REGULAMIN OCHRONY DANYCH OSOBOWYCH

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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) dla:

- Członków Polskiego Towarzystwa Medycyny Pracy.
- Zleceniobiorców, posiadających dostęp do danych osobowych przetwarzanych przez Administratora.

Każda z w/w osób powinna zapoznać się z poniższym Regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych.

SPIS TREŚCI

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, NOŚNIKÓW I PROGRAMÓW PRZETWARZAJĄCYCH DANE OSOBOWE.

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, kserokopiarki, laptopy.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT przetwarzającego dane.
3. Użytkownik jest zobowiązany do uniemożliwienia osobom nieupoważnionym wglądu do danych wyświetlanych na monitorach komputerowych – obowiązuje **tzw. polityka czystego ekranu.**
4. W sytuacji zawieszenia wykonywanej pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
5. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy;
    b. zabezpieczyć wszelkie nośniki elektroniczne, magnetyczne i optyczne na których znajdują się dane osobowe;
6. Użytkownik jest zobowiązany do usuwania plików z nośników i dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas wspólnego użytkowania komputerów).

7. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrivia, np. młotkiem, spawarką łukową itp).
8. Użytkownicy komputerów przenośnych i zewnętrznych pamięci, na których znajdują się dane osobowe, zobowiązani są do stosowania zasad bezpieczeństwa w postaci szyfrowania tych komputerów.

2 ZARZĄDZANIE UPRAWNIENIAMI

1. Każdy użytkownik z dostępem do danych osobowych (na swoim komputerze, w poczcie elektronicznej) powinien posiadać swój własny indywidualny identyfikator (login) niezbędny do logowania się w systemie.
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie Administratora danych.
3. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom wykonywanie pracy na koncie danego użytkownika.

3 POLITYKA HASEŁ

1. Hasła powinny składać się z co najmniej 8 znaków.
2. Hasła powinny zawierać duże litery, małe litery ,cyfry i znaki specjalne.
3. Hasła nie mogą być łatwe do identyfikacji. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach, naklejać ich na monitorze komputera ani trzymać pod klawiaturą lub w niezabezpieczonej szufladzie biurka.
5. W przypadku ujawnienia hasła należy je natychmiast zmienić.
6. Hasła powinny być zmieniane co **30** dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

4 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Użytkownicy przetwarzający dane osobowe są zobowiązani do stosowania tzw. **polityki czystego biurka**. Polega ona na zabezpieczaniu (zamykaniu) dokumentów w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
2. Członkowie PTMP zobowiązani są do niszczenia dokumentów i wydruków w pomieszczeniach PTMP. Wydruki niepotrzebne i nieprzydatne są utylizowane za pomocą niszczarki w pomieszczeniach PTMP lub za pośrednictwem specjalistycznej firmy. Firma powinna wykazać się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001).
3. Zabrania się pozostawiania dokumentów z danymi osobowymi w kserokopiarkach, drukarkach oraz poza zabezpieczonymi pomieszczeniami firmy.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz.

5 ZASADY WYNOSZENIA DANYCH OSOBOWYCH POZA SIEDZIBĘ PTMP.

1. Użytkownicy nie mogą wynosić na zewnątrz wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora/Lokalnego Administratora. Do takich nośników zalicza się: wymienne twarde dyski, pendrivy, płyty CD, DVD, pamięci typu flash.
2. Dane osobowe wynoszone, przewożone i wykorzystywane poza siedzibą PTMP powinny być zaszyfrowane (szyfrowane całe dyski, ich wyodrębnione części gdzie znajdują się dane osobowe, zaszyfrowane pendrivy, zabezpieczone hasłem pliki lub foldery).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach i pojemnikach.

4. Należy korzystać ze sprawdzonych firm kurierskich.

5. W przypadku, gdy użytkownik wynosi, przewozi lub użytkuje poza siedzibą PTMP przenośny sprzęt informatyczny, nośniki zewnętrzne lub dokumentację papierową zawierające dane osobowe zobowiązany jest on do ich zabezpieczenia w taki sposób, aby ochronić je przed zniszczeniem, zagubieniem, kradzieżą i dostępem osób nieuprawnionych.

6 ZASADY KORZYSTANIA Z INTERNETU.

1. Zabrania się zapisywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
3. Zabrania się przeglądania stron na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo. Przeglądanie tych stron grozi zainstalowaniem szkodliwego oprogramowania infekującego w sposób automatyczny system operacyjny komputera.
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
5. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikony (symbol kłódki) oraz adresu www rozpoczynającego się frazą ”https:”. Dla bezpieczeństwa należy kursorem uaktywnić ikonę kłódki i sprawdzić, czy właściciel certyfikatu jest wiarygodny.
6. Należy zachować szczególną ostrożność w przypadku żądania lub prośby zalogowania się na konkretną stronę internetową (banku, portalu społecznościowego, sklepu internetowego, poczty e-mail) lub podania loginów i haseł, PIN-ów, numerów kart płatniczych.

7 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ.

1. Użytkownicy mogą komunikować się ze sobą za pomocą poczty elektronicznej, z wykorzystaniem adresu e-mail wskazanego w deklaracji członkowskiej, dla celów związanych z działalnością PTMP.

2. Korzystanie z elektronicznej poczty dla innych celów może się odbywać jedynie w sytuacji wyrażenia zgody na przesyłanie informacji handlowych drogą elektroniczną – zgodnie ze złożoną deklaracją członkowską.
3. Przy korzystaniu z poczty elektronicznej użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.
4. Przesyłanie danych osobowych pocztą elektroniczną może dokonywać tylko osoba posiadająca upoważnienie do przetwarzania danych wydane przez Administratora/Administratora Lokalnego.
5. W przypadku przesyłania danych osobowych należy wykorzystywać mechanizmy kryptograficzne (zabezpieczenie hasłem wysyłanych dokumentów lub plików skompresowanych, podpis elektroniczny).
6. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 9 znaków: duże i małe litery i cyfry oraz znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
7. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
8. Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
9. **WAŻNE:** Nie należy otwierać załączników (plików i folderów) otrzymanych w poczcie elektronicznej, nawet od znanych nadawców, bez weryfikacji nadawcy. Załączniki z nieznanych źródeł zawierać mogą pliki ze szkodliwym oprogramowaniem, które po otworzeniu infekuje komputer użytkownika. W wyniku działania szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem dysku przez kryptowirusy.
10. **WAŻNE:** Bez weryfikacji wiarygodności nadawcy, nie należy otwierać hiperlinków (tzn. odnośników do innych stron WWW), gdyż może to skutkować przekierowaniem do stron zainfekowanych lub niebezpiecznych. Użytkownik bezwiednie wówczas infekuje swój komputer oraz niejednokrotnie pozostałe komputery w sieci. W wyniku takiej

infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem dysku przez kryptowirusy.

11. Należy zgłaszać Administratorowi/Administratorowi Lokalnemu przypadki otrzymania podejrzanych wiadomości.
12. Podczas wysyłania poczty elektronicznej do wielu adresatów jednocześnie, należy użyć opcji „**Ukryte do wiadomości – UDW**”. Zabronione jest rozsyłanie wiadomości do wielu adresatów z użyciem opcji „Do wiadomości – DW”. Skutkować to może ujawnieniem przesyłanych danych i naruszeniem zasad ochrony danych osobowych.
13. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości lub je okresowo archiwizować.
14. Użytkownicy nie mają prawa korzystać z elektronicznej poczty w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

8 OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.

2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów o zainfekowaniu użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora/Administratora Lokalnego.

9 INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora/Administratora Lokalnego o przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do incydentów wymagających powiadomienia, należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
b. zdarzenia losowe wewnętrzne (awarie, komputerów, twardych dysków, oprogramowania, pomyłki, użytkowników, utrata, zagubienie danych);
c. 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);

3. Typowe przykłady incydentów wymagające reakcji:
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   b. dokumentacja jest niszczona bez użycia niszczarki;
   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
   e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
   f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Administratora/Administratora Lokalnego;
   g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
   h. telefoniczne próby wyłudzenia danych osobowych;
   i. kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive'a z danymi osobowymi'
   j. wiadomości zachęcające do ujawnienia identyfikatora i/lub hasła;
   k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
   l. hasła do systemów znajdują są w pobliżu komputera;

10 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
    a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora/Administratora Lokalnego zadaniach;
    b. zachowania w tajemnicy danych osobowych do których ma lub będzie miał/a dostęp w związku z wykonywaniem powierzonych zadań;
    c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań;
    d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
    e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem;
2. Osoba upoważniona do przetwarzania musi odbyć szkolenie z zasad ochrony danych osobowych;
3. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są podpisać oświadczenie o poufności;
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego;
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych;

11 POSTĘPOWANIE DYSCYPLINARNE I KARNE.

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako naruszenie obowiązujących zasad w zakresie ochrony danych osobowych.

2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może skutkować powiadomieniem organów ścigania o naruszeniu przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

Zatwierdzający *Prezes PTMP* *Prof. dr hab. n.med. Jolanta Walusiak-Skorupa* *19.10.2018 r.*	Zatwierdzający *Sekretarz* *Dr n. med. Marcin Rybacki* *19.10.2018 r.*