1/ „Regulamin przetwarzania i ochrony danych osobowych"

Dyrektor Szpitala Specjalistycznego w Brzozowie na podstawie art. 24 ***Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)***wprowadził **zarządzeniem Nr 65/2018 z dnia 25 maja 2018 roku** ***„Regulamin przetwarzania i ochrony danych osobowych"*** – zwany w dalszej części ***„Regulaminem przetwarzania"***, określający zasady i procedury obowiązujące przy przetwarzaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Szpital Specjalistyczny w Brzozowie.
Regulamin stanowi zbiór ogólnych zasad postępowania, których przestrzeganie jest niezbędne do zapewnienia bezpiecznego przetwarzania danych osobowych.

2/ Podstawowe pojęcia

Zgodnie z przepisami art. 4 rozporządzenia **dane osobowe oznaczają** informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Wyróżniamy 2 kategorie danych osobowych:

1/ **dane osobowe zwykłe;**

2/ **szczególne kategorie danych osobowych**, w tym dane dotyczące zdrowia: wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. **Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej:** numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Natomiast **przetwarzanie danych oznacza** operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

1. zbieranie,
2. utrwalanie,
3. organizowanie,
4. porządkowanie,
5. przechowywanie,
6. adaptowanie lub modyfikowanie,
7. pobieranie,
8. przeglądanie,
9. wykorzystywanie,
10. ujawnianie poprzez przesłanie,
11. rozpowszechnianie lub innego rodzaju udostępnianie,
12. dopasowywanie lub łączenie,

13. ograniczanie,
14. usuwanie,
15. niszczenie.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują **Administrator Danych**, którym jest Szpital Specjalistyczny w Brzozowie, reprezentowany przez Dyrektora Szpitala, oraz wyznaczony przez niego **Inspektor Ochrony Danych**.
W przypadku danych osobowych przetwarzanych w systemach informatycznych, za bezpieczeństwo przetwarzania tych danych odpowiada **Administrator Systemów Informatycznych** oraz podlegli mu pracownicy Sekcji Obsługi i Konserwacji Urządzeń.

3/ Zasady przetwarzania i ochrony danych osobowych

W celu zabezpieczenia danych osobowych przed nieautoryzowanym dostępem osób nieupoważnionych do ich przetwarzania oraz wypłynięciem tych danych poza zakład pracy stosuje się trzy rodzaje zabezpieczeń:

- **Zabezpieczenia fizyczne** – systemy antywłamaniowe, systemy przeciwpożarowe, sejfy, szafy pancerne, szafy i biurka zamykane na klucz, monitoring pomieszczeń i obszarów na zewnątrz budynków, itp.

- **Zabezpieczenia informatyczne** – stanowią zespół zabezpieczeń przed programami kradnącymi dane z komputerów: na zespół ten składa się przede wszystkim z oprogramowania antywirusowego oraz firewall'a.

- **Zabezpieczenia proceduralne** – stanowiące listę czynności, do których jest zobowiązana każda osoba przetwarzająca dane osobowe lub poruszająca się w obszarach przetwarzania danych osobowych.

Kierownika Sekcji Higieny Szpitalnej zobowiązuje się do zorganizowania pracy sprzątaczek w obszarach przetwarzania danych osobowych, w szczególności poza rozkładem czasu pracy pracowników Administracji w taki sposób, by wykonywały one niżej wymienione czynności:

- sprawdzanie zamknięć drzwi i okien oraz stosowanych zabezpieczeń;
- sprawdzanie stanu technicznego urządzeń i armatury w pomieszczeniach higieniczno-sanitarnych;
- podejmowanie natychmiastowych czynności wyjaśniających w przypadku zaobserwowania w obszarach przetwarzania danych osobowych obecności, bez nadzoru pracowników Szpitala, osób nie będących pracownikami Szpitala;
- natychmiastowe reagowanie poprzez zawiadomienie odpowiednich służb (Policja, Straż Pożarna) o zaobserwowanych próbach stworzenia zagrożenia dla życia, zdrowia oraz utraty lub zniszczenia mienia.

Dyrektor Szpitala wyznacza pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy. Zamknięcia dostępu zewnętrznego do strefy administracyjnej po godzinie 15^{00} dokonuje sprzątaczka.

4/ Niszczenie dokumentacji zawierającej dane osobowe

1/ W przypadku konieczności zniszczenia materiałów zawierających dane osobowe (dokumentacja medyczna, dokumentacja pracownicza, wydruki z systemów informatycznych, wyniki badań, płyty DVD, płyty CD, dokumentacja zbiorcza etc.) każda osoba będąca w posiadaniu takich materiałów zobowiązana jest do ich przekazywania osobie wyznaczonej przez kierownika danej komórki organizacyjnej do zabezpieczania tych materiałów.

Zabrania się wynoszenia poza teren Szpitala wszelkich materiałów zawierających dane osobowe.

2/ Materiały powyższe muszą być przechowywane w obrębie danej komórki organizacyjnej oraz

w odpowiedni sposób zabezpieczone.

3/ Po zebraniu odpowiedniej ilości tych materiałów (stosownie do możliwości przechowywania tych materiałów przez każdą komórkę organizacyjną Szpitala) osoba wyznaczona przez kierownika danej komórki organizacyjnej do zabezpieczania tych materiałów zawiadamia telefonicznie Inspektora Ochrony Danych w Szpitalu Specjalistycznym w Brzozowie o konieczności zniszczenia materiałów zawierających dane osobowe.

4/ Inspektor Ochrony Danych – po konsultacji z Kierownikiem Sekcji Gospodarczej w Szpitalu Specjalistycznym w Brzozowie – wyznacza termin odbioru materiałów przeznaczonych do zniszczenia.

5/ W przypadku stanowisk samodzielnych lub jednoosobowych stanowisk pracy – osoby zajmujące te stanowiska osobiście przedkładają do zniszczenia zbędne materiały zawierające dane osobowe.

6/ W przypadku fizycznej likwidacji urządzeń przetwarzających dane osobowe proces kasacji zostaje przeprowadzony przez Administratora Systemów Informatycznych w obecności osoby zlecającej kasację.

Na osobach sprzątających pomieszczenia Szpitala ciąży obowiązek zwracania szczególnej uwagi na zawartość koszy na śmieci – w przypadku znalezienia przez osobę sprzątającą pomieszczenia Szpitala w koszu na śmieci przedmiotów zawierających dane osobowe (np. wydruków komputerowych, kopii dokumentacji zawierającej dane osobowe, płyt CD, DVD itp.) – osoba sprzątająca jest zobowiązana zabezpieczyć te przedmioty i powiadomić o tym fakcie, w najbliższym możliwym czasie, Inspektora ochrony danych.

5/ Zagrożenie bezpieczeństwa danych osobowych i incydenty zagrażające bezpieczeństwu danych

- **zagrożenia bezpieczeństwa danych** oznaczają wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
- **incydent** oznacza takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
- **naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Do **typowych zagrożeń bezpieczeństwa danych** osobowych należy nieprzestrzeganie zasad ochrony danych osobowych (np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

Do **typowych incydentów zagrażających bezpieczeństwu danych** osobowych należą:

zdarzenia losowe:
pożar, zalanie, awarie serwera, awarie
komputerów, twardych dysków, oprogramowania, pomyłki informatyków,
użytkowników systemu informatycznego, utrata lub zagubienie danych;
umyślne incydenty:
włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub
sprzętu, wyciek informacji,
ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie
wirusów i innego
szkodliwego oprogramowania

6/ Procedura postępowania w przypadku naruszenia ochrony danych osobowych

1/ Każda osoba upoważniona przez Administratora danych do przetwarzania danych lub do przebywania w obszarach przetwarzania danych, która stwierdzi fakt naruszenia bezpieczeństwa danych jest zobowiązana niezwłocznie zgłosić to Inspektorowi ochrony danych; w przypadku, gdy poinformowanie Inspektora ochrony danych jest niemożliwe, fakt naruszenia ochrony danych należy zgłosić swojemu bezpośredniemu przełożonemu, który z kolei jest zobowiązany do zgłoszenia tego faktu Administratorowi danych, a w przypadku jego nieobecności, Administratorowi Systemów Informatycznych.

2/ Do czasu przybycia na miejsce Inspektora ochrony danych lub Administratora danych, lub Administratora Systemów Informatycznych należy:

- niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony danych (o ile to jest możliwe);
- ustalić przyczynę i sprawcę naruszenia ochrony danych (o ile jest to możliwe);
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

7/ Odpowiedzialność

1. Za przestrzeganie zasad dotyczących bezpieczeństwa przetwarzania danych osobowych, odpowiedzialni są wszyscy pracownicy Szpitala oraz osoby wykonujące na jego rzecz pracę w oparciu o umowy cywilnoprawne oraz umowy kontraktowe.

2. W przypadku pracowników Szpitala, których zakres obowiązków pracowniczych nie obejmuje konieczności przetwarzania danych osobowych, a które z racji tych obowiązków mogą mieć dostęp do pomieszczeń, w których przetwarza się dane osobowe – pracownicy Sekcji Gospodarczej, Sekcji Higieny Szpitalnej, Sekcji Technicznej, Kuchni i Pralni – nałożono obowiązek pisemnego oświadczenia zawierającego klauzulę zobowiązującą do zachowania w tajemnicy, nieujawniania i niewykorzystywania wszelkich informacji, z którymi zapoznali się z racji wykonywanych obowiązków, w szczególności dotyczących danych osobowych.

3. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień dotyczących zasad przetwarzania danych osobowych. **Przypadki, nieuzasadnionego zaniechania obowiązków pracowniczych w powyższym zakresie potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.**

Wobec osoby, która w przypadku naruszenia bezpieczeństwa przetwarzania danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła określonego działania, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi procedurami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

Kara dyscyplinarna nie wyklucza odpowiedzialności karnej tej osoby zgodnie z odpowiednimi przepisami, oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.