danych osobowych w gabinecie specjalisty opiera się o reguły:

    a. **legalności** – specjalista dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
    b. **bezpieczeństwa** – Specjalista zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stałe działania w tym zakresie.
    c. **poszanowania praw jednostki** – Specjalista umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
    d. **rozliczalności** – Psychotera peuta dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z wytycznymi RODO.

2. Specjalista przetwarza dane osobowe z poszanowaniem następujących zasad:

    a. w oparciu o podstawę prawną i zgodnie z prawem (**legalizm**);
    b. rzetelnie i uczciwie (**rzetelność**);
    c. w sposób przejrzysty dla osoby, której dane dotyczą (**transparentność**);
    d. w konkretnych celach i nie „na zapas” (**minimalizacja**);
    e. nie więcej niż potrzeba (**adekwatność**);

3. System ochrony danych osobowych w gabinecie Specjalisty składa się z następujących elementów:
    a. **Inwentaryzacji danych**, przez co należy rozumieć że Specjalista dokonuje identyfikacji zasobów danych osobowych w gabinecie Specjalisty, klas danych, zależności między

zasobami danych, identyfikacji sposobów wykorzystania danych (tzw. inwentaryzacja), w tym

i. przypadków przetwarzania danych szczególnych kategorii i danych karnych;
ii. przypadków przetwarzania danych osób, których Specjalista nie identyfikuje (tzw. dane niezidentyfikowane);
iii. przypadków przetwarzania danych dzieci;
iv. profilowania;
v. współadministrowania danymi.

b. **Rejestru**, przez co należy rozumieć że Specjalista opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w gabinecie Specjalisty (tzw. Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w gabinecie Specjalisty.
c. **Podstaw prawnych** działania, przez co należy rozumieć że Specjalista zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
    i. utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
    ii. inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Specjalista przetwarza dane na podstawie prawnie uzasadnionego interesu Specjalisty.
d. **Obsługi praw jednostki**, przez co należy rozumieć że Specjalista spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
    i. obowiązki informacyjne, gdyż Specjalista przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
    ii. możliwość wykonania żądań prawem wymaganych, gdyż Specjalista weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich dalszych przetwarzających;

iii. obsługa żądań, gdyż Specjalista zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane;

iv. zawiadamianie o naruszeniach, gdyż Specjalista stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

e. **Minimalizacja**, przez co należy rozumieć że Specjalista posiada zasady i metody zarządzania minimalizacją (tzw. privacy by default), a w tym:

i. zasady zarządzania adekwatnością danych;

ii. zasady reglamentacji i zarządzania dostępem do danych;

iii. zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

f. **Odpowiedni poziom bezpieczeństwa**, przez co należy rozumieć że Specjalista zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

i. przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

ii. przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

iii. dostosowuje środki ochrony danych do ustalonego ryzyka;

iv. posiada system zarządzania bezpieczeństwem informacji;

v. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych, w tym zarządza incydentami.

g. **Odpowiedni poziom doboru podmiotów przetwarzających**, przez co należy rozumieć że Specjalista posiada zasady doboru przetwarzających dane na rzecz Specjalisty, a także wymogów co do warunków przetwarzania (umowa powierzenia), jak również zasad weryfikacji wykonywania umów powierzenia.

h. **Dbanie o odpowiedni eksport danych**, przez co należy rozumieć że Specjalista posiada zasady weryfikacji, czy nie przekazuje danych do państw trzecich (czyli poza UE,

Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

i. **Troska o tzw. privacy by design**, przez co należy rozumieć że specjalista zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w gabinecie Specjalisty uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

j. **Dbanie o bezpieczne przetwarzanie transgraniczne**, przez co należy rozumieć że Specjalista posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO dla takich przypadków.

§ 6

INWENTARYZACJA

1. Dane **szczególnych kategorii** i dane **karne** – tutaj Specjalista identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych Specjalista postępuje zgodnie z przyjętymi zasadami w tym zakresie.
2. Dane **niezidentyfikowane** – tutaj Specjalista identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.
3. **Profilowanie** – tutaj specjalista identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych, i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Specjalista postępuje zgodnie z przyjętymi zasadami w tym zakresie.

4. **Współadministrowanie** – tutaj Specjalista każdorazowo identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

§ 7

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

1. **Rejestr Czynności Przetwarzania Danych** (w skrócie oznaczany także jako: „Rejestr" lub „RCPD") stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2. Specjalista prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
3. Rejestr jest jednym z podstawowych narzędzi umożliwiających specjaliście rozliczanie większości obowiązków ochrony danych.

§ 8

PODSTAWY PRZETWARZANIA

1. Wskazując w dokumentach podstawę prawną: zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel, Specjalista określa podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne.
2. Specjalista wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość np. poprzez email, telefon, wiadomości sms, oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności jako choćby wniesiony sprzeciw co do przetwarzania.

§ 9

SPOSÓB OBSŁUGI PRAW JEDNOSTKI

1. Specjalista dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza
2. Specjalista dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
3. Specjalista wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
4. W celu realizacji praw jednostki Specjalista zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Specjalistę, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
5. Specjalista dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

§ 10

WYKONYWANE OBOWIĄZKI INFORMACYJNE

1. Specjalista określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. Specjalista informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
3. Specjalista informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
4. Specjalista informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
5. Specjalista określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe, np. tabliczka z adnotacją o objęciu danego obszaru monitoringiem wizyjnym.

6. Specjalista informuje osobę o planowanej zmianie celu przetwarzania danych.
7. Specjalista informuje osobę przed uchyleniem ograniczenia przetwarzania.
8. Specjalista informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe.
9. Specjalista informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
10. Specjalista bez zbędnej zwłoki powiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

§ 11

SPOSOBY REAGOWANIA NA ŻĄDANIA OSÓB

1. Prawa „osób trzecich", w tym przypadku, realizując prawa osób, których dane dotyczą, Specjalista wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Specjalista może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2. „Nieprzetwarzanie", w tym przypadku, Specjalista informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
3. „Odmowa", w tym przypadku Specjalista informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych. Żądanie „dostępu do danych" przez osobę której dane dotyczą, w tym przypadku Specjalista informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany

przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Specjalista nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

4. Żądanie „kopii danych" przez osobę której dane dotyczą, w tym przypadku Specjalista wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Specjalista wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.
5. Żądanie „sprostowania danych" przez osobę której dane dotyczą, w tym przypadku Specjalista dokonuje sprostowania nieprawidłowych danych na żądanie właściwej osoby. Specjalista ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Specjalista informuje osobę o odbiorcach danych, na żądanie tej osoby.
6. Żądanie „uzupełnienia danych" przez osobę której dane dotyczą, w tym przypadku Specjalista uzupełnia i aktualizuje dane na żądanie osoby. Specjalista ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych, np. Specjalista nie musi przetwarzać danych, które są Psychoterapeucie zbędne).
7. Specjalista może polegać na oświadczeniu osoby co do uzupełnionych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Specjalistę procedur, np. co do pozyskiwania takich danych, bądź niewystarczające z uwagi na przepisy prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
8. Żądanie „usunięcia danych" przez osobę której dane dotyczą, w tym przypadku Specjalista usuwa dane, gdy:
    a. dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
    b. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
    c. osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
    d. dane były przetwarzane niezgodnie z prawem,

e. konieczność usunięcia wynika z obowiązku prawnego,
f. żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

9. Specjalista określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki przewidziane w art. 17 ust. 3 RODO.
10. W razie gdy dane podlegające usunięciu zostały upublicznione przez Specjalistę, Specjalista podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Specjalista informuje osobę o odbiorcach danych, na żądanie tej osoby.
11. Żądanie „ograniczenia przetwarzania" przez osobę której dane dotyczą, w tym przypadku Specjalista dokonuje ograniczenia przetwarzania danych na wniosek osoby, gdy:
    a. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
    b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
    c. Specjalista nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
    d. osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Specjalisty zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
12. W trakcie ograniczenia przetwarzania Specjalista przechowuje dane, natomiast nie przetwarza ich, czyli ani ich nie wykorzystuje, ani ich nie przekazuje, bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Specjalista

informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Specjalista informuje osobę o odbiorcach danych, na żądanie tej osoby.

13. Żądanie „przenoszenia danych" zgłoszone przez osobę której dane dotyczą, w tym przypadku Specjalista wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Psychoterapeucie, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Specjalisty.
14. Zgłoszenie „sprzeciwu w szczególnej sytuacji" przez osobę której dane dotyczą, w tym przypadku jeżeli osoba zgłosi umotywowany, jej szczególną sytuacją, sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Specjalistę w oparciu o uzasadniony interes Specjalisty lub w oparciu o powierzone Psychoterapeucie zadanie w interesie publicznym, Specjalista uwzględni sprzeciw, o ile nie zachodzą po stronie Specjalisty ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
15. Zgłoszenie „sprzeciwu przy badaniach naukowych, historycznych lub celach statystycznych" przez osobę której dane dotyczą, w tym przypadku jeżeli Specjalista prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, a osoba wniesie umotywowany, jej szczególną sytuacją, sprzeciw względem takiego przetwarzania, wówczas Specjalista uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
16. Zgłoszenie „sprzeciwu względem marketingu bezpośredniego" przez osobę której dane dotyczą, w tym przypadku Specjalista uwzględni sprzeciw i zaprzestanie takiego przetwarzania.
17. Jeżeli Specjalista przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Specjalista zapewnia możliwość odwołania się do interwencji i decyzji wynikłych po stronie Specjalisty, chyba że taka automatyczna decyzja:
    a. jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a specjalistą,

b. jest wprost dozwolona przepisami prawa,
c. opiera się na wyraźnej zgodzie odwołującej osoby.

§ 12

MINIMALIZACJA PRZETWARZANIA DANYCH

1. **Specjalista dba o minimalizację przetwarzania danych** pod kątem: adekwatności danych do celów przetwarzania, w tym pod kątem ich ilości i zakresu, jak również pod kątem dostępu do danych, a także czasu przechowywania danych.
2. „Minimalizacja zakresu" oznacza, że Specjalista zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.
3. Specjalista dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
   Specjalista przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą, tzw. privacy by design.
4. „Minimalizacja dostępu" oznacza, że Specjalista stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). Specjalista stosuje kontrolę dostępu fizycznego.
5. Specjalista dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.
6. Specjalista dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok. Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Specjalisty

7. „Minimalizacja czasu" oznacza, że Specjalista wdraża mechanizmy kontroli cyklu życia danych osobowych w gabinecie Specjalisty, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów produkcyjnych Specjalisty, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Specjalistę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

§ 13

BEZPIECZEŃSTWO PRZETWARZANIA DANYCH

1. Specjalista zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Specjalistę.
2. Specjalista przeprowadza oraz dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych, a w tym celu:
    a. Specjalista zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
    b. Specjalista kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
    c. Specjalista przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Specjalista analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

3. Specjalista ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania, jak również Specjalista ustala przydatność oraz stosuje takie środki jak:
    a. pseudonimizacja,
    b. szyfrowanie danych osobowych,
    c. środki cyberbezpieczeństwa wpływające na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
    d. środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
4. Specjalista dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
5. Specjalista stosuje metodykę oceny skutków przyjętą w gabinecie Specjalisty.
6. Specjalista stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w gabinecie Specjalisty i są bliżej opisane w procedurach przyjętych przez Specjalistę dla tych obszarów.
7. Specjalista stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie maksymalnie siedemdziesięciu dwóch godzin od ustalenia naruszenia.

§ 14

DALSI PRZETWARZAJĄCY

1. Specjalista posiada zasady doboru i weryfikacji dalszych przetwarzających dane na rzecz Specjalisty, a opracowane w celu zapewnienia, aby owi przetwarzający dawali wystarczające

gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na specjaliście.

2. Specjalista przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych, stanowiące Załącznik nr 2 do niniejszej Polityki: „Wzór umowy powierzenia przetwarzania danych" – wersja oznaczona jako „a", natomiast dodatkowo z uwagi na specyfikę pracy Specjalisty i konieczność przeprowadzania superwizji wprowadza się także: „Wzór umowy powierzenia przetwarzania danych – superwizja", wersja wzoru umowy oznaczona jako „b".
3. Specjalista rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

§ 15

EKSPORT DANYCH POZA EUROPEJSKI OBSZAR GOSPODARCZY

1. Specjalista rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. to: Unia Europejska, Islandia, Liechtenstein i Norwegia), o ile taki eksport danych następuje.
2. Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, Specjalista okresowo weryfikuje zachowania w sieci internet.

§ 16

DBANIE O PRYWATNOŚĆ W RAZIE PLANOWANIA ZMIAN ORGANIZACYJNYCH

Specjalista zarządza planowaną zmianą w gabinecie Specjalisty mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez

Specjalistę odwołują się do zasad bezpieczeństwa danych osobowych i zasad minimalizacji przetwarzania danych, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od samego początku projektu lub inwestycj.

§ 17

OPIS PRZETWARZANIA

1. Na warunkach określonych w polityce prywatności uczestnik powierza przetwarzanie swoich danych osobowych do wykonywania niezbędnych czynności w celu ich zbierania.
2. Charakter przetwarzania określony jest rolą przetwarzającego.
3. Celem przetwarzania danych osobowych może być:
    a. członkostwo w towarzystwie,
    b. prowadzenie dokumentacji specjalistycznej niezbędnej do prawidłowego wykonywania swojej pracy,
    c. przetwarzanie danych do celów księgowych i rozliczeniowych,
    d. inne jeśli wystąpi taka konieczność, specjalista wystosuje dodatkową informację.
4. Przetwarzanie obejmować może następujące rodzaje danych osobowych:
    a. imię i nazwisko,
    b. numer ewidencyjny PESEL,
    c. adres e-mail,
    d. adres IP,
    e. numery telefonów,
    f. adres zamieszkania,
    g. data urodzenia,
    h. NIP,
    i. seria i numer dokumentu tożsamości,
    j. imiona rodziców,
    k. numer rachunku bankowego.

5. Przetwarzanie danych może dotyczyć następujących **kategorii osób:**
    a. klienci/pacjenci korzystający z usługi Administratora,
    b. pracownicy Administratora,
    c. pracownicy podmiotów stowarzyszonych z Administratorem,
    d. osoby z którymi klienci/pacjenci Administratora wchodzą w interakcje społeczne,
    e. członkowie towarzystwa,
    f. kursanci,
    g. stażyści i praktykanci.

§ 18

PODPOWIERZENIE

1. Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („podpowierzenie") w drodze pisemnej umowy podpowierzenia („Umowa Podpowierzenia") innym podmiotom przetwarzającym („Podprzetwarzający"), pod warunkiem **wyraźniej i niezbędnej takiej potrzeby.**
2. W razie zgłoszenia sprzeciwu przetwarzający nie ma prawa powierzyć danych podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu podprzetwarzającemu.
3. Dokonując podpowierzenia, przetwarzający ma obowiązek zobowiązać podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

§ 19

OBOWIĄZKI PRZETWARZAJĄCEGO

Przetwarzający ma następujące obowiązki:

1. Przetwarzający przetwarza dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.
2. Przetwarzający oświadcza, że nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy – EOG). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.
3. Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać dane poza EOG, informuje o tym Administratora w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.
4. Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.
5. Przetwarzający zapewnia ochronę danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.
6. Przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, tzw. podprzetwarzającego.
7. Przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale „prawa jednostki" RODO. Przetwarzający oświadcza, że zapewnia obsługę praw jednostki w odniesieniu do powierzonych danych. Szczegóły obsługi praw jednostki, w tym procedura obsługi, zostaną między Stronami osobno uzgodnione.
8. Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32–36 RODO, czyli takich jak: ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób

dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym.

9. Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.
10. Planując dokonanie zmian w sposobie przetwarzania danych, Przetwarzający ma obowiązek zastosować się do wymogu tzw. projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO, i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i w takich terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania danych przez Przetwarzającego.
11. Przetwarzający zobowiązuje się do ograniczenia dostępu do danych wyłącznie do osób, których dostęp do danych jest potrzebny do realizacji Umowy i posiadających odpowiednie upoważnienie.
12. Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania danych, w tym rejestru czynności przetwarzania danych osobowych zgodnie z wymogiem art. 30 RODO. Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.
13. Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.
14. Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

§ 20

OBOWIĄZKI ADMINISTRATORA

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

§ 21

BEZPIECZEŃSTWO DANYCH

1. Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych, udostępnił ją Administratorowi i stosuje się do jej wyników co do organizacyjnych i technicznych środków ochrony danych.
2. Przetwarzający zapewnia i zobowiązuje się, że:

a) dokonał oceny przydatności pseudonimizacji i szyfrowania i stosuje te techniki w takim zakresie, w jakim są potrzebne do zapewnienia poziomu bezpieczeństwa danych odpowiedniego do ustalonego ryzyka naruszenia praw lub wolności osób, przy ich przetwarzaniu;

b) posiada zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności swoich systemów i usług przetwarzania;

c) posiada zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularnie testuje, mierzy i ocenia skuteczność stosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

§ 22

ZABEZPIECZENIE DANYCH W SYSTEMACH INFORMATYCZNYCH

1. Podstawową zasadą jest zapewnienie pełnej ochrony informacji przed nieuprawnionym dostępem, a także przed przypadkowym zniszczeniem lub przypadkową zmianą.

2. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych, w tym zasady uwierzytelniania użytkowników systemu informatycznego, aby zachować poufność, rozliczalność oraz autentyczność danych
3. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
    a. w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
    b. dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
4. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
    a. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
    b. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
5. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. Do uwierzytelniania użytkowników używa się hasła, a jego zmiana następuje nie rzadziej niż co 30 dni. W przypadku podejrzenia, że hasło mogło zostać ujawnione należy je niezwłocznie zmienić.
7. U Specjalisty stosuje się wysoki poziom bezpieczeństwa przetwarzania danych osobowych, dlatego hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
8. Hasła nie powinny zawierać powszechnie używanych słów, np. imion.
9. Hasło jest poufne także wtedy gdy minął czas jego używania.

Procedury związane z zarządzaniem środkami uwierzytelniania i użytkowaniem

1) Hasło dostępu do systemu dla nowego użytkownika nadaje administrator systemu informatycznego lub osoba przez niego upoważniona.
2) W razie gdy użytkownik zapomni hasła zwraca się na piśmie do administrator systemu informatycznego o nadanie nowego hasła.
3) Administrator systemu informatycznego po każdym nadaniu hasła lub zmianie hasła zapisuje hasła i przechowuje w sejfie, do którego dostęp ma wyłącznie administrator uprawnień, administrator systemu informatycznego oraz każda z osób uprawnionych, zgodnie z ogólnymi przepisami prawa, do reprezentacji Specjalisty.

4) Użytkownik ma obowiązek zapamiętać hasło i nie może hasła nigdzie zapisywać, ani haseł obecnych, ani haseł poprzednich.
5) Inspektor ochrony danych przy udziale administratora systemu informatycznego stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Procedura rozpoczęcia pracy przez użytkownika systemu

1) Użytkownik systemu informatycznego po uruchomieniu komputera w celu uzyskania dostępu do systemu musi podać identyfikator i hasło.
2) Użytkownik systemu informatycznego może korzystać tylko z przypisanych do danego komputera i do danego użytkownika aplikacji.

Procedura zawieszenia pracy przez użytkownika systemu

1) Użytkownik systemu informatycznego kiedy w trakcie pracy oddala się od komputera, choćby na moment, powinien wylogować się z systemu.
2) W trakcie zawieszenia pracy żadne dane nie mogą być wyświetlane na ekranie.
3) Zaleca się korzystanie z wygaszaczy ekranu.
4) Zawieszenie pracy przez użytkownika systemu informatycznego powinno się odbyć w taki sposób, aby ponowne uzyskanie dostępu do systemu następowało poprzez podanie identyfikatora i hasła.

Procedura zakończenia pracy przez użytkownika systemu

1) Użytkownik systemu informatycznego powinien zamknąć wszystkie uruchomione programy.
2) Użytkownik systemu informatycznego powinien zamknąć system.
3) Użytkownik systemu informatycznego powinien wyłączyć komputer i ewentualne urządzenia peryferyjne, np. skaner, drukarka.

Sposób i miejsce przechowywania elektronicznych nośników informacji.

1) Przez elektroniczne nośniki informacji rozumie się także komputerowe nośniki informacji zdefiniowane w niniejszej Instrukcji

2) Elektroniczne nośniki informacji są przechowywane w Specjalisty na obszarze przetwarzania danych osobowych, a określonym w Polityce Ochrony Danych Osobowych obowiązującej w Specjalisty.
3) Elektroniczne nośniki informacji nie powinny być wynoszone poza obręb Specjalisty.
4) Po zakończeniu korzystania z elektronicznego nośnika informacji każdorazowo należy taki nośnik przechowywać w zamkniętej szafce.
5) 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 osoby upoważnionej przez inspektora danych osobowych.

6) Elektroniczny nośnik informacji który uległ uszkodzeniu należy fizycznie zniszczyć w sposób trwały, co powinno zostać potwierdzone pisemnym protokołem.

Okres przechowywania elektronicznych nośników informacji

Dane osobowe zapisane na elektronicznym nośniku informacji powinny zostać trwale usunięte z tego elektronicznego nośnika informacji, w sposób uniemożliwiający ich odtworzenie, niezwłocznie po użyciu tych danych, nie później jednak niż w ciągu 1 dnia od użycia danych, chyba że z odrębnych przepisów wynika obowiązek dłuższego przechowywania takich danych.

Stosowana ochrona przed nieuprawnionym dostęp do systemu komputerowego

1) System informatyczny służący do przetwarzania danych osobowych należy chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, które to zabezpieczenia obejmują:
    a) kontrolę przepływu informacji pomiędzy systemem informatycznym inspektora danych osobowych a siecią publiczną,

b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego inspektora danych osobowych.

2) System informatyczny służący do przetwarzania danych osobowych należy chronić przed zagrożeniami pochodzącymi z sieci publicznej także poprzez wdrożenie fizycznych zabezpieczeń.
3) Administrator systemu informatycznego odpowiada za właściwe i skuteczne zapewnienie ochrony przed zagrożeniami pochodzącymi z sieci publicznej, o której mowa w pkt 1 i 2 powyżej.
4) Administrator uprawnień przy udziale administratora systemu informatycznego monitoruje stale, w sposób ciągły, wdrożone zabezpieczenia systemu informatycznego.

§ 23

POWIADOMIENIE O NARUSZENIACH DANYCH OSOBOWYCH

1. Przetwarzający powiadamia Administratora o każdym podejrzeniu naruszenia ochrony danych nie później niż w ciągu dwudziestu czterech godzin od pierwszego zgłoszenia, jak również umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia lub jego braku.
2. Przetwarzający przesyła powiadomienie o stwierdzeniu naruszenia wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.

§ 24

NADZÓR

1. Administrator kontroluje sposób przetwarzania powierzonych danych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli ze strony Administratora.

2. Administrator lub wyznaczone przez niego osoby są uprawnione do wstępu do pomieszczeń, w których przetwarzane są dane, a także mają prawo wglądu do dokumentacji związanej z przetwarzaniem danych.
3. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania danych oraz udostępnienia rejestrów przetwarzania z zastrzeżeniem tajemnicy handlowej Przetwarzającego.
4. Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.
5. Przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO.
6. Przetwarzający umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji, a nadto Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.
7. Administrator oświadcza, że jest Administratorem danych oraz że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
8. Przetwarzający oświadcza, że z najwyższą starannością zajmie się przetwarzaniem danych osobowych objętych niniejszą umową, a nadto posiada w tym zakresie niezbędną wiedzę, którą stale poszerza, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię prawidłowego wykonania niniejszej Umowy.
9. Na żądanie Administratora Przetwarzający okaże Administratorowi stosowne referencje, wykaz doświadczenia, informacje finansowe lub inne dowody, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

§ 25

ODPOWIEDZIALNOŚĆ

1. Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego, lub gdy

Przetwarzający działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa.

2. Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

§ 26

USUNIĘCIE DANYCH

1. Z chwilą rozwiązania umowy, przetwarzający nie ma prawa do dalszego przetwarzania powierzonych danych i jest zobowiązany do przekazania danych administratorowi.

§ 27

SUPERWIZJA

1. Standardem pracy specjalistów Towarzystwa Psychopedagogicznego w Polsce i na świecie jest regularne korzystanie z superwizji. **Superwizja** jest procesem w którym specjalista współpracuje z innymi specjalistami, aby poszerzyć umiejętności zawodowe i zapewnić bezpieczeństwo toczącej się działalności dla klienta / pacjenta.
2. Przetwarzanie danych osobowych przez innych specjalistów uczestniczących w superwizji jest identyczne jak specjaliście,
3. **Przetwarzający superwizor przetwarza dane wyłącznie w celu prawidłowego prowadzenia procesu superwizji.**

§ 28

INFORMACJA OD SPECJALISTY O PRZETWARZANIU DANYCH OSOBOWYCH

Jako specjalista, uprzejmie informuję, że przetwarzam Twoje dane osobowe. Troska o poufność powierzonych przez Ciebie danych jest dla mnie kluczowa. Stosuję wymogi prawa, w tym RODO, a

także dbam w sposób praktyczny, aby Twoje dane osobowe były w pełni bezpieczne. Zakres i szczegóły przetwarzania Twoich danych osobowych przedstawiam poniżej.

W razie jakichkolwiek pytań, czy uwag proszę śmiało o kontakt ze mną.

§ 29

ADMINISTRATOR DANYCH OSOBOWYCH

1. Administratorem głównym danych osobowych jest Zarząd Główny Towarzystwa Psychopedagogicznego.
2. Administratorem upoważnionym przez Zarząd Główny jest kierownik / dyrektor danej placówki.

§ 30

PODMIOTY UPOWAŻNIONE

Istnieje możliwość, iż dane osobowe mogą być udostępnione podmiotom upoważnionym przez administratora danych. Przykładowo może to być:

- firma księgowa,
- firma informatyczna,
- kierownik placówki,
- asystent poradni / placówki,
- dyrektor działu.

§ 31

OKRES PRZECHOWYWANIA DANYCH OSOBOWYCH

Dane osobowe są przechowywane i przetwarzane nie dłużej, niż wymaga do tego prawo np. do celów księgowych, informacyjnych.

§ 32

PRAWA PRZETWARZANYCH DANYCH

1. Osobie, której są przetwarzane dane osobowe przysługuje:
    a. prawo dostępu do swoich danych oraz otrzymania ich kopii
    b. prawo do sprostowania (poprawiania) swoich danych
    c. prawo do usunięcia danych.
    d. ograniczenia przetwarzania danych.
    e. prawo do wniesienia sprzeciwu wobec przetwarzania danych:
        i. Sprzeciw „marketingowy". Masz prawo sprzeciwu wobec przetwarzania Twoich danych w celu prowadzenia marketingu bezpośredniego.
        ii. Sprzeciw z uwagi na szczególną sytuację.
    f. prawo do przenoszenia danych;
    g. prawo do wniesienia skargi do administratora danych;
    h. prawo do cofnięcia zgody na przetwarzanie danych osobowych;
2. Przekazywane dane osobowe Towarzystwu lub specjalistom są dobrowolne, lecz jeśli z powodu ich braku otrzymania usługa, członkostwo lub inne korzyści płynące z przekazania danych mogą nie być dalej realizowane.

§ 33

ZGODA NA PRZETWARZANIE DANYCH

Członkowie Towarzystwa, klienci, pacjenci, kursanci, praktykanci itp. wyrażają zgodę na przetwarzanie danych osobowych do celów informacyjnych, tj.

1. wysyłania i otrzymywania niezbędnych informacji drogą sms,
2. wysyłania i otrzymywania niezbędnych informacji drogą e-mail,
3. wysyłania i otrzymywania niezbędnych informacji drogą telefoniczną.

§ 34

OŚWIADCZENIE, ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Tak, zgadzam się na przetwarzanie moich danych osobowych przez Towarzystwo Psychopedagogiczne i osoby upoważnione przez administratora danych osobowych, które zbierane są w celu niezbędnych działań do ich realizacji. Wiem, że wyrażenie zgody jest dobrowolne i mogą ją w każdym momencie wycofać. Mam świadomość, że cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie mojej zgody przed jej wycofaniem.

Niniejsza zgoda jest akceptowana i realizowana w momencie podpisania deklaracji członkowskiej, kontraktu terapeutycznego lub bezpośredniego kontaktu z sekretariatem towarzystwa lub specjalistą pracujacym / współpracującym z Towarzystwem Psychopedagogicznym.