# DEKLARACJA ZARZĄDU

1. Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia 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) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się Politykę Bezpieczeństwa Informacji wraz z zestawem procedur.

2. Zarząd Szpitala Powiatowego w Rykach spółka z o. o., świadomy wagi problemów związanych z ochroną prawa do prywatności, w szczególności prawa osób fizycznych powierzających Szpitalowi swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklaruje zamiar:

    1) podejmowania działań niezbędnych dla ochrony praw związanych z bezpieczeństwem danych osobowych;
    2) stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Szpitalu w zakresie problematyki bezpieczeństwa tych danych;
    3) traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania;
    4) podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

3. Zarząd Szpitala deklaruje, że będzie stale doskonalić i rozwijać organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznymi tak, aby skutecznie zapobiegać zagrożeniom związanym z/ze:

    1) infekcjami wirusów i koni trojańskich, które instalując się na komputerze mogą wykradać zasoby tego komputera (zarówno stacjonarne jak i sieciowe);
    2) spamem, posiadającym niekiedy programy pozwalające wykradać zasoby komputera;
    3) dostępem do stron internetowych, na części których zainstalowane są skrypty pozwalające wykradać zasoby komputera;
    4) ogólnie dostępnymi komunikatorami internetowymi, w których występują luki, przez które można uzyskać dostęp do komputera;
    5) użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku poza Szpital;
    6) możliwością niekontrolowanego kopiowania danych na zewnętrzne, przenośne nośniki;

7) możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane;
8) lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez zabezpieczenia;
9) brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy;
10) atakami z sieci uniemożliwiającymi przetwarzanie (ataki typu DoS na serwer/serwery);
11) działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści;
12) kradzieżą sprzętu lub nośników z danymi, które zazwyczaj są niezabezpieczone.