



**Podstawowe zasady związane z bezpieczeństwem informacji obowiązujące Dostawców (Wykonawców)
na terenie Szpitala Uniwersyteckiego w Krakowie**

Przedstawione poniżej zasady wynikają z wymagań 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) (Dz.U.UE.L.2016.119.1), zwanego dalej „RODO”.

Ochrona informacji polega na zabezpieczeniu informacji zbieranej, utrwalanej, wprowadzanej, przetwarzanej, opracowywanej, zmienianej, udostępnianej, przesyłanej i składowanej w systemie informacyjnym **przed nieautoryzowanym ujawnieniem, przetwarzaniem, kradzieżą oraz nieuprawnioną modyfikacją lub usunięciem.**

Ochrona informacji polega na zapewnieniu jej **poufności, integralności i dostępności.**

- przez **poufność** rozumiemy zapewnienie, iż dostęp do informacji mają tylko i wyłącznie osoby uprawnione.
- poprzez **integralność** rozumiemy zapewnienie, iż informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób (niezgodny z wewnętrznymi regulacjami).
- poprzez **dostępność** rozumiemy zapewnienie, iż informacje będą dostępne na żądanie uprawnionej do tego osoby.

1. Dostawcy (Wykonawcy) zobowiązują się **akceptować i stosować wszystkie obowiązujące w Szpitalu Uniwersyteckim zasady** związane z bezpieczeństwem informacji - odpowiednio do rodzaju i zakresu przyznanego im dostępu do zasobów informacyjnych.
2. **Dostawcy (Wykonawcy) współpracujący ze Szpitalem Uniwersyteckim odpowiedzialni są w szczególności za:**
 - a. **zapoznanie się z przepisami prawa** w zakresie bezpieczeństwa informacji w szczególności z przepisami dotyczącymi ochrony danych osobowych,
 - b. **zapewnienie bezpieczeństwa informacji**, w tym przetwarzanych danych osobowych m.in. poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem,
 - c. **zachowanie w tajemnicy wszelkich informacji**, a w szczególności danych osobowych, które przetwarzają oraz sposobów ich zabezpieczenia uzyskanych w związku z realizacją umowy zawartej ze Szpitalem Uniwersyteckim,
 - d. **stosowanie środków technicznych i organizacyjnych** zapewniających ochronę informacji,
 - e. **informowanie Inspektora Ochrony Danych Szpitala Uniwersyteckiego** o każdym zauważonym przypadku naruszenia bezpieczeństwa.

Inspektora Ochrony Danych – pracownik odpowiedzialny za bezpieczeństwo informacji, nadzorujący przestrzeganie przepisów RODO.



3. W przypadku stwierdzenia **naruszenia bezpieczeństwa informacji** Dostawca (Wykonawca) współpracujący ze Szpitalem Uniwersyteckim jest zobowiązany:
 - a. **powiadomić Inspektora Ochrony Danych** o podejrzeniu lub fakcie naruszenia bezpieczeństwa informacji w szczególności ochrony danych osobowych i powiadomić osoby odpowiedzialne za realizację umowy,
 - b. **powstrzymać się od wszelkich działań** mogących utrudnić ustalenie okoliczności naruszenia,
 - c. **przygotować notatkę** opisującą naruszenie bezpieczeństwa informacji.
4. **W trakcie realizacji umowy zawartej** ze Szpitalem Uniwersyteckim osoba odpowiedzialna za realizację tej umowy ze strony Szpitala Uniwersyteckiego w porozumieniu z Inspektorem Ochrony Danych **może uznać za konieczne i zażądać podpisania imiennych oświadczeń** o zachowaniu poufności przez Pracowników Dostawcy (Wykonawcy).