**ZAŁĄCZNIK NR 2**

**RYZYKO W PODMIOCIE LECZNICZYM**

**I Zasady analizy ryzyka w podmiocie leczniczym**

1. Podmiot leczniczy wprowadza politykę zarządzania ryzykiem, której zadaniem jest monitorowanie zagrożeń dla działalności systemu ochrony danych osobowych podmiotu leczniczego.
2. Obowiązującym standardem w działalności podmiotu leczniczego jest przygotowanie się do następstw wystąpienia zagrożenia lub zagrożeń, określenie prawdopodobieństwa jego wystąpienia oraz zaplanowania działań na rzecz minimalizacji możliwości jego wystąpienia.
3. Procedurą analizy ryzyka objęte są wszystkie elementy działalności podmiotu leczniczego, a w szczególności te dziedziny, w których przetwarzane są dane osobowe dotyczące zdrowia pacjentów.
4. W trakcie analizy ryzyka należy wyodrębnić następujące elementy:

- aktywa – są to wszystkie środki i narzędzia mające istotne znaczenie dla podmiotu leczniczego,

- zagrożenia – są to przykłady potencjalnych naruszeń systemu,

- skutki – są to niepożądane następstwa zrealizowania się zagrożeń w praktyce,

- ryzyko – jest to prawdopodobieństwo, że zagrożenia się zrealizują i przyniosą konkretny, negatywny skutek dla aktywów.

**II Procedura analizy ryzyka w podmiocie leczniczym**

1. Administrator określa i definiuje zagrożenia jakie występują w podmiocie leczniczym. Wykaz potencjalnych zagrożeń znajduje się w załączniku nr 2 A.
2. Zagrożenia są identyfikowane z uwzględnieniem odniesienia się do aktywów.
3. Wyliczenie poziomu Ryzyka (R) następuje poprzez iloczyn określonego przez Administratora Prawdopodobieństwa (P) wystąpienia zagrożenia w podmiocie leczniczym i Skutku (S) wystąpienia takiego zagrożenia w podmiocie leczniczym tj. R = P x S.
4. Skalę Prawdopodobieństwa (P) wystąpienia zagrożenia obrazuje Tabela A.

Tabela A

|  |  |
| --- | --- |
| **Prawdopodobieństwo wystąpienia zagrożenia** | **Skala** |
| Wysokie | 3 |
| Średnie | 2 |
| Niskie | 1 |

1. Skalę Skutków (S) określa Tabela B. Do określenia skali stosuje się pomocniczo dodatkowe kryteria oceny pozwalające na prawidłowe oszacowanie potencjalnych strat.

Tabela B

|  |  |
| --- | --- |
| **Skutki wystąpienia zagrożenia** | **Skala** |
| Wysokie (utrata dobrego wizerunku, brak możliwości realizacji zadań, naruszenie prawa, incydent prasowy o charakterze ogólnopolskim, straty finansowe powyżej 100.000 zł) | 3 |
| Średnie (obniżenie dobrej reputacji na rynku, możliwe naruszenie prawa, incydent prasowy o charakterze lokalnym, straty finansowe powyżej 10.000 zł) | 2 |
| Niskie (wystąpienie nie ma wpływu na posiadane aktywa i działalność podmiotu leczniczego) | 1 |

1. Administrator, po dokonaniu wyliczenia Ryzyka (R) ma obowiązek odniesienia jego poziomu do skali i podejmuje dalsze działania związane z ryzykiem.
2. Skalę Ryzyka w podmiocie leczniczym określa tabela C.

Tabela C

|  |  |
| --- | --- |
| **Poziom ryzyka** | **Wartość ryzyka R = P x S** |
| Wysokie (należy przeprowadzić czynności mające na celu obniżenie ryzyka) | 9 |
| Opcjonalne (Administrator może je obniżyć lub zaakceptować) | 3-6 |
| Akceptowalne (pomijane) | 1-2 |

**III Reakcja na ryzyko w podmiocie leczniczym**

1. Jeśli ryzyko w podmiocie leczniczym jest na poziomie akceptowalnym, Administrator potwierdza jedynie, że zastosowane zabezpieczenia są właściwe.
2. W przypadku ryzyka na poziomie opcjonalnym Administrator musi ocenić czy jest możliwość obniżenia jego poziomu poprzez zastosowanie stosownych zabezpieczeń lub czy może je zaakceptować. W przypadku akceptacji ryzyka Administrator ma obowiązek jego monitorowania.
3. Listę potencjalnych zabezpieczeń w podmiocie leczniczym stanowi Załącznik nr 2 B.
4. W celu obniżenia poziomu ryzyka Administrator może przeprowadzić następujące czynności:
5. przeniesienie ryzyka – np. zakup ubezpieczenia, powierzenie procesów przetwarzania podmiotom zewnętrznym,
6. unikanie ryzyka – np. poprzez modyfikację procedur, które mają na celu wyeliminowanie potencjalnie niebezpiecznych sytuacji,
7. obniżanie ryzyka – np. poprzez zastosowanie zabezpieczeń, o których mowa w Załączniku nr 2 B.
8. W przypadku, kiedy ryzyko jest na poziomie nieakceptowalnym, Administrator po wprowadzeniu dodatkowych zabezpieczeń, przeprowadza ponowną analizę ryzyka.
9. Analiza ryzyka przeprowadzana jest za pomocą szablonu, o którym mowa w Załączniku nr 2 C.

**OCENA SKUTKÓW DLA SYSTEMU OCHRONY DANYCH W PODMIOCIE LECZNICZYM**

**I Ocena skutków dla ochrony danych w podmiocie leczniczym (DPIA)**

1. Ocena skutków dla ochrony danych - (DPIA – Data Protection Impact Assesment) – nałożony przez RODO obowiązek analizy w jaki sposób operacja przetwarzania danych osobowych (planowana a także już prowadzona) wpływa lub będzie wpływać na prawa i wolności osób, których dane są przetwarzane w ramach danej operacji przetwarzania.
2. DPIA stosowana jest dla operacji przetwarzania danych osobowych, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
3. Ocena skutków dla ochrony danych w praktyce przeprowadzana będzie dla wszelkich przedsięwzięć (np. projektów, zakupów urządzeń i nowych technologii) i procesów, podczas których przetwarzane są lub będą dane osobowe i z tym przetwarzaniem wiąże się ryzyko (obecnie lub w przyszłości) naruszenia praw i wolności osób fizycznych.
4. Operacje przetwarzania danych osobowych w podmiocie leczniczym mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, ponieważ:
5. Przetwarzane są dane osobowe wrażliwe oraz o charakterze wysoce osobistym,
6. Dane osobowe przetwarzane są na dużą skalę,
7. Przetwarzane są dane o stanie zdrowia/dane pacjentów,
8. Głównym przedmiotem działalności podmiotu leczniczego jest przetwarzanie danych pacjentów.
9. O konieczności przeprowadzania DPIA decyduje Administrator, po zasięgnięciu opinii u Inspektora Ochrony Danych Osobowych (IOD). Wykaz zbiorów lub operacji przetwarzania dla których jest przeprowadzana DPIA znajduje się w Załączniku nr 1.

**II Naruszenie praw i wolności**

1. Definicja naruszenia praw i wolności jest bardzo szeroka i ma charakter otwarty. Szczegółowe odniesienie się do zagrożeń w tej materii znajduje się w Motywie 75 RODO, ale wszystkie łączne przesłanki sprowadzają się do prawa do prywatności osób, których dane przetwarzamy.
2. W podmiocie leczniczym dodatkowo należy brać pod uwagę prawa osób, których dane są przetwarzane z perspektywy praw przysługujących im jako pacjentów podmiotu leczniczego.
3. Oceniając naruszenie praw i wolności należy odnieść się do szkód fizycznych oraz strat o charakterze materialnym i niematerialnym.

**III Odpowiedzialność za przeprowadzenie DPIA w podmiocie leczniczym**

1. Za przeprowadzanie DPIA oraz wszelką weryfikację konieczności jej przeprowadzania odpowiedzialność ponosi Administrator. Może on wyznaczyć dodatkowo pracownika, który będzie odpowiadał za realizację DPIA, jednak odpowiedzialność za brak lub niewłaściwe przeprowadzenie DPIA ponosi ADO.
2. Administrator danych przeprowadzając DPIA ma obowiązek konsultowania się z Inspektorem Ochrony Danych Osobowych.
3. Jeśli IOD oceni, że Administrator powinien przeprowadzić DPIA dla jakiegoś procesu w podmiocie leczniczym, winien poinformować o tym pisemnie Administratora. Ostateczna decyzja co do konieczności przeprowadzenia DPIA spoczywa na Administratorze.
4. Administrator może również zasięgnąć opinii w kwestii oceny skutków dla ochrony danych wśród osób, których dane osobowe są przetwarzane.
5. Wszelkie czynność związane z przeprowadzaniem DPIA lub oceną konieczności jej przeprowadzenia są dokumentowane i odbywają się pisemnie.
6. Jeżeli Administrator zasięga opinii IOD lub innych pracowników podmiotu leczniczego w zakresie DPIA musi pozostawić im rozsądny termin, nie krótszy niż 7 dni roboczych, na przekazanie przez nich pisemnej opinii.

**IV Elementy DPIA w podmiocie leczniczym**

1. Ocena wpływu na ochronę danych osobowych zawiera co najmniej następujące elementy:
2. Systematyczny opis planowanej operacji przetwarzania danych osobowych
3. Ocenę niezbędności i proporcjonalności przetwarzania danych w stosunku do celów przetwarzania,
4. Analizę i ocenę ryzyka w odniesieniu do potencjalnego naruszenia praw i wolności osób fizycznych wraz ze środkami minimalizującymi to ryzyko oraz uzasadnieniem dokonanego wyboru środków,
5. Określenie uczestników procesu DPIA,
6. Wyniki konsultacji z Inspektorem ochrony danych,
7. Opinie osób, których dane dotyczą lub ich przedstawicieli, gdy ich zasięgnięto.
8. Szczegółowy opis części elementów DPIA znajduje się w załączniku numer 2 D.
9. Jeżeli przeprowadzona w ramach DPIA analiza ryzyka wskazuje na wysokie ryzyko szczątkowe, Administrator ma obowiązek zwrócić się pisemnie o uprzednie konsultacje w celu przetwarzania do organu nadzorczego.
10. Administrator zwraca się do organu nadzorczego niezwłocznie, jednak nie później niż 14 dni od zakończenia oceny skutków operacji dla ochrony danych osobowych. Administrator dostarcza organowi nadzorczemu dokumentację DPIA.

**V Publikacja DPIA**

1. Zaleca się Administratorowi publikację wyników przeprowadzanej DPIA jeżeli operacje przetwarzania mają istotny wpływ na liczną grupę odbiorców.
2. Publikacji może podlegać całość lub część dokumentu albo jego podsumowanie z zastrzeżeniem braku konieczności ujawniania systemów zabezpieczeń lub innych informacji poufnych lub stanowiących tajemnicę podmiotu leczniczego.