SPIS TREŚCI:

1. ZASADY OGÓLNE

1.1. Niniejszy dokument określa podstawowe zasady odnoszące się do postępowania w relacjach z dostawcami, ze szczególnym uwzględnieniem występujących w nich ryzyk oraz zasad zachowania bezpieczeństwa informacji. W ramach relacji z dostawcami chcemy promować świadome podejście do ryzyk, które mogą występować w trakcie współpracy i bezpieczeństwa informacji, dostrzegając przy tym znaczący ich wkład w kształtowanie się biznesowej kultury zaufania.

1.2. Zasady postępowania mają zastosowanie do wszystkich aktualnych lub potencjalnych dostawców / wykonawców towarów i usług zewnętrznych.

1.3. Usługami zewnętrznymi w Szpitalu mogą być między innymi:

- szkolenia,
- usługi budowlane,
- pomoc techniczna w zakresie aplikacji komputerowych,
- naprawa komputerów i sprzętu IT,
- naprawa aparatury i sprzętu medycznego,
- dostarczanie systemów IT,
- dostarczanie aparatury medycznej,
- obsługi kadrowe,
- usługi księgowe,
- ochrona budynków i mienia,
- wideo monitoring budynku,
- sprzątanie,
- wywóz śmieci i nieczystości,

- usługi BHP (w tym szkolenia w zakresie BHP),
- usługi doradcze,
- usługi kserograficzne (drukowanie, kopiowanie),
- świadczenia opieki zdrowotnej,
- transport.

2. BEZPIECZEŃSTWO INFORMACJI W RELACJACH Z DOSTAWCAMI

2.1. System zarządzania bezpieczeństwem informacji w relacji do zewnętrznych usługodawców powinien obejmować w szczególności:

a) analizę dostawców w ramach identyfikacji kontekstu działalności organizacji w celu podejmowania odpowiednich działań prewencyjnych,
b) ocenę wpływu dostawców jako strony zainteresowanej na zakres systemu zarządzania bezpieczeństwem informacji,
c) uwzględnienie relacji z dostawcami w analizie ryzyka bezpieczeństwa informacji,
d) nadzór nad bezpieczeństwem informacyjnym procesów lub zamówień, których wykonanie zlecono na zewnątrz.

2.2. W praktyce bezpieczeństwo informacji z relacjach z dostawcami oznacza kierowanie się trzema atrybutami:

a) **Dostępność** – czyli zapewnienie upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami, w relacji z dostawcami przez potrzebę należy rozumieć wykonanie kontraktu lub zlecenia;
b) **Poufność** – czyli zapewnienie, że informacje są dostępne tylko dla osób do tego uprawnionych, w szczególności będą to pracownicy lub podwykonawcy dostawcy, dla których wykonanie kontraktu lub zlecenia będzie wymagało dostępu do informacji poufnych [chronionych].
c) **Integralność** – czyli zagwarantowanie dokładności i kompletności informacji, oraz metod ich przetwarzania; poprzez sformalizowanie zasad współpracy z dostawcami.

3. IDENTYFIKACJA ZAGROŻEŃ.

3.1. Ryzyka związane z bezpieczeństwem informacji.

Rodzaj ryzyka	Zakres występowania ryzyka	Opis
Kradzież sprzętu komputerowego, urządzenia mobilnego laptop, smartfon, itp.), urządzenia medycznego przetwarzającego dane lub zewnętrznych nośników pamięci.	Firmy serwisujące, sprzątające, remontowe, szkoleniowe. Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku SP ZOZ MSWiA w Katowicach	Dotyczy głównie kradzieży urządzeń mobilnych oraz zewnętrznych nośników pamięci, pozostawionych w ogólnie dostępnych miejscach, do których dostęp posiadają również firmy zewnętrzne świadczące różnego rodzaju usługi w budynku SP ZOZ MSWiA w Katowicach

Fizyczna kradzież dokumentów	Firmy serwisujące, sprzątające, remontowe, szkoleniowe. Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku SP ZOZ MSWiA w Katowicach	Dotyczy kradzieży dokumentów papierowych pozostawionych o ogólnie dostępnych miejscach w wyniku niefrasobliwości pracowników w budynku SP ZOZ MSWiA w Katowicach, jak również w wyniku celowego działania
Brak sformalizowanych zasad współpracy z zewnętrznymi dostawcami towarów lub usług	Wszyscy aktualni i potencjalni dostawy	Brak formalnych zasad współpracy skutkuje niewiedzą dostawców w zakresie polityki bezpieczeństwa informacji, postępowania z informacjami poufnymi i sposobami zgłaszania incydentu naruszenia bezpieczeństwa informacji. Jednocześnie może oznaczać brak procedur zapewniających bezpieczeństwo danych oraz brak zdefiniowanych kar za naruszenie bezpieczeństwa danych
Zniszczenie lub uszkodzenie sprzętu komputerowego/lub nośników pamięci	Firmy serwisujące, sprzątające, remontowe, szkoleniowe. Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku SP ZOZ MSWiA w Katowicach	Działanie tego typu może być zamierzone (celowe) lub niezamierzone będące skutkiem wykonywania prac/usług w budynku SP ZOZ MSWiA w Katowicach, np. w wyniku nienależytego zabezpieczenia sprzętu komputerowego w trakcie wykonywania usługi, korzystania z wadliwych urządzeń specjalistycznych do wykonania usługi, nienależytego przeszkolenia pracowników dostawcy
Korzystanie z portali B2B (business-to-business) dostawcy	Wszyscy dostawcy wymagający realizacji bieżących zamówień poprzez własne portale typu B2B	Korzystanie z portali B2B dostawców, oznacza przechowywanie danych handlowych (lista zamawianych produktów, ceny, rabaty) na zewnętrznych serwerach, co wiąże się z ograniczonym wpływem na kontrolę sposobu w jaki są chronione
Przekazywanie informacji nieuprawnionym podmiotom (poprzez realizację usługi przez niezdefiniowanych wcześniej podwykonawców)	Potencjalnie wszyscy dostawcy, którzy przy realizacji kontraktu lub zlecenia mogą korzystać z pomocy podwykonawców	Ryzyko odnosi się do sytuacji, w której dostawca nie poinformował wcześniej o realizowaniu kontraktu lub zlecenia przy pomocy podwykonawców, przez co pozostają oni nierozpoznani i niezidentyfikowani dla SP ZOZ MSWiA w Katowicach

Ujawnienie danych poufnych	Wszyscy aktualni i potencjalni dostawcy	Może mieć charakter przypadkowy lub celowy. Może wystąpić zarówno w wyniku zaniedbań pracowników SP ZOZ MSWiA w Katowicach jak i pracowników zewnętrznego dostawcy. Skutkuje to narażeniem na szwank reputacji szpitala lub ewentualnymi konsekwencjami prawnymi. Przykładem przypadkowego ujawnienia danych jest wyrzucenie na śmietnik wydruków archiwalnych szpitala lub utylizacja komputerów bez uprzedniego należytego zniszczenia dysków twardych. Celowym ujawnieniem informacji poufnych może być umieszczenie w Internecie przez nielojalnego pracownika dostawcy części kodu źródłowego istotnego dla funkcjonowania w SP ZOZ MSWiA w Katowicach oprogramowania
Zniszczenie danych (np. w postaci papierowej)	Firmy serwisujące, sprzątające, remontowe, szkoleniowe. Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku SP ZOZ MSWiA w Katowicach	Może mieć charakter przypadkowy - kiedy do zniszczenia dokumentów dochodzi w wyniku źle wykonywanej usługi (np. przy braku zabezpieczenia dokumentów podczas wykonywania prac remontowo-konserwatorskich), lub celowy - kiedy jest wynikiem złej woli
Dostęp do haseł zapisanych w postaci papierowej	Firmy serwisujące, sprzątające, remontowe, szkoleniowe, kurierskie Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku SP ZOZ MSWiA w Katowicach	Skutkuje uzyskaniem dostępu do ważnych aplikacji, które mogą zawierać informacje poufne lub kluczowe dla funkcjonowania SP ZOZ MSWiA w Katowicach
Brak szkoleń z zakresu bezpieczeństwa informacji dla pracowników zewnętrznych dostawców	Firmy serwisujące, sprzątające, remontowe, szkoleniowe, kurierskie Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku SP ZOZ MSWiA w Katowicach	Zagrożenie może wystąpić w sytuacji, kiedy procedury z zakresu bezpieczeństwa informacji są na tyle złożone, iż wymagają oddzielnych szkoleń dla pracowników zewnętrznych dostawców prowadzonych przez przedstawicieli SP ZOZ MSWiA w Katowicach
Brak nadzoru nad pracą serwisów zewnętrznych	Firmy serwisujące i remontowe	Zbyt duże zaufanie do dostawców, które skutkuje pozostawieniem ich bez nadzoru w miejscach, w których mają dostęp do dokumentacji i informacji poufnych
Pomyłki pracowników	Wszyscy aktualni i potencjalni dostawcy	Wynikające z indywidualnych pomyłek pracowników, będące skutkiem niedopatrzenia, braku koncentracji lub niefrasobliwości (np. przesłanie do dostawcy niewłaściwego maila, zawierającego informacje nie przeznaczone dla niego)

Zbyt duże uprawnienie dostępu do budynków i pomieszczeń dla firm zewnętrznych	Firmy serwisujące, sprzątające, remontowe, szkoleniowe, kurierskie Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku SP ZOZ MSWiA w Katowicach	Zbyt duża swoboda poruszania się po budynkach i dostępu do pomieszczeń służbowych, w których przechowywane są dokumenty mogące zawierać informacje poufne
Zbyt duże uprawnienie dostępu do infrastruktury teleinformatycznej dla firm zewnętrznych	Firmy serwisujące, sprzątające, remontowe, szkoleniowe, kurierskie Wszystkie firmy zewnętrzne wykonujące usługi regularne lub jednorazowe w budynku SP ZOZ MSWiA w Katowicach. Dostawcy wszelkiego rodzaju usług np.: systemy BMS, systemy wentylacji / klimatyzacji, sterowania systemami zasilania, dostawcy gazów medycznych, systemy medyczne (PET, CT, RM, KTG, monitoring pacjenta), urządzenia medyczne itd.	Dostęp do infrastruktury teleinformatycznej może umożliwić podłączenie nieautoryzowanych przez SP ZOZ MSWiA w Katowicach urządzeń lub systemów umożliwiających między innymi zdalny dostęp do infrastruktury SP ZOZ MSWiA w Katowicach, stwarza ryzyko przełamania zabezpieczeń infrastruktury bądź przejęcia sterowaniem systemem bądź urządzeniami przez osoby nieuprawnione co może skutkować naruszeniem danych osobowych, brakiem zachowania ciągłości działania oraz bezpośrednim zagrożeniem dla życia i zdrowia pacjentów. Naraża na szwank reputację szpitala i może skutkować ewentualnymi konsekwencjami prawnymi. Może mieć charakter przypadkowy lub celowy. Może wystąpić zarówno w wyniku zaniedbań pracowników SP ZOZ MSWiA w Katowicach jak i pracowników zewnętrznego dostawcy.
Duża rotacja pracowników firm zewnętrznych / brak dedykowanych opiekunów do realizacji kontraktu	Wszyscy aktualni i potencjalni dostawcy	Duża rotacja skutkuje przekazywaniem informacji zbyt dużej liczbie pracowników dostawcy. Brak dedykowanych opiekunów oznacza chaos informacyjny i brak transferu wiedzy.

Utrata wsparcia technicznego	Głównie dostawcy specjalistycznego lub dedykowanego oprogramowania.	Utrata wsparcia technicznego jest szczególnie groźna w przypadku oprogramowania niestandardowego, tworzonego na potrzeby SP ZOZ MSWiA w Katowicach. W przeciwieństwie do sprzętu, którego podzespoły zazwyczaj dostępne są na rynku i który można łatwo zastąpić innym o zbliżonych lub nawet tych samych parametrach wymiana oprogramowania bywa trudna i skomplikowana. Wiąże się często z koniecznością przeprowadzenia długotrwałego wdrożenia i konwersji danych między systemami. Najczęściej problem ten występuje w przypadku: - upadłości lub likwidacji właściciela oprogramowania, - zmiany formy prawnej lub organizacyjnej organizacji, - wygaśnięcia dotychczasowych umów, - zaprzestania wsparcia oprogramowania w związku z wprowadzeniem nowych wersji, - brakiem porozumienia, które może mieć przyczyny biznesowe, ekonomiczne, społeczne lub personalne

3.2. Ryzyka wynikające z korzystania z usług typu cloud computing.

Rodzaj ryzyka	Zakres występowania ryzyka	Opis
Przesunięcie kompetencji administratora danych, na dostawcę usługi w chmurze	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	Administrator nie zauważa naruszeń bezpieczeństwa informacji (poufności, integralności, dostępności danych), przywiązuje do nich mniejszą wagę. Działania te mogą prowadzić do popełnienia czynów naruszających przepisy ochrony danych i prywatności. Administrator danych lub strona trzecia nie będzie w stanie na odpowiednim poziomie monitorować dostawcy usługi w chmurze
Brak zdefiniowanych tzw. wiążących reguł korporacyjnych (BCR)	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	BCR zawierają indywidualne warunki, które nakładają na podmioty z nimi powiązane określone obowiązki w zakresie zwiększenia bezpieczeństwa danych. Dostawca cloud, który zobowiąże się do przestrzegania BCR jest bardziej wiarygodny, co wpływa na zwiększenie poziomu zaufania do swoich usług

Nieprzestrzeganie zdefiniowanych BCR (Wiążące zasady korporacyjne)	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, niewymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	Dostawca nie przestrzega wcześniej ustalonych BCR co skutkuje brakiem należytego zabezpieczenie danych
Przekazanie danych do jurysdykcji, które nie zapewniają odpowiedniego poziomu ochrony.	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	Dane mogę być przechowywane na serwerach znajdujących się poza granicami Polski, w kraju, gdzie obowiązuje inne prawo odnośnie zachowania bezpieczeństwa informacji
Brak możliwości ustalenia odpowiedzialności w łańcuchu usługodawców.	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	Jeżeli dostawca cloudcomputingu będzie korzystał z podwykonawców (firmy przetwarzające dane), to ustalenie odpowiedzialności w łańcuchu usługodawców może być niezwykle trudne
Wykorzystanie danych administratorów bez ich zgody	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	Istnieje ryzyko, iż korzystając z cloudcomputingu straci się kontrolę nad danymi i ich przetwarzaniem. Największym zagrożeniem jest możliwość wykorzystania danych administratorów danych przez dostawców usług cloud lub ich podwykonawcy do własnych celów bez wiedzy lub zgody administratorów danych
Zablokowanie dostępu do usługi	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	W zależności od specyfiki działalności jak również czasu wystąpienia tego typu awarii, straty związane z brakiem dostępu do zasobów organizacji będą różne, uzależnione od wielu czynników, min. poziomu uzależnienia codziennej pracy od dostępu do zablokowanej usługi
Utrata danych	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	Może ona nastąpić zarówno w wyniku przypadkowego jak i celowego usunięcia zbiorów danych, a także uszkodzenia urządzeń służących do ich przechowywania. Skasowanie informacji często wiąże się z bezpowrotną utratą ich części lub całości. Dodatkowo skasowanie niewielkiej liczby danych może przez długi czas pozostać niezauważone

Vendor lock-in czyli uzależnienie od dostawcy	Wszyscy aktualni oraz potencjalni dostawcy oferujący usługi w chmurze lub licencjonowany dostęp do usługi, nie wymagający wykorzystania infrastruktury informatycznej SP ZOZ MSWiA w Katowicach	Uzależnienie kluczowych procesów w firmie bez uzgodnienia zasad zakończenia współpracy lub rozwiązania umowy oraz "odzyskania" przekazanych danych

3.3. Zakres umów z dostawcami oferującymi usługi z wykorzystaniem cloud computing.
Odpowiednio sformułowana umowa powinna zawierać między innymi klauzule:

- umożliwiające przenoszenie danych (portability) i kontrolowanie ich,
- zakazujące nielegalnego przekazywanie danych do jurysdykcji, bez wystarczającego poziomu ochrony danych,
- dostawca usług opartych o cloud powinien zapewnić, że usunięcie danych osobowych z dysków oraz z innych nośników może być przeprowadzone w skuteczny sposób.

Istotne jest także zabezpieczenie dostępu do danych. Nikt poza klientem usług w chmurze nie powinien mieć dostępu do jego danych. Umowa lub inna forma porozumienia z dostawcą, powinna gwarantować także odpowiednie tworzenie i zapisywanie kopii zapasowych w bezpiecznych lokalizacjach oraz wprowadzać zasadę przejrzystości lokalizacji, w których dane mogą być przechowywane i przetwarzane.

4. PRZETWARZANIE DANYCH PRZEZ USŁUGODAWCÓW ZEWNĘTRZNYCH

W przypadku, gdy usługi zewnętrzne obejmują przetwarzanie danych (w szczególności danych o wysokim stopniu poufności [dane chronione w tym dane osobowe]) poza infrastrukturą teleinformatyczną SP ZOZ MSWiA w Katowicach (np. w modelu cloud computing lub innych formach modelu Application Service Provision, w zewnętrznych centrach przetwarzania danych itp.), należy w szczególności:

- wprowadzić odpowiednie mechanizmy kontrolne zapewniające poufność tych danych (np. poprzez ich szyfrowanie),
- zapewnić, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez dostawcę,
- zapewnić skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia),
- zagwarantować możliwość weryfikacji stosowanych przez dostawcę mechanizmów kontrolnych, w tym w zakresie środków ochrony i kontroli dostępu do pomieszczeń usługodawcy, w których odbywa się świadczenie usług na rzecz SP ZOZ MSWiA w Katowicach.

5. ZASADY POSTĘPOWANIA Z INFORMACJAMI POUFNYMI.

5.1. W niniejszym dokumencie przyjmuje się, że informacje poufne [chronione], to wszystkie przekazane dostawcy informacje, materiały oraz dokumenty, które nie są publicznie udostępniane przez SP ZOZ

MSWiA w Katowicach. Przetwarzanie informacji należących do SP ZOZ MSWiA w Katowicach przez dostawców / wykonawców musi odbywać się z uwzględnieniem klasyfikacji informacji.

	Opis	Zasady oznaczania	Zasady kontroli	Zasady kopiowania	Dystrybucja informacji
Publiczne	Nie wymagające dodatkowych zabezpieczeń, ich utrata nie spowoduje istotnych szkód i strat; informacje nie mające wpływu na ciągłość działania SP ZOZ MSWiA w Katowicach oraz jej wartości materialne i prawne	Umieszcza się w nagłówku - **kategoria jawności: III (publiczne)**	Brak szczególnych zasad bezpieczeństwa	Brak szczególnych zasad bezpieczeństwa	Brak szczególnych zasad bezpieczeństwa
Wewnętrzne	Informacja dostępna wszystkim pracownikom SP ZOZ MSWiA w Katowicach, dostęp na podstawie oświadczenia o zapoznaniu się z zasadami ochrony informacji obowiązującymi w SP ZOZ MSWiA w Katowicach, chronione przed nieuprawnioną modyfikacją, utrata może mieć wpływ na ciągłość działania SP ZOZ MSWiA w Katowicach oraz jej wartości materialne i prawne;	Umieszcza się w nagłówku dokumentu **kategoria jawności: II (wewnętrzne)** lub na segregatorze / kopercie. Jeśli jest taka możliwość	Wytwórca informacji odpowiedzialny jest za właściwe oznaczenie informacji Właściciel grupy informacji odpowiada za przydział do odpowiedniej grupy informacji zgodnie z załącznikiem nr 2 do PO 30/2016 Odbiorca informacji: odpowiedzialny za należyte przechowywanie i kontrolę nośnika informacji (wersja tradycyjna, elektroniczna)	Limitowane kopie, mogą być zrobione tylko przez uprawnionych pracowników albo przez kontrahentów i osoby trzecie, które podpisały odpowiednie oświadczenie poufności	Na zewnątrz organizacji: zaleca się odpowiednie zabezpieczenie np. używanie zamkniętych kopert. Forma elektroniczna: zaleca się przekazywanie za pośrednictwem wewnętrznej poczty. Możliwe umieszczanie w zasobach sieciowych SP ZOZ MSWiA w Katowicach (np. foldery sieciowe, ikonka "i"). W przypadku zewnętrznego konta zaleca się szyfrowanie transmisji. Faksowanie: zaleca się zwrócenie szczególnej uwagi na numer faksu, na który jest wysyłana informacja. Faks powinien być dostępny tylko dla osób upoważnionych.

Chronione	Informacje o istotnym znaczeniu dla funkcjonowania SP ZOZ MSWiA w Katowicach, zasady ochrony tych informacji regulują przepisy zewnętrzne oraz wewnętrzne, utrata informacji może spowodować istotne utrudnienie w działalności statutowej, mieć wpływ na ciągłość działania SP ZOZ MSWiA w Katowicach oraz jej wartości materialne i prawne	Umieszcza się w nagłówku dokumentu **kategoria jawności: I (chronione)** lub na segregatorze / kopercie. Jeśli jest taka możliwość.	Wytwórca informacji odpowiedzialny jest za upewnianie się, że chroniona informacja jest wykorzystywana zgodnie z przeznaczeniem/celem Odbiorca informacji odpowiedzialny jest za upewnianie się, że poufna informacja jest zakodowana i/lub znajduje się w zabezpieczonym pomieszczeniu/szafie pod kluczem.	Limitowane kopie mogą być zrobione tylko na podstawie pozwolenia wytwórcy informacji albo wg określonych przez niego zasad. Wymagane jest udokumentowanie faktu przekazania informacji. Wymagane jest upoważnienie do przetwarzania danych osobowych lub odrębne pełnomocnictwo.	Wewnętrznie: wykorzystanie kopert / teczek; dostarczać „do rąk własnych" jeśli to możliwe. Na zewnątrz organizacji: używać zwykłej zaklejonej koperty. Dostarczać „do rąk własnych" albo wysyłać przez zaufanego kuriera. Forma elektroniczna: wysyłać tylko jako zaszyfrowane dane lub umieszczać w zasobie sieciowym dostępnym tylko dla upoważnionych osób. Faksowanie: wymaga się potwierdzenia, wydruku/raportu poprawnego przesłania dokumentu niezwłocznie po wysłaniu dokumentu

- Osoby reprezentujące podmiot zewnętrzny, z którym SP ZOZ MSWiA w Katowicach zawarł umowę, mogą uzyskać dostęp do informacji należących do SP ZOZ MSWiA w Katowicach wyłącznie po podpisaniu umowy o współpracę / zlecenia oraz dokumentu regulującego zasady i odpowiedzialność związaną z zachowaniem poufności przekazywanych informacji.
- W przypadku powierzenia przetwarzania danych osobowych wymagane jest zawarcie umowy powierzenia przetwarzania danych osobowych zgodnie obowiązującym w SP ZOZ MSWiA w Katowicach *[załącznik nr 1].*
- Każdy z pracowników podmiotu zewnętrznego może posiadać dostęp wyłącznie do informacji, które są mu niezbędne do prawidłowej i sprawnej realizacji zadań i obowiązków wynikających z umowy podpisanej pomiędzy podmiotem zewnętrznym a SP ZOZ MSWiA w Katowicach.
- Dostawcy / Wykonawcy zobowiązują się akceptować i stosować wszystkie obowiązujące w SP ZOZ MSWiA w Katowicach zasady związane z bezpieczeństwem informacji - odpowiednio do rodzaju i zakresu przyznanego im dostępu do zasobów informacyjnych.
- Oznaczanie informacji powstałych w wyniku pracy intelektualnej pracowników Dostawców / Wykonawców powinno być czytelne i nie pozostawiać wątpliwości, co do klasy oraz właściciela. Identyfikacja dotyczy wszystkich zapisów (w wersji ustnej, papierowej i elektronicznej).
- W przypadku wątpliwości dotyczących właściwej klasyfikacji informacji oraz w sytuacji, gdy mamy do czynienia z informacjami niesklasyfikowanymi, należy bezwzględnie traktować je jak informacje o najwyższym stopniu ochrony.
- Nośniki mobilne zawierające informacje należące do SP ZOZ MSWiA w Katowicach sklasyfikowane jako wewnętrzne i chronione muszą zostać zaszyfrowanie programem wykorzystującym minimum standard AES 256.

- W przypadku zbywania lub wycofywania z użytku dokumentów lub nośników elektronicznych zawierających informacje wrażliwe (czyli wewnętrzne i/lub chronione) należy usunąć je w sposób uniemożliwiający odtworzenie.
  - zapisy elektroniczne powinny być niszczone specjalnym oprogramowaniem lub/i fizycznie.
  - zapisy papierowe muszą być niszczone w niszczarkach o klasie bezpieczeństwa minimum P-4.

6. WYMAGANIA WZGLĘDEM DOSTAWCÓW / WYKONAWCÓW

6.1. Zarządzanie hasłami i kontami

6.1.1 Obowiązkiem dostawcy / wykonawcy jest ustanowienie odpowiedniego procesu zarządzania hasłami w systemach mających styczność z informacjami należącymi do SP ZOZ MSWiA w Katowicach z uwzględnieniem następujących zasad:

- Przydzielanie haseł do systemów, w których znajdują się informacje należące do SP ZOZ MSWiA w Katowicach musi być realizowane przez wyznaczony zespół lub osobę.
- Hasła powinny być unikatowe oraz spełniać wymagania dla tzw. „silnych" haseł, składających się z co najmniej 15 znaków zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.
- Nie należy stosować tych samych haseł do różnych systemów informatycznych, programów, portali, poczty e-mail itp.
- Zalecane jest zmienianie hasła co najmniej co 90 dni, nowe hasło nie może być powtórzeniem wcześniej stosowanych haseł.
- Przechowywanie haseł w wersji czytelnej niezależnie od tego czy są przechowywane w plikach czy zapisywane na papierze jest zabronione.
- Zabrania się zapamiętywania haseł na potrzeby procesów automatycznego logowania w programach takich jak przeglądarki internetowe, programy pocztowe itp.
- W przypadku, gdy hasło zostanie ujawnione lub gdy zaistnieje chociażby podejrzenie ujawnienia niepowołanym osobom należy je natychmiast zmienić lub zablokować konto.

6.1.2 Logowanie do systemów Podmiotu Zewnętrznego przetwarzających informacje należące do SP ZOZ MSWiA w Katowicach z kawiarenek internetowych oraz innych urządzeń, które nie są administrowane przez Podmiot Zewnętrzny lub w miejscach nie przystosowanych do przetwarzania danych osobowych jest zabronione.

6.1.3 Wszystkie pliki oraz bazy danych zawierające hasła mogą być przechowywane wyłącznie w postaci zaszyfrowanej oraz chronione przed dostępem nieupoważnionych osób. W tym celu należy stosować techniki kryptograficzne oraz zapewnić odpowiednie środki bezpieczeństwa fizycznego urządzeń przetwarzających hasła.

6.1.4 Współdzielenie kont i haseł jest zabronione. Każda z osób posiadająca dostęp do systemów musi posiadać indywidualne konto dostępowe. Właściciel konta odpowiedzialny jest za wszystkie czynności zrealizowane przy jego użyciu.

6.2. Urządzenia przenośne i praca na odległość

6.2.1 Zaleca się, aby Podmiot Zewnętrzny ustanowił proces zabezpieczenia urządzeń przenośnych oraz nośników danych.
Proces musi uwzględniać następujące wytyczne:

- Pracownik zobowiązany jest dostarczyć podpisane oświadczenie dotyczące przestrzegania zasad dotyczących korzystania z urządzeń przenośnych podczas pracy poza siedzibą Podmiotu Zewnętrznego.
- Oprogramowanie na urządzeniach mobilnych wykorzystywanych przez pracowników Podmiotu Zewnętrznego powinno pochodzić wyłącznie z zasobów firmy oraz być zarejestrowane i zweryfikowane pod kątem legalności.
- W przypadku używania prywatnych urządzeń przenośnych lub nośników danych – Pracownik Podmiotu Zewnętrznego musi uzyskać akceptację osób z kierownictwa firmy.
- Podmiot Zewnętrzny musi zapewnić bezpieczeństwo urządzeń przenośnych i nośników z uwzględnieniem wymuszonych haseł BIOS, wygaszaczy (np. po 15 min) oraz szyfrowania.

6.2.2 Dostęp pracowników Podmiotu Zewnętrznego z sieci publicznych do jego systemów IT zawierających informacje SP ZOZ MSWiA w Katowicach może być realizowany wyłącznie przy użyciu metod kryptograficznych takich jak VPN, tunele IPSec.

6.2.3 Komputery osobiste pracowników Podmiotu Zewnętrznego muszą być zabezpieczone za pomocą aktualnych i legalnych programów antywirusowych.

6.2.4 Infrastruktura przetwarzająca informacje SP ZOZ MSWiA w Katowicach musi być chroniona za pomocą urządzeń typu Firewall.

6.3. Kopie bezpieczeństwa danych

6.3.1 Podmiot Zewnętrzny odpowiedzialny jest za wdrożenie i nadzorowanie procesu tworzenia kopii bezpieczeństwa wraz możliwością odzyskania danych i przywrócenia funkcji biznesowych w obszarze, gdzie są przetwarzane Informacje należące do SP ZOZ MSWiA w Katowicach.

6.4. Poczta elektroniczna

6.4.1 Podmiot Zewnętrzny odpowiedzialny jest za ustanowienie, wdrożenie i nadzorowanie procesu związanego z przepływem informacji za pomocą poczty elektronicznej.

6.4.2 Poczta elektroniczna musi być przetwarzana wyłącznie przy użyciu urządzeń będących własnością lub zaakceptowanych przez Podmiot Zewnętrzny.

6.4.3 Przechowywanie i przetwarzanie informacji będących własnością SP ZOZ MSWiA w Katowicach przy pomocy systemów pocztowych nienależących do Podmiotu Zewnętrznego np. gmail.com, hotmail.com jest zabronione.

6.4.4 Podmiot Zewnętrzny powinien zwrócić uwagę pracownikom na niewłaściwość wykorzystywania konta pocztowego do dystrybucji treści określanych mianem „spamu", łańcuszków szczęścia oraz innych niepożądanych wiadomości.

6.4.5 System poczty elektronicznej Podmiotu Zewnętrznego musi specyfikować informacje (sygnatura) identyfikujące właściciela danego konta pocztowego takie jak: Imię, Nazwisko, nazwę obejmowanego stanowiska oraz nazwę firmy.

6.4.6 Zasady dotyczące poczty elektronicznej powinny jasno określać zakaz otwierania załączników poczty elektronicznej pochodzących z niewiadomych źródeł.

6.4.7 Podmiot Zewnętrzny zobowiązany jest wdrożyć system ochrony antywirusowej w zakresie poczty elektronicznej.

6.5. Ochrona danych osobowych

6.5.1 Podmiot zewnętrzny powinien zapewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679w 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: RODO) i chroniło prawa osób, których dane dotyczą. W szczególności powinien zagwarantować, że:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora,
- zapewnia, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy,
- podejmuje wszelkie środki zapewniające bezpieczeństwo przetwarzania na mocy art. 32 RODO.
- w miarę możliwości pomaga administratorowi (za pomocą odpowiednich środków technicznych i organizacyjnych) wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO (np. prawo do bycia zapomnianym, przenoszenia danych),
- pomaga administratorowi wywiązać się z obowiązków dotyczących bezpieczeństwa przetwarzania, zgłaszania naruszeń, oceny skutków dla ochrony danych i uprzednich konsultacji,
- po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa ich istniejące kopie, chyba że prawo UE lub prawo państwa członkowskiego nakazuje przechowywanie danych,
- udostępnia administratorowi informacje niezbędne do spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów (w tym inspekcji) i przyczynia się do nich.
- Dostawca / Wykonawca zobowiązuje się do spełnienia wymagań zapisów RODO w zakresie przeprowadzenia analizy ryzyka, z zagwarantowanym prawem Zamawiającego do rozliczalności tego obowiązku wobec Dostawcy / Wykonawcy.
- Dostawca / Wykonawca [podmiot przetwarzający] - gdy ma to zastosowanie – prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Zamawiającego [administratora danych] danych zgodnie z art. 30 ust 2 RODO.

6.6. Zarządzanie incydentami

6.6.1 Podmiot Zewnętrzny powinien ustanowić, wdrożyć i nadzorować proces zarządzania incydentami adekwatny do wielkości firmy. Proces ten może obejmować całość Organizacji lub dotyczyć zasobów przetwarzających informacje należące do SP ZOZ MSWiA w Katowicach w zakresie aktywów informacyjnych należących do SP ZOZ MSWiA w Katowicach. Każdy incydent musi być zgłoszony

Inspektorowi Ochrony Danych Osobowych oraz/lub Administratorowi Danych Osobowych ze strony SP ZOZ MSWiA w Katowicach.

6.6.2 Proces powinien również obejmować dalszą analizę zbiorczą incydentów zidentyfikowanych w organizacji. Do analizy można wykorzystać metodologię proponowaną przez COBIT lub normę ISO 27001 lub 9001.

6.6.3 Zarządzanie incydentami powinno obejmować szkolenia dla pracowników oraz czytelny opis procesu wraz z klasyfikacją incydentów i sposobem ich zgłaszania.

6.6.4 Zaleca się, aby Proces zarządzania incydentami zawierał wyspecyfikowane w sposób nie pozostawiający wątpliwości co do postępowania następujące obszary:

- zgłaszanie incydentów (analiza wstępna);
- rozpowszechnienie informacji (raportowanie i eskalacja);
- materiały dowodowe (zbieranie i zabezpieczenie);
- analiza końcowa.

6.7. Czysty ekran i czyste biurko

6.7.1 Podmiot Zewnętrzny powinien ustanowić, wdrożyć i nadzorować zasady dotyczące czystego biurka i czystego ekranu.

6.7.2 Zasady dotyczące czystego biurka powinny szczególnie obejmować:

- sposób zarządzania dokumentami papierowymi oraz w wersji elektronicznej przed, w trakcie i po użyciu;
- sposób przechowywania, archiwizacji i niszczenia dokumentów szczególnie w aspekcie zasobów, gdzie będą przetwarzane informacje należące do SP ZOZ MSWiA w Katowicach;
- zobowiązanie pracowników Podmiotu Zewnętrznego do uporządkowania swojego stanowiska po zakończeniu pracy, szczególnie w aspekcie dokumentów i nośników zawierających wrażliwe dane dla Podmiotu Zewnętrznego lub należące do SP ZOZ MSWiA w Katowicach.

6.7.3 Zasady dotyczące czystego ekranu powinny obejmować:

- zasady logowania i wylogowania się z komputerów osobistych, terminali i drukarek oraz sposobu ich zabezpieczenia po zakończeniu pracy w biurze Podmiotu Zewnętrznego;
- zasady zabezpieczenia komputera przed dostępem osób nieupoważnionych podczas nieobecności na stanowisku pracy lub po jej zakończeniu.

6.8. Dostęp do sieci

6.8.1 Dostęp do zasobów Podmiotu Zewnętrznego powinien być określony i usankcjonowany z zachowaniem następujących wymagań:

- przydzielenie uprawnień musi być zgodne z „zasadą wiedzy koniecznej". Oznacza to, że Pracownik Podmiotu Zewnętrznego może otrzymać tylko taki zakres uprawnień, który jest niezbędny do realizacji zadań mu powierzonych;
- pracownicy Podmiotu Zewnętrznego mogą uzyskiwać dostęp wyłącznie do standardowych systemów wykorzystywanych w obrębie działów, w których są zatrudnieni;
- w celu zachowania integralności przydzielonych uprawnień z rzeczywistymi potrzebami konieczne

jest wykonywanie regularnej weryfikacji kont;

- wszystkie uprawnienia związane z dostępem elektronicznym oraz fizycznym muszą zostać bezwzględnie odebrane w przypadku odejścia z pracy pracownika Podmiotu Zewnętrznego.

6.9. Audyt drugiej strony

6.9.1 W celu zapewnienia bezpieczeństwa informacji należących do SP ZOZ MSWiA w Katowicach i przetwarzanych przez Podmiot Zewnętrzny zastrzega się możliwość wykonania audytu przez Pracowników SP ZOZ MSWiA w Katowicach lub firmę zewnętrzną.

6.9.2 Audyt obejmie swoim zakresem wszystkie obszary mające wpływ na bezpieczeństwo danych powierzanych Podmiotowi Zewnętrznemu przez SP ZOZ MSWiA w Katowicach.

7. RYZYKA NIEZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI

Rodzaj ryzyka	Zakres występowania ryzyka	Opis
Brak dedykowanych pracowników odpowiedzialnych za przekazywanie rzetelnych i dokładnych informacji.	Wszyscy aktualni i potencjalni dostawcy / wykonawcy	Brak informacji kluczowych dla realizacji kontraktu lub zamówienia, zarówno po stronie zleceniodawcy jak i zleceniobiorcy.
Ryzyko związane z wyborem dostawcy / wykonawcy: ryzyko związane z upadłością dostawcy / wykonawcy, ryzyko związane z brakiem ciągłości w świadczeniu usługi, w wyniku zdarzeń losowych, ryzyko związane z nagłym wycofaniem się usługodawcy ze świadczenia usługi,	Wszyscy aktualni i potencjalni dostawcy / wykonawcy	Procedury doboru usługodawców zewnętrznych powinny uwzględniać ryzyko związane z określonymi usługami i obejmować w szczególności ocenę sytuacji ekonomiczno-finansowej usługodawcy oraz jakości świadczonych usług (w miarę możliwości również na podstawie doświadczeń innych podmiotów biznesowych). Ryzyko związane z wyborem dostawcy można minimalizować poprzez zastosowanie odpowiednich procedur zakupowych i przetargowych, skłaniając się również w kierunku wdrożenia strategii dywersyfikacji dostaw, przy jednoczesnym przestrzeganiu Prawa Zamówień Publicznych w zakresie zakazu zakupu tych samych produktów w różnych umowach dostaw. Zalecane jest także zawarcie w umowach zapisów dotyczących wykonania zastępczego na ryzyko i koszt wykonawcy w przypadkach trudności realizacji po stronie wykonawcy.
Spadek jakości świadczonych usług	Wszyscy aktualni i potencjalni dostawcy / wykonawcy	Spadek jakości usług może mieć różne przyczyny. Wskazane jest regularne monitorowanie jakości świadczonych usług. Zakres i częstotliwość monitorowania i raportowania powinny uwzględniać specyfikę świadczonych usług oraz ich istotność z perspektywy ciągłości i bezpieczeństwa działania SP ZOZ MSWiA w Katowicach. Dodatkowym zabezpieczeniem powinna być dywersyfikacja dostawców, która umożliwi płynne przejście od jednego do drugiego dostawcy, w przypadku znaczącego spadku jakości usług.
Pozycja monopolistyczna dostawcy / usługodawcy	Wszyscy aktualni i potencjalni dostawcy / wykonawcy	Dywersyfikacja dostaw poprzez zastosowanie odpowiednich procedur zakupowych i przetargowych. Zagwarantowanie alternatywnych dostawców dla kluczowych obszarów jako element strategii przetargowo - zakupowej.

Nieadekwatne zapisy w umowach z dostawcami lub brak umów	Wszyscy aktualni i potencjalni dostawcy / wykonawcy	Brak umowy może oznaczać równocześnie brak sformalizowanego narzędzia regulującego współpracę, brak zdefiniowanych ścieżek rozwiązywania sporów na linii zleceniodawca - zleceniobiorca oraz brak gwarancji dla bezpieczeństwa współpracy
Brak płynności dostaw w obszarach kluczowych	Wszyscy aktualni i potencjalni dostawcy / wykonawcy	Może prowadzić do utrudnień w codziennym funkcjonowaniu SP ZOZ MSWiA w Katowicach.

8. ZAKRES UMÓW PODPISYWANYCH Z DOSTAWCAMI.

8.1. Prawidłowo przygotowane umowy mogą zapobiec wystąpieniu problemów w obszarze współpracy z dostawcami / wykonawcami i bezpieczeństwa informacji lub ułatwić ich szybkie rozwiązanie. Umowa przewidująca zagrożenia i ryzyka, które mogą wystąpić i zagrozić realizacji dostaw towarów i usług, zwiększa możliwość szybkiego i efektywnego działania. Zabezpieczenie w postaci zastosowania odpowiednich konstrukcji prawnych oddziałuje z jednej strony „prewencyjnie", wskazując pracownikom czy kontrahentom, na ich zobowiązania i potencjalnie negatywne konsekwencje ich niedopełnienia, z drugiej strony „reaktywnie", umożliwiając lub zdecydowanie ułatwiając dochodzenie roszczeń przed sądem.

Rodzaj umowy	Sugerowana zawartość umowy i zasady weryfikacji treści umów
Umowy z dostawcami / wykonawcami usług teleinformatycznych	- zakresy odpowiedzialności stron umowy, - zakres informacji i dokumentacji przekazywanych przez usługodawcę w ramach świadczonych usług, - zasady wymiany i ochrony informacji, w tym warunki nadawania pracownikom podmiotów zewnętrznych praw dostępu do informacji oraz zasobów środowiska teleinformatycznego SP ZOZ MSWiA w Katowicach, uwzględniające w szczególności obowiązujące przepisy prawa oraz regulacje SP ZOZ MSWiA w Katowicach w tym zakresie; w przypadku usługodawców posiadających dostęp do informacji o wysokim stopniu poufności, powinna zostać również uregulowana kwestia odpowiedzialności za zachowanie tajemnicy tych informacji w okresie wykonywania usług oraz po zakończeniu umowy, - zasady związane z prawami do oprogramowania (w tym jego kodów źródłowych) w trakcie współpracy i po jej zakończeniu, - parametry dotyczące jakości świadczonych usług oraz sposoby ich monitorowania i egzekwowania, - zasady tworzenia kopii zapasowych, - zapisy dotyczące lokalizacji w których dane mogą być przechowywane i przetwarzane, zasady i tryb obsługi zgłoszeń dotyczących problemów w zakresie świadczonych usług,

	- zasady i tryb dokonywania aktualizacji oprogramowania i komponentów infrastruktury znajdujących się pod kontrolą dostawcy, - zasady współpracy w przypadku wystąpienia incydentu bezpieczeństwa środowiska teleinformatycznego, - zasady w zakresie dalszego zlecania czynności podwykonawcom zewnętrznego dostawcy usług, - kary umowne związane z nieprzestrzeganiem warunków umownych, w szczególności w zakresie bezpieczeństwa informacji przetwarzanych przez dostawcę usług,
Umowy z dostawcami / wykonawcami towarów i usług niebędących usługami teleinformatycznymi	- zapewnienie, że realizacja umowy odbywać się będzie zgodnie z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi oraz przyjętymi w SP ZOZ MSWiA w Katowicach standardami, - umowy zawierane przez SP ZOZ MSWiA w Katowicach z dostawcami / wykonawcami usług powinny być weryfikowane w odpowiednim zakresie przez jednostki SP ZOZ MSWiA w Katowicach odpowiedzialne za obszar prawny oraz obszar bezpieczeństwa środowiska teleinformatycznego, - regulacje dotyczące współpracy z pracownikami zewnętrznych dostawców usług, uwzględniające w szczególności: • warunki udzielania dostępu do informacji o wysokim stopniu poufności, • zasady sprawowania nadzoru nad działaniami pracowników zewnętrznych, • konieczność zapewnienia, że każdy pracownik dostawców / wykonawców objęty jest co najmniej takimi samymi restrykcjami w zakresie bezpieczeństwa, jak pracownicy SP ZOZ MSWiA w Katowicach,

8.2. Zasady współpracy pomiędzy SP ZOZ MSWiA w Katowicach, a zewnętrznym dostawcą / wykonawcą usług powinny uwzględniać reguły w zakresie komunikacji i koordynacji wykonywanych przez usługodawcę czynności (np. w zakresie przeprowadzania migracji danych, czynności konserwacyjnych, dostępu do infrastruktury teleinformatycznej, skanowania infrastruktury teleinformatycznej itp.), minimalizujące ich negatywny wpływ na jakość i bezpieczeństwo usług nie tylko teleinformatycznych.

9. KARTA ZMIAN.

Nr karty zmian	Symbol zmian	Podpis	Data	Nr karty zmian	Symbol zmian	Podpis	Data

10. Załączniki.

10.1. Załącznik nr 1: Wzór umowy powierzenia przetwarzania danych osobowych

Oświadczenie pracowników

.....

(komórka organizacyjna SP ZOZ MSWiA w Katowicach - pieczątka)

Oświadczam, że zapoznałem/am się z treścią niniejszej polityki zobowiązuję się do przestrzegania wszystkich zaleceń w niej zawartych

.....

(nazwa instrukcji)

L.p	Nazwisko i imię	Stanowisko	Data	Podpis

Umowa powierzenia przetwarzania danych osobowych nr: .....
zawarta dnia ..... w Katowicach pomiędzy:
(zwana dalej „Umową")

Samodzielnym Publicznym Zakładem Opieki Zdrowotnej Ministerstwa Spraw Wewnętrznych i Administracji w Katowicach im. Sierżanta Grzegorza Załogi
z siedzibą w Katowicach; 40-042; ul. Wita Stwosza 39-41 zarejestrowanym w Sądzie Rejonowym Katowice-Wschód w Katowicach, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, numer KRS 0000011889, NIP: 634-23-09-181, REGON: 271241038.
zwanym w dalszej części umowy **„Administratorem"**
reprezentowanym przez:
dr inż. Karolina Mielczarek – Dyrektor
oraz
.....
.....
.....

zwanym w dalszej części umowy **„Podmiotem przetwarzającym"**
reprezentowanym przez:
.....

łącznie zwane **„Stronami"**, a odrębnie **„Stroną"**

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (EU) nr 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 (ogólnego rozporządzenia o ochronie danych), zwanego w dalszej części „Rozporządzeniem", dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§ 2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy następujące rodzaje danych osobowych:
   1) Pacjenci administratora:
      - imię (imiona) i nazwisko,
      - imię ojca,
      - imię matki,
      - nazwisko rodowe,
      - płeć,
      - obywatelstwo,
      - wykształcenie,
      - numer PESEL,
      - data urodzenia,
      - numer paszportu albo innego dokumentu stwierdzającego tożsamość (w przypadku osób, które nie mają nadanego numeru PESEL)
      - adres miejsca zamieszkania i adres do korespondencji,
      - adres miejsca pobytu na terytorium Rzeczypospolitej Polskiej, jeżeli dana osoba nie ma na terytorium Rzeczypospolitej Polskiej miejsca zamieszkania,
      - adres e-mail,
      - numer i rodzaj dokumentu potwierdzającego prawo do świadczeń opieki zdrowotnej finansowanych ze środków publicznych,

- rodzaj uprawnień oraz numer i termin ważności dokumentów potwierdzających uprawnienia do świadczeń opieki zdrowotnej określonego rodzaju oraz datę utraty tych uprawnień,
- numery identyfikacyjne i numery ewidencyjne nadawane usługobiorcom przez płatników lub usługodawców,
- informacja o prawie do świadczeń opieki zdrowotnej finansowanych ze środków publicznych,
- numer identyfikacyjny płatnika,
- numer telefonu kontaktowego,
- informacja o sprzeciwie zawartym w centralnym rejestrze sprzeciwów na pobranie komórek, tkanek i narządów ze zwłok ludzkich,
- dane medyczne,
- numer karty zaopatrzenia na środki pomocnicze,
- inne dane medyczne (w szczególności: zestawienia refundacyjne zawierające numer PESEL lub inny identyfikator pacjenta, zestawienia refundacyjne za środki pomocnicze zawierające numer PESEL, recepty, dokumenty realizacji recept, książka kontroli narkotyków, wnioski na import docelowy, faktury sprzedaży, inne dane medyczne).

2) Przedstawiciele ustawowi pacjentów:
- imię (imiona) i nazwisko,
- adres zamieszkania,
- numer PESEL

3) Osoby upoważnione do uzyskiwania dokumentacji i informacji o stanie zdrowia:
- imię (imiona) i nazwisko,
- adres zamieszkania,
- numer telefonu kontaktowego,
- data urodzenia.

4) Pracownicy Administratora i personel Administratora zatrudniony na innej podstawie niż umowa o pracę:
- imię (imiona) i nazwisko,
- nazwisko rodowe,
- wykształcenie,
- zawód lub specjalizacje,
- numer prawa wykonywania zawodu,
- numer PESEL,
- identyfikator w NFZ.
- numer umowy POZ,
- adres miejsca zamieszkania,
- numery identyfikacyjne nadawane przez Administratora,
- adres e-mail,
- numer rachunku bankowego.

5) Kontrahenci:
- imię (imiona) i nazwisko,
- adres,
- numer telefonu kontaktowego,
- adres e-mail,
- numer rachunku bankowego,
- numer NIP.

2. Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:
1) Pacjenci administratora.
2) Przedstawiciele ustawowi pacjentów.
3) Osoby upoważnione do uzyskiwania dokumentacji i informacji o stanie zdrowia.
4) Pracownicy Administratora i personel Administratora zatrudniony na innej podstawie niż umowa o pracę.
5) Kontrahenci.
3. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy Podstawowej, tj.:..... <nazwa> z dnia: ..... nr: ..... w zakresie: .....
4. Zakres danych osobowych wymienionych powyżej jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy. Zakres danych może ulec zmianie w przypadku zmiany aktualnie obowiązujących przepisów prawa.

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień

bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.

2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania danych odpowiednie szkolenie z zakresu ochrony danych osobowych.
5. Podmiot przetwarzający na żądanie Administratora dostarcza Administratorowi wykaz upoważnionych osób oraz informuje Administratora o cofnięciu upoważnień.
6. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
8. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
9. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w czasie nie przekraczającym *24 h*.
   Powiadomienie o stwierdzeniu naruszenia powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.
10. Podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 Rozporządzenia.
11. Ze względu na obowiązek powierzenia przetwarzania danych przez Administratora podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniło wymagania rozporządzenia i chroniło prawa osób, których dane dotyczą Podmiot Przetwarzający zobowiązany jest do wypełnienia ankiety bezpieczeństwa danych osobowych *(załącznik nr: 1 - Ankieta bezpieczeństwa danych osobowych).*
12. Przestrzeganie zasad określonych w wprowadzonej w Szpitalu „Polityce współpracy z dostawcami i Wykonawcami" dostępnej na stronie www Szpitala: https://www.gov.pl/web/spzoz-mswia-katowice/rodo.

§ 4

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora pod rygorem nieważności w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy Podstawowej.
3. Zobowiązanie do zachowania poufności trwa przez cały okres obowiązywania Umowy Podstawowej, o której mowa w § 2 punkt 3 powyżej oraz po upływie okresu przedawnienia roszczeń wynikających z Umowy Podstawowej.

§ 5

Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy lub Rozporządzenia.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum *7 dniowym* uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż *7 dni.*
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 6

Dalsze powierzenie danych do przetwarzania

1. Podmiot Przetwarzający może powierzyć konkretne operacje przetwarzania Danych (*„podpowierzenie"*) jedynie w celu wykonania Umowy Podstawowej, w drodze pisemnej umowy podpowierzenia (*„Umowa Podpowierzenia"*) innym podmiotom przetwarzającym (*„Podprzetwarzającym"*) pod warunkiem uzyskaniu uprzedniej pisemnej akceptacji Podprzetwarzającego przez Administratora.
2. Lista Podprzetwarzających zaakceptowanych przez Administratora stanowi *załącznik nr 2 do Umowy – Lista Zaakceptowanych Podprzetwarzających*.
3. Zmiana bądź dodanie Podprzetwarzającego wymaga każdorazowo pisemnej zgody Administratora pod rygorem nieważności.
4. Dokonując podpowierzenia, Podmiot Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia.
5. Podmiot Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi pisemne oświadczenie o zobowiązaniu się do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.
6. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy (*„Podprzetwarzającego"*) obowiązków w zakresie ochrony danych.
7. W przypadku dalszego powierzenia przetwarzania danych osobowych Podmiot Przetwarzający zobowiązuje się do zawarcia w umowach z dalszymi podmiotami przetwarzającymi (*„Podprzetwarzającym"*) postanowień, zgodnie z którymi, umowy dalszego przetwarzania będą ulegały automatycznemu rozwiązaniu w chwili zakończenia obowiązywania niniejszej Umowy.
8. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
9. Podmiot Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy Podstawowej.

§ 7
Oświadczenia Stron

1. Administrator oświadcza, że jest Administratorem danych osobowych oraz że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
2. Podmiot Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.
3. Przetwarzający na żądanie administratora powinien przedstawić dokumentację potwierdzająca przetwarzanie danych osobowych zgodnie z wymogami RODO, mogą to być między innymi: certyfikat potwierdzający wdrożenie normy PN-EN ISO/IEC 27001, raporty z przeprowadzonych przez niezależne podmioty audytów, dokumentacja potwierdzająca przeprowadzenie szkoleń, dokumentacja potwierdzająca wdrożenie zabezpieczeń technicznych i organizacyjnych.

§ 8
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot Przetwarzający odpowiada za szkody, jakie powstaną po stronie Administratora lub osób trzecich w wyniku niezgodnego z Umową, lub obowiązującymi przepisami prawa, przetwarzania danych osobowych przez Podmiot Przetwarzający.
3. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez Pracowników Urzędu upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§ 9
Czas obowiązywania umowy

1. Niniejsza umowa zostaje zawarta na czas trwania Umowy Podstawowej, o której mowa w § 2 pkt 3 powyżej.
2. Rozwiązanie umowy, o której mowa w § 2 pkt 3 powyżej skutkować będzie ustaniem niniejszej Umowy.

3. Zamawiający może rozwiązać umowę, o której mowa w § 2 pkt 3 powyżej ze skutkiem natychmiastowym, bez zachowania okresu wypowiedzenia, gdy Wykonawca narusza zobowiązania wynikające z niniejszej Umowy.

§ 10
Rozwiązanie, zmiana umowy

1. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową lub Rozporządzeniem;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 11
Inspektor Ochrony Danych

1. Kontakt z Inspektorem Ochrony Danych [IOD] w **Samodzielnym Publicznym Zakładem Opieki Zdrowotnej Ministerstwa Spraw Wewnętrznych i Administracji w Katowicach im. Sierżanta Grzegorza Załogi** e-mail: **iod@zozmswia.katowice.pl.; telefon: 32 341 1888**
2. Kontakt z Inspektorem Ochrony Danych [IOD] w Podmiocie Przetwarzającym lub pełnomocnikiem Podmiotu Przetwarzającego właściwym z uwagi na przedmiot Umowy e-mail: .....; telefon: .....

§ 12
Koordynatorzy Umowy

1. Podejmowanie decyzji oraz bieżące zarządzanie realizacją Umowy odbywać się będzie przez wzajemne uzgodnienia Koordynatorów Umowy. Koordynatorzy Umowy będą uprawnieni w szczególności do dokonywania zmian w Załącznikach do Umowy, przy czym zmiany Załączników nie będą uważane za zmiany Umowy i nie będą wymagały zawarcia aneksu do Umowy. Koordynatorzy Umowy nie są uprawnieni do zmiany lub rozwiązania Umowy Głównej.
2. Strony ustanawiają następujących Koordynatorów Umowy:
   a) ze strony Administratora: .....; e-mail: .....; tel.: ..... .
   b) ze strony Podmiotu przetwarzającego: .....; e-mail: .....; tel.: ..... .
3. Zmiana adresów i danych koordynatorów Umowy nie stanowi zmiany Umowy, jednak wymaga powiadomienia drugiej Strony z zachowaniem co najmniej formy dokumentowej.

§ 13
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. Każdorazowo przez pojęcie „dni" rozumie się dni kalendarzowe.
3. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.
4. W sprawach nieuregulowanych zastosowanie będą miały przepisy ustawy krajowej o ochronie danych osobowych oraz Rozporządzenia.
5. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych.

.....	.....
Administrator	Podmiot przetwarzający

ANKIETA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Załącznik nr 1 do umowy powierzenia danych osobowych nr: ..... z dnia: ..... .

Podmiot przetwarzający:	
Imię I Nazwisko osoby wypełniającej	
Stanowisko	
Adres e-mail i nr telefonu	

Lp.	Pytanie	Odpowiedź	Uwagi
1	Proszę podać ilość lokalizacji i kraje, w których będą przetwarzane powierzone dane osobowe.		
2	Czy Państwa personel został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?		
3	Czy personel przetwarzający powierzone dane osobowe w pozostałych krajach został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?		
4	Czy powierzone dane osobowe będą przekazywane poza EOG? Np. ze względu na lokalizację systemu IT, będą przetwarzane przez osoby zlokalizowane poza EOG lub osoby te będą miały możliwość dostępu do tych danych?		
5	Jeśli tak to w jakim kraju?		
6	Czy w Państwa organizacji przeprowadzane są okresowe audyty zgodności z przepisami ochrony danych osobowych?		
7	Czy w Państwa organizacji przeprowadzane są okresowe audyty bezpieczeństwa IT?		
8	Czy posiadają Państwo wdrożoną politykę bezpieczeństwa przetwarzania danych osobowych zgodną z zasadami RODO?		
9	Czy prowadzą Państwo rejestr czynności przetwarzania, w tym dla procesora, zgodnie z art. 30 RODO?		

10	Czy jesteście Państwo zobowiązani do wyznaczenia IOD, zgodnie z art. 37 RODO?		
11	Jeśli tak, to czy wyznaczono IOD?		
12	Jeśli nie, to czy wyznaczyli Państwo osobę, która będzie odpowiedzialna za zapewnienie zgodności przetwarzania danych z przepisami i bezpieczeństwa danych?		
13	Czy do przetwarzania danych w Państwa organizacji są dopuszczone wyłącznie osoby posiadające upoważnienia?		
14	Czy osoby te zostały zobowiązane do zachowania poufności danych oraz informacji o stosowanych przez Państwa zabezpieczeniach?		
15	Czy korzystają Państwo z usług podwykonawców i podpowierzają lub planują podpowierzyć im przetwarzanie danych przekazanych przez administratora danych?		
16	Jeśli tak, to czy z podwykonawcami zawarto pisemne umowy powierzenia danych odpowiadające wymogom określonym w art. 28 RODO?		
17	Czy wdrożyli Państwo instrukcję postępowania w przypadku sytuacji naruszenia ochrony danych osobowych?		
18	Jeśli tak, to czy zgodnie z tą instrukcją zdołają Państwo przekazać administratorowi danych informacje o incydencie bez zbędnej zwłoki w czasie nie przekraczającym 24 h od stwierdzenia naruszenia?		
19	Czy w celu zaplanowania środków bezpieczeństwa przeprowadzono analizę ryzyka?		
20	Czy wdrożyli Państwo system zarządzania bezpieczeństwem informacji np. ISO 27001?		
21	Czy do przetwarzania danych w Państwa pomieszczeniach, stosuje się fizyczne zabezpieczenia przed dostępem osób nieuprawnionych? Proszę krótko opisać jakie np. system kontroli dostępu, drzwi zamykane na klucz, system alarmowy, ochrona fizyczna, monitoring wizyjny.		

22	Czy przetwarzanie danych było już przedmiotem zewnętrznych audytów lub kontroli, np. PUODO w Państwa organizacji?		
23	Jeśli tak, proszę zwięźle opisać wyniki kontroli/ audytów		
24	Czy posiadają Państwo wdrożoną instrukcję zarządzania systemami IT służącymi do przetwarzania danych osobowych lub inne dokumenty wewnętrzne regulujące zasady zarządzania infrastrukturą IT?		
25	Czy Państwa systemy IT zapewniają rozliczalność operacji wykonywanych na danych osobowych, tzn. czy istnieje odnotowują nazwę użytkownika, datę oraz charakter operacji wykonanej na konkretnym rekordzie w bazie?		
26	Czy w przypadku przekazywania danych osobowych środkami telekomunikacyjnymi lub na nośnikach zewnętrznych, przekazywane dane są szyfrowane?		
27	Czy stosują Państwo pseudonimizację i szyfrowanie danych?		
28	Czy podjęli Państwo środki, aby zapewnić zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania?		
29	Czy w Państwa organizacji są stosowane środki służące ochronie systemów IT przed działaniem tzw. złośliwego oprogramowania?		
30	Jeśli tak, to czy podlegają one cyklicznej aktualizacji?		
31	Czy podjęli Państwo środki, aby zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? Np. regularny backup		
32	Czy dostęp do systemów IT wymaga uwierzytelniania użytkownika tj. podania indywidualnego identyfikatora i hasła?		
33	Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników?		

Lista Zaakceptowanych Podprzetwarzających

Załącznik nr 2 do umowy powierzenia danych osobowych nr: ..... z dnia: ..... .

L.p.	Nazwa i dane kontaktowe podmiotu podprzetwarzającego	Dane kontaktowe inspektora ochrony danych	Cel podpowierzenia	Zakres podpowierzenia
1				
2				
3				
4				
5				
6				
7				
8				