Załącznik nr 7 do SWKO

UMOWA O OCHRONIE DANYCH
(Umowa powierzenia przetwarzania danych osobowych)

zawarta pomiędzy Administratorem i Podmiotem Przetwarzającym

Załącznik nr 7 do SWKO

Strony Umowy powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych, (dalej jako Umowa) na podstawie art. 28 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 (Rozporządzenie o ochronie danych osobowych) zawarta pomiędzy:

Szpitalem Wojewódzkim im. M. Kopernika w Koszalinie (75-581) ul. Chałubińskiego 7, 75-581 reprezentowanym przez Piotra Sołtysińskiego - Dyrektora, zwanym w dalszej części umowy „Administratorem”,

a

.....

.....

zwanym dalej „Podmiotem przetwarzającym”

zwani dalej łącznie : Stronami, a każdą z osobna Stroną.

W odniesieniu postanowień zawartych pomiędzy Stronami, w tym: w odniesieniu do zmian, poprawek i aneksów oraz wszystkich powiązanych z nimi porozumień umownych, a także dla uniknięcia wątpliwości Udzielający zamówienia pełni rolę Administratora, Przyjmujący zamówienie pełni rolę Podmiotu przetwarzającego.

Zważywszy, iż realizacja Umowy Głównej w przedmiocie świadczenia przez Podmiot przetwarzający na rzecz Administratora usługi w zakresie opisów badań diagnostyki obrazowej: badań radiologicznych (RTG) oraz badań tomografii komputerowej (TK) jest uzależniona od dostępu Podmiotu przetwarzającego do danych osobowych pacjentów Administratora, Strony zgodnie postanawiają, co następuje:

1. Oświadczenia Stron.
   1) Przetwarzanie danych przez Podmiot przetwarzający będzie odbywać się wyłącznie na udokumentowane polecenie Administratora, którym jest zlecenie Podmiotowi przetwarzajacemu zadań określonych Umową Główną,
   2) Strony zawierając Umowę powierzenia przetwarzania danych dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni przepisom 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 (Dz. Urz. UE L 119, s. 1) zwane dalej rozporzadzeniem o ochronie danych.
2. Postanowienia umowne.
   1) Umowa i Załączniki stanowią integralną część i będą przechowywane przez obie Strony w formie pisemnej, w tym w formie elektronicznej,
   2) Strony zobowiązują się nie zmieniać postanowień zawartych w niniejszej Umowie, za wyjątkiem dodawania informacji do Załączników lub aktualizowania zawartych w nich informacji.
   3) Wszelkie zmiany w Załącznikach nie mogą być bezpośrednio lub pośrednio sprzeczne z niniejszymi postanowieniami i nie mogą naruszać podstawowych praw lub wolności osób, których dane dotyczą.
   4) Każda zmiana Załącznika wymaga akceptacji Stron.
   5) Do Umowy dołączone są cztery Załączniki:

a. Załącznik A zawiera informacje na temat przetwarzania danych osobowych, w tym informacje dotyczące celu i charakteru przetwarzania, rodzaju danych osobowych, kategorii osób, których dane dotyczą.

b. Załącznik B zawiera warunki dotyczące korzystania przez Podmiot przetwarzający z Podwykonawców przetwarzających dane oraz wykaz Podwykonawców, których Administrator zatwierdził.

c. Załącznik C zawiera informacje dotyczące środków bezpieczeństwa, oraz sposób przeprowadzania przez Administratora audytów u Podmiotu przetwarzającego i Podwykonawców.

d. Załącznik D zawiera pozostałe uzgodnienia zawarte pomiędzy Stronami, w tym Ankietę dla Podmiotów przetwarzających dane.

6) Wykładnia.

Jeżeli w Umowie użyto terminów zdefiniowanych odpowiednio w rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725, terminy te mają takie samo znaczenie jak w tych rozporządzeniach.

3. Czas przetwarzania .

Przetwarzanie danych przez Podmiot przetwarzający odbywa się wyłącznie przez okres określony w Załączniku A.

4. Poufność przetwarzania.

1) Strony oświadczają, że dane osobowe powierzone do przetwarzania na podstawie niniejszej Umowy powierzenia przetwrzania danych, o których Strony uzyskają wiadomość w związku z zawarciem i wykonywaniem Umowy Głównej są poufne, posiadają wartość aktywów chronionych i co do swej istoty nie są jawne,

2) Dane osobowe stanowią informacje chronione rozporządzeniem o ochronie danych i przepisami prawa powszechnie obowiązującego,

3) Obowiązek zachowania w tajemnicy danych osobowych/informacji chronionych powierzonych przez Administratora odnosi się zarówno do Podmiotu przetwarzającego i Podwykonawców, zaangażowanych przez Podmiot przetwarzający, jak również obowiązek ten stosuje się w całości do kolejnych podmiotów zatrudnionych przez Podwykonawców.

4) Obowiązek zachowania w tajemnicy danych osobowych/informacji chronionych nie dotyczy;

a. obowiązku ujawniania, wynikającego z bezwzględnie obowiązujących przepisów prawa,

b. gdy druga Strona wyraziła zgodę na jej ujawnienie,

c. gdy dane stały się powszechnie znane wskutek okoliczności od Stron niezależnych,

d. gdy dane są niezbędne do świadczenia na rzecz każdej ze Stron usług przez podmioty zobowiązane do zachowania tajemnicy zawodowej, w szczególności biegłych rewidentów, radców prawnych.

5. Bezpieczeństwo przetwarzania.

1) Podmiot przetwarzający, przed rozpoczęciem przetwarzania, przekaże Administratorowi informacje zawarte w Ankiecie dla Podmiotu przetwarzającego dane – Załącznik D.

2) Administrator ocenia zagrożenia dla praw i wolności osób fizycznych związane z przetwarzaniem i wskazuje referencyjny poziom bezpieczenstwa, mając na uwadze zapewnienie danym osobowym atrybutów: poufności, dostępności i integralności,

3) Podmiot Przetwarzający, projektując, eksploatując, doskonaląc środki bezpieczeństwa uwzględnia referencyjny poziom bezpieczeństwa, wskazany przez Administratora, a w przypadku braku możliwości ich zastosowania w całości lub części, poinformuje o tym niezwłocznie Administratora. Wszelkie rozbieżności w zakresie stosowania referencyjnego poziomu bezpieczeństwa zostaną wyjaśnione i skorygowane przez Strony niezwłocznie, mając na uwadze obowiązki Administratora i Podmiotu Przetwarzającego w zakresie bezpieczeństwa danych osobowych oraz posiadane środki i możliwości,

4) Podmiot przetwarzający niezależnie od Administratora ocenia zagrożenia dla praw i wolności osób fizycznych związane z przetwarzaniem i podejmuje odpowiednie środki w celu zminimalizowania tych zagrożeń,

6. Korzystanie z usług podmiotów pod przetwarzających (podwykonawców).

1) Jeżeli należyta realizacja obowiązków wynikających ze świadczenia usług z Umowy będzie tego wymagała, Podmiot przetwarzający może dokonać dalszego powierzenia przetwarzania danych osobowych na warunkach określonych w art. 28 ust. 2 i 4 Rozporządzenia o ochronie danych,
2) Warunkiem korzystania przez Podmiot przetwarzający z Podwykonawcy jest zgoda Administratora, z jednoczesnym oświadczeniem, że podmiot, któremu podpowierzono dane osobowe (podwykonawca przetwarzający dane) spełnia wymogi określone w art.28 RODO i zostanie to zagwarantowane w dalszej umowie powierzenia (umowie podpowierzenia),
3) Uprawnienie do dalszego powierzania danych osobowych przez Podmiot przetwarzajacy nie obejmuje przekazywania danych do państwa trzeciego, w rozumieniu art. 44 RODO. W takim wypadku wymagana jest zgoda Administratora.
4) W przypadku, gdy Podmiot przetwarzający uzyskał:
   a. konkretną pisemną zgodę Administratora, to składa wniosek o zatwierdzenie Podwykonawcy, w terminie określonym przez Administratora,
   b. ogólną zgodę Administratora, to powiadamia Administratora na piśmie, w treminie 14 dni o wszelkich planowanych zmianach dotyczących dodania lub zastąpienia Podwykonawców, powiadomienie o wybraniu Podwykonawcy Podmiot przetwarzający może dokonać w formie pisemnej lub elektronicznej,

5) uprawnienie dotyczące powiadomienia o Podwykonwcy nie wyłącza możliwości wyrażenia sprzeciwu przez Administratora,

6) w przypadku wyrażenia sprzeciwu Podmiot przetwarzający dołoży staranności przy wyborze podwykonawcy i przeprowadzi proces weryfikacji pod kątem zgodności z prawem i bezpieczeństwa przetwarzania danych osobowych.

7) uprawnienia podmiotu, któremu Podmiot przetwarzający powierzy dane osobowe nie mogą być szersze aniżeli uprawnienia, które Strona uzyskała w wyniku niniejszej Umowy,

8) odpowiedzialność Podmiotu przetwarzającego w związku z podpowierzeniem danych osobowych.

Podmiot przetwarzający:

a. jest odpowiedzialny za wymaganie od Podwykonawcy przestrzegania obowiązków Podmiotu przetwarzającego wynikajacych z niniejszej Umowy,

b. ponosi pełną odpowiedzialność wobec Administratora wynikającą z przepisów Rozporządzenia o ochronie danych, w szczególności z art. 79 i 82.

c. kopia umowy o podwykonawstwo oraz wszelkie późniejsze zmiany są, przekazywane Administratorowi, w celu sprawdzenia czy Podwykonawca podlega tym samym obowiązkom, co do zakresu i ochrony danych osobowych, które określone zostały w niniejszej Umowie. Postanowienia handlowe, które nie wpływają na treść umowy

o podwykonawstwo z zakresu ochrony danych osobowych, nie podlegają wymogowi przekazania kopii do Administratora.

13. Pomoc dla Administratora.

1) Podmiot przetwarzający zobowiązany jest wspierać Administratora w wywiązywaniu się z obowiązków w zakresie bezpieczeństwa danych, zarządzania naruszeniem ochrony danych osobowych oraz ich zgłaszaniem do organu nadzoru oraz osoby, której dane dotyczą, oceny skutków dla ochrony danych oraz konsultacjami z organem nadzoru zgodnie z art.32-36 RODO.

2) Podmiot przetwarzający zobowiązany jest współpracować z Administratorem w zakresie udzielania odpowiedzi na żądanie osoby, której dane dotyczą, opisane w rozdziale III RODO.

3) W sytuacji wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Administratora za przetwarzanie powierzonych danych osobowych Podmiot przetwarzający;

   a. zobowiązany jest niezwłocznie podjąć działania w celu ich usunięcia,

   b. pomaga Administratorowi w zgłoszeniu incydentu bezpieczenstwa,naruszenia ochrony danych właściwemu organowi nadzorczemu. Oznacza to, że Podmiot przetwarzający pomaga w uzyskaniu informacji, które zgodnie: z art. 33 pkt 3 rozporządzenia o ochronie danych Administrator przekazuje w zgłoszeniu naruszenia do właściwego organu nadzorczego,a w przypadku incydentu bezpieczeństwa zgodnie z art. 11 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Administrator jako operator usługi klczowej przekazuje do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego.

14. Odpowiedzialność

1) Podmiot przetwarzający ponosi odpowiedzialność odszkodowawczą wobec Administratora za działania własne i Podwykonawców, z tytułu niewykonania lub nienależytego wykonania zobowiązań wynikających z niniejszej Umowy lub przepisów prawa bezwzględnie obowiązującego.

2) W przypadku naruszenia niniejszej Umowy nie stosuje się ograniczeń odpowiedzialności uzgodnionych przez Strony w Umowie Głównej lub innych dokumentach.

15. Usuwanie i zwrot informacji.

Zasady usuwania informacji określone zostały w Załączniku C.

16. Audyt, w tym kontrole.

Zasady prowadzenia audytu w tym kontroli określone zostały w Załączniku C.

17. Hierarchia.

W razie sprzeczności między niniejszymi postanowieniami a postanowieniami powiązanych umów zawartych między Stronami, a istniejących w chwili uzgadniania niniejszych postanowień lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze postanowienia.

18. Osoby do kontaktu u Administratora i Podmiotu przetwarzającego dane.

1) Strony mogą kontaktować się ze sobą za pośrednictwem poniższych osób kontaktowych.

2) Strony zobowiązują się do informowania się na bieżąco o zmianach dotyczących osób do kontaktu;

Po stronie Administratora

[Imię i nazwisko] –

[POZYCJA] – Inspektor Ochrony Danych

[NUMER TELEFONU] -94-34-88-545, 151

Adres e-mail [E-MAIL] sekretariat@swk.med.pl, iod@swk.med.pl

Po stronie Podmiotu przetwarzającego

[Imię i nzawisko] – .....

[POZYCJA] – .....

[NUMER TELEFONU] .....

[Adres e-mail] .....

19. Wejście w życie i wypowiedzenie

1) Umowa obowiązuje od dnia podpisania przez obie Strony.
2) Strony mogą żądać renegocjacji postanowień Umowy, jeżeli uzasadnią to zmiany przepisów prawa lub niezgodności w Umowie.
3) Umowa obowiązuje przez czas świadczenia usług przetwarzania danych.
4) W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy prawa polskiego.
5) Spory wynikłe z zastosowania tej Umowy rozpatrywane będą przez sąd właściwy dla siedziby Administratora.

W imieniu Administratora

W imieniu Podmiotu przetwarzającego

Załącznik A Informacja o przetwarzaniu

Nr Załącznika	Wersja	Data aktualizacji	Nr Umowy Głównej	Wprowadzone zmiany (określone w pkt.od ...do)	(Czas trwania Umowy Głównej)
A.	0.1				
A.					

A.1. Cel przetwarzania.

Celem przetwarzania danych osobowych przez Podmiot przetwarzający w imieniu Administratora danych jest (opis celu przetwarzania) realizacja przedmiotu Umowy Głównej, która obejmuje: transmisję danych oraz wykonanie usługi teleradiologicznej (opisu badanialub /i oceny) w terminach ustalonych w Umowie Głównej;

A.2. Charakter przetwarzania.

Podmiot przetwarzający przetwarza dane okresowo w zakresie realizowanych usług;

a. oceny i opisów brazów z badań radiologicznych, przy wykorzystaniu technologii cyfrowych i systemów informatycznych,
b. przekazywania drogą elektroniczną opisu badania wraz z autoryzacją osoby uprawnionej do opisu badania,
c. wzajemnej konsultacji drogą telefoniczną lub elektroniczną w celu doprecyzowania wymagań diagnostycznych.

A.3. Zakres przetwarzanych danych.

1) dane zawarte w zleceniu,

2) dane zawarte w ocenie i opisie obrazu radiologicznego:

Przetwarzanie obejmuje:

A4. Rodzaj danych.

1) dane zawarte w Zleceniu na badanie:

a. dane pacjenta: imię (imiona) i nazwisko, adres miejsca zamieszkania, data urodzenia, numer PESEL, a w przypadku osób, którym nie nadano numeru PESEL – serię i numer paszportu albo innego dokumentu stwierdzającego tożsamość albo niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej dla celów transgranicznej identyfikacji,

b. datę wykonania badania radiologicznego,

c. informacje dotyczące: rodzaju badania radiologicznego, użytej metody obrazowania, zastosowanych parametrów fizycznych oraz ilości i rodzaju zastosowanego środka kontrastującego oraz drogi jego podania, zakresu zobrazowanych struktur anatomicznych,

d. oznaczenie osoby zlecającej usługę teleradiologiczną,

e. datę wystawienia zlecenia na usługę teleradiologiczną,

f. nazwę i adres podmiotu zlecającego,

g. identyfikator podmiotu zlecającego – I część jego kodu resortowego z systemu resortowych kodów identyfikacyjnych, o którym mowa w przepisach wydanych na podstawie art. 105 ust. 5 ustawy z dnia 15 kwietnia 2011 r. działalności leczniczej,

h. nazwę i adres podmiotu świadczącego usługę;

2) dane zawarte w ocenie i opisie obrazu radiologicznego:

a. dane zawarte w Zleceniu na badanie, wg wykazu powyżej (pkt 1. lit od a.do h),

b. oznaczenie lekarza, wykonujacego usługę: imię (imiona) i nazwisko, informacja o uzyskanych specjalizacjach, numer prawa wykonywania zawodu, kwalifikowany podpis elektroniczny albo podpis zaufany; nazwa i adres podmiotu wykonującego działalność leczniczą, w którym wykonano badanie radiologiczne, oraz data wykonania tego badania,

c. omówienie obrazu radiologicznego obejmujące stwierdzone nieprawidłowości, ich rozmiar i umiejscowienie oraz wskazanie elementów lub procesów utrudniających interpretację obrazu radiologicznego; w przypadku odmowy wykonania opisu obrazu radiologicznego informację, że obraz nie jest wystarczający do oceny,

d. zalecenia dotyczące dalszego postępowania diagnostyczno-terapeutycznego.

A.5. Sposób przetwarzania.

1. Sposób przetwarzania danych polegać będzie w szczególności na wykonywaniu czynności niezbędnych dla celów realizacji Umowy Głównej, dotyczącej wykonania usługi opisów badań w zakresie diagnostyki obrazowej, opisów badań radiologicznych (RTG) oraz opisów badań tomografii komputerowej (TK),

2. Dane przekazywane drogą elektroniczną, w sposób zdalny, za pośrednictwem publicznej sieci internet, z wykorzystaniem połączenia internetowego (VPN) między ośrodkiem wykonujacym badanie (Administratorem) a ośrodkiem opisującym badanie (Podmiotem przetwarzającym):

A.6. Czas trwania przetwarzania.

Podmiot przetwarzajacy uprawniony jest do przetwarzania danych przez czas trwania Umowy Głównej.

A.7. Podstawy prawne.

1) Ustawa z dnia 6 listopada 2008 r.o prawach pacjenta i Rzeczniku Praw Pacjenta,

2) Ustawa z dnia 15 kwietnia 2011 r.o działalności leczniczej.

3) Rozporządzenie Ministra Zdrowia z dnia 11 kwietnia 2019 r. w sprawie standardów organizacyjnych opieki zdrowotnej w dziedzinie radiologii i diagnostyki obrazowej wykonywanej za pośrednictwem systemów teleinformatycznych.

Załącznik B Podwykonawcy przetwarzania

Nr Załącznika	Wersja	Data aktualizacji	Nr Umowy Głównej	Wprowadzone zmiany (określone w pkt.od .....do)	Czas trwania powierzenia przetwarzania od..do...
B.	0.1				
B					

B.1. Zawiadomienie o zatwierdzeniu podwykonawców przetwarzania

Termin zgłoszenia Administratorowi danych do zatwierdzenia podwykonawcy wynosi 14 dni.

Nr umowy podpowierzenia	Zgłoszony Podwykonawca	Data zgłoszenia Podwykonawcy przez Podmiot przetwarzajacy	Decyzja Administratora	Opis przetwarzania

B.2 Zatwierdzeni podwykonawcy przetwarzania

Administrator danych wyraża zgodę na korzystanie z następujących podmiotów przetwarzających dane:

Nr umowy podpowierzenia	Data zatwierdzenia Podwykonawcy przez Podmiot przetwarzajacy	Nazwa Podwykonawcy	Adres Podwykonawcy

Administrator danych wyraził zgodę na powierzenie danych osobowych ww. podprocesorom do czynności przetwarzania danych. Przetwarzający dane nie może - bez wyraźnej pisemnej zgody Administratora danych - wykorzystywać Podprzetwarzającego dane do innej czynności przetwarzania niż uzgodniona dla niego ani używać innego Podprzetwarzającego poddawanych danych do opisanej czynności przetwarzania.

Załącznik C Polecenie przetwarzania - Instrukcja przetwarzania danych osobowych.

Nr Załącznika	Wersja	Data aktualizacji	Nr Umowy Głównej	Wprowadzone zmiany (określone w pkt.od .....do)	Czas trwania powierzenia przetwarzania od ..do..
C.					
C					

C.1. Przedmiot przetwarzania danych/ instrukcja przetwarzania

Podmiot przetwarzający, wykonuje następujące czynności przetwarzania w postaci:

a) zapewnia transmisję danych - obsługę techniczną i informatyczną oraz oprogramowanie,

b) wykonuje opisy badań RTG i TK,

c) prowadzi dokumentację kontroli jakości usług teleinformatycznych (§3 ust.2 pkt 6-§7 Rozporządzenia)

C.2. Bezpieczeństwo informacji.

Podmiot przetwarzajacy pomaga Administratorowi w wypełnianiu obowiązków wynikających z art. 32 rozporzadzenia o ochronie danych dostarczając niezbędnych informacji na temat podjętych środków zaradczych wobec zidentyfikowanych zagrożeń. Podmiot przetwarzający ma prawo podejmowania decyzji o tym, jakie techniczne i organizacyjne środki bezpieczeństwa należy wdrożyć w celu ustalenia niezbędnego poziomu bezpieczeństwa, jednakże jeśli w opini Administratora wymagane jest podjęcie dodatkowych środków Podmiot przetwarzający wdraża następujące środki, które zostały uzgodnione z Administratorem:

1. Wymagania dotyczące zachowania poufności danych pacjentów.

1) Wymagania dotyczące zachowania tajemnicy informacji dotyczących pacjenta obejmują wszystkich uczestników Umowy, zarówno w trakcie i po realizacji niniejszej Umowy, w szczególności dotyczą; sposobów zabezpieczania danych, zakazu ujawniania w jakiejkolwiek formie treści informacji i udostępniania danych osobowych/informacji innym podmiotom, bez pisemnej zgody Administratora.
2) Podmiot przetwarzajacy jak i jego pracownicy/ współpracownicy, serwisanci zobowiązani są do zachowania w tajemnicy danych osobowych/ informacji związanych z pacjentem, także po śmierci pacjenta,

2. Wymagania dotyczące dostępu do danych osobowych przetwarzanych w imieniu Administratora.

Podmiot przetwarzający udziela dostępu do danych swoim pracownikom wyłącznie w niezbędnym zakresie i tylko tym osobom, które zobowiazane zostały do zachowania poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania poufności. Podmiot przetwarzajacy prowadzi i na bieżaco sprawdza listę osób, którym przyznano dostęp do danych.

3. Wymagania dotyczące pseudonimizacji i szyfrowania danych.

Przesyłanie danych może odbywać się jedynie w niezbędnym zakresie przy zastosowaniu technik szyfrujących.

Strony uznają, że przesyłanie danych z użyciem faksu wiąże się z ryzykiem dla danych osobowych, z powyższym rozwiązanie takie stosowane będzie tylko dorywczo, po wcześniejszym poinformowaniu odbiorcy. Uprawnionym do odbioru faksu jest osoba wskazana przez Stronę do kontaktu w zakresie wysyłania/ odbioru przesyłanych danych.

4. Wymagania dotyczące zapewnienia ciągłej poufności, dostępności i integralności systemów przetwarzania i usług.

Podmiot przetwarzający zapewnia dostęp do danych tylko osobom upoważnionym, zapoznaje pracowników z konsekwencjami prawnymi wynikajacymi z utraty poufności danych pacjentów, zobowiązuje pracowników do przestrzegania procedur pracy w systemach informatycznych, zapoznaje pracowników z zagrożeniami .

5. Wymagania dotyczące możliwości przywrócenia dostępności do danych w systemie informatycznym;

Powyższe wymagania zostały określone w §.3 Umowy Głównej.

6. Wymagania dotyczące procesów regularnego badania, oceny i oceny efektywności środków technicznych i organizacyjnych dotyczących zabezpieczenia bezpieczeństwa informacji osobowych.

Przetwarzanie danych pacjentów wymaga regularnej oceny przez Pomiot przetwarzający zagrożeń związanych z przetwarzaniem i podejmujmowania środków w celu zminimalizowania tych zagrożeń.

7. Wymagania dotyczące dostępu do informacji przez internet.

Wymania uregulowane zostały w § 3 Umowy Głównej.

8. Wymagania dotyczące ochrony informacji podczas przesyłania.

Uregulowania dotyczące zasad dostępu do danych osobowych poprzez połączenie VPN zawiera Załącznik D.

9. Wymagania dotyczące ochrony informacji podczas przechowywania.

   a. dokumentacja medyczna prowadzona w formie papierowej (wydruk z faksu) wymaga zabezpieczeń przed nieuprawnionym udostępnieniem,np. przekazaniem osobie nieuprawnionej, zgubieniem lub zniszczeniem,

   b. dokumentacja medyczna w formie elektronicznej wymaga zabezpieczeń o podwyższonym poziomie gwarantujacym poufność, dostepność i integralność danych.

10. Wymagania dotyczące bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe.

Przetwarzanie danych powinno odbywać sie tylko w strefie chronionej, z prawem dostępu tylko dla pracowników, którym wydano uprawnienia dostępu do pomieszczeń. Przebywanie w strefie chronionej osób nieuprawnionych możliwe jest tylko w obecności osby uprawnionej.

11. Wymagania dotyczące pracy poza siedzibą.

Podmiot przetwarzający może polecić pracownikowi wykonywanie pracy zdalnej tylko wtedy, gdy dysponuje on stosownymi umiejętnościami oraz niezbędnymi środkami technicznymi do wykonywania takich czynności poza miejscem pracy. Podmiot przetwarzający uwzględnia ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez osoby, którym zlecił prace poza siedzibą.

12. Wymagania dotyczące zachowania zwiększonej czujności.

Podmiot przetwarzający zobowiązany jest do stosowania się do wymogów ogłaszanych stopnii alarmowych (zagrożeń w cyberprzestrzeni). Zgłaszania Administratorowi wszelkich informacji o anomaliach w pracy komputerów, w tym poczty e-mail pod nr tel. 94-34-88-460.

13. Wymagania dotyczące rozliczalności.

Podmiot przetwarzający na żądanie Administratora danych jest w stanie wykazać, że osoby, którym udzielił dostępu do danych podlegają wyżej wymienionemu obowiązkowi zachowania poufności.

C.3 Pomoc dla Administratora.

1. Podmiot przetwarzający pomaga Administratorowi w wywiązywaniu się z obowiązków określonych w rozporządzeniu o ochronie danych.

2. Podmiot przetwarzający zobowiązuje się współpracować z Administratorem w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą, opisane w rozdziale III rozporządzenia o ochronie danych.

3. Procedura postępowania w przypadku incydentu bezpieczeństwa, w tym naruszenia ochrony danych:

Podmiot przetwarzający zgłasza incydent bezpieczeństwa/naruszenie ochrony danych Administratorowi niezwłocznie po powzięciu wiadomości. Administrator nie dopuszcza, aby zdarzenie mogące mieć wpływ na bezpieczeństwo systemu, nie zostało formalnie zgłoszone, nawet jeśli problem Podmiot przetwarzający rozwiązał we własnym zakresie.

1) Zgłoszenie powinno nastąpić:

   a. bez zbędnej zwłoki i w miarę możliwości, nie później niż w ciągu 8 godzin od powzięcia wiadomości, w sytuacji, gdy naruszenie będzie wiązało się z zagrożeniem dla praw i wolności osób fizycznych,
   b. bez zbędnej zwłoki i w miarę możliwości, nie później niż w ciągu 8 godzin od powzięcia informacjii, w stuacji gdy incydent będzie się wiązał z przerwaniem ciagłości udzielania świadczeń opieki zdrowotnej lub obrotu i dystrybucji produktów leczniczych przez Administratora, jako operatora usługi kluczowej w sektorze ochrony zdrowia,

2) Zgłoszenie powinno zawierać co najmniej:
   a. w stosunku do stwierdzonego naruszenia danych osobowych:
      - opis charakteru naruszenia danych osobowych oraz o ile to możliwe wskazanie kategorii i przybliżoną liczbę osób, których dane zostały naruszone,
      - ilość i rodzaj naruszonych danych osobowych,
      - opis konsekwencji naruszenia ochrony danych osobowych,
      - opis zastosowanych lub proponowanych do zastosowania przez Podmiot przetwarzajacy środków zaradczych minimalizujących negatywne skutki,

   b. w stosunku do stwierdzonego incydentu, który może mieć wpływ na cyberbezpieczeństwo
      - wskazanie zadania publicznego, na który incydent miał wpływ,
      - liczbę osób, na które incydent miał wpływ,
      - moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
      - zasięg geograficzny obszaru, którego dotyczy incydent,
      - przyczynę zaistnienia incydentu i sposób jego przebiegu oraz jego oddziaływania na systemy informacyjne podmiotu publicznego,
      - informacje o przyczynie i źródle incydentu,
      - informacje o podjętych działaniach naprawczych,
      - inne istotne informacje

3) Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, Podmiot przekazuje w zgłoszeniu informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

C.4 Okres przechowywania / procedury usuwania.

Podmiot przetwarzający w terminie 14 dni od upływu terminu, na jaki Umowa Główna została zawarta , a w przypadku wcześniejszego rozwiązania Umowy Głównej – w terminie 14 dni od daty rozwiązania.

	Okres przechowywania /procedury usuwania	Wpisać jeśli dotyczy
1.	Dane osobowe są przechowywane w systemie informatycznym, po czym są automatycznie usuwane przez Podmiot przetwarzający.	
2.	Po zakończeniu świadczenia usług Podmiot przetwarzający usuwa lub zwraca dane osobowe, w zależności od wyboru Administratora. Wykonanie obowiązku Podmiot przetwarzający poświadczy Administratorowi.	
3.	Kopie zapasowe zawierające dane osobowe, sporządzone przez Podmiot przetwarzający i zarejestrowane na nośnikach elektronicznych stanowią dokumentację Administratora, przechowywaną zgodnie z przepisami prawa. Wszelkie zmiany muszą być udokumentowane i przechowywane w formie pisemnej, w tym w formie elektronicznej, wraz z Umową.	

C.5 Miejsce przetwarzania

Przetwarzanie danych osobowych objętych Umową nie może, bez uprzedniej pisemnej zgody Administratora danych, odbywać się w miejscach innych niż:

a) siedziba Administratora :ul. T. Chałubińskiego 7 w Koszalinie

b) siedziba Podmiotu przetwarzającego: .....

C.6 Instrukcje dotyczące przekazywania danych osobowych do państw trzecich (do wyboru).

Umowa przewiduje/nie przewiduje transferu danych do państw trzecich.

C.7 Procedury audytów, w tym kontroli przetwarzania danych osobowych (do wyboru I lub II).

I Audyt/ kontrola Podmiotu przetwarzającego przeprowdzana przez Administratora.

1) Administrator lub przedstawiciel Administratora przeprowadza okresową kontrolę polegającą na żądaniu udzielania pisemnej informacji lub wyjaśnień dotyczących wykorzystywanych sposobów oraz środków zabezpieczających dane, w celu ustalenia, czy Podmiot przetwarzający spełnia obowiązujące przepisy dotyczące ochrony danych osobowych.

2) Oprócz planowanej kontroli Administrator może przeprowadzić fizyczną kontrolę miejsc, w których przetwarzane są dane osobowe, gdy Administrator uzna to za konieczne, w szczególności w sytuacji wystąpienia incydentu bezpieczeństwa w tym naruszenia ochrony danych.

3) Administrator, powiadomi Podmiot przetwarzający o zamiarze przeprowadzenia audytu/kontroli, w terminie wspólnie ustalonym przez Strony, nie później jednak niż 3 dni robocze przed planowanym terminem audytu/kontroli.

4) W przypadku powzięcia przez Administratora informacji o rażącym naruszeniu zobowiązań wynikających z niniejszej Umowy/przepisów ustawy o ochronie danych osobowych/ rozporządzenia o ochronie danych/ wymagań prawnych lub wystąpienia incydentu bezpieczeństwa, w tym naruszenia ochrony danych Administratorowi przysługuje uprawnienie do dokonania niezapowiedzianej kontroli.

5) Ponadto Podmiot przetwarzający zobowiązuje się do udostępnienia organom nadzorczym, lub przedstawicielom działającym w imieniu tych organów nadzorczych, dostępu do pomieszczeń Podmiotu przetwarzającego, za okazaniem odpowiednich uprawnień.

6) Podmiot przetwarzający jest zobowiązany do zastosowania się do zaleceń pokontrolnych sformułowanych przez Administratora dotyczących zabezpieczenia danych osobowych/ informacji.

7) Podmiotowi przetwarzającemu przysługuje prawo:

   a. kierowania zapytań do Administratora w zakresie prawidłowości wykonania obowiązków dotyczących zabezpieczania powierzonych danych osobowych/informacji chronionych,

   b. do odmowy udzielenia pisemnej informacji lub wyjaśnień oraz udzielenia dostępu do miejsc przetwarzania danych osobowych, prawo ograniczenia wglądu do dokumentów, jeśli informacje, dokumenty lub ich części zawierają tajemnicę przedsiębiorstwa lub ich ujawnienie groziłoby ujawnieniem innych tajemnic podlegających ochronie na podstawie odrębnych przepisów.

II I Audyt/ kontrola Podmiotu przetwarzającego przeprowdzana przez stronę trzecią.

1) Podmiot przetwarzający jest zobowiązany uzyskać raport z badania/ kontroli od niezależnej strony trzeciej,

2) Rodzaje raportów/protokołów z kontroli jakie mogą być stosowane:

   a) .....

   b) .....:

3) Raport z audytu/protokół z kontroli przesyłany bez zbędnej zwłoki do administratora danych w celach informacyjnych. Administrator danych może zakwestionować zakres i/lub sposób zgłoszenia i w takich przypadkach może zażądać ponownej weryfikacji/kontroli o innym zakresie i/lub w inny sposób.

4) Opis zatwierdzonych raportów z audytu / protokołów z kontroli.
   Na podstawie wyników audytu/kontroli Administrator może zażądać podjęcia dalszych środków w celu zapewnienia zgodności z Umową, przepisami prawa polskiego, rozporządzeniem o ochronie danych.

III Audyt/ kontrola przetwarzania danych u Podwykonawcy.

1) Podmiot przetwarzający lub przedstawiciel przedstawiciel podmiotu przetwarzającego ma prawo do kontroli Podwykonawcy.
2) Na podstawie wyników z audytu/ kontroli Administrator może zażądać podjęcia środków w celu zapewnienia zgodności z Umową, przepisami o ochronie danych, wymaganiami prawnymi.
3) Administrator może również zdecydować o rozpoczęciu i udziale w audycie/ kontroli Podwykonawcy, w przypadku, gdy nadzór Podmiotu przetwarzającego nad Podwykonawcą nie dał Administratorowi wystarczającej pewności, że przetwarzanie przez Podwykonawcę odbywa się zgodnie z Umową, rozporządzeniem o ochronie danych osobowych, przepisami prawa.
4) Zaaangażowanie Administratora w kontrolę Podwykonawcy nie zwalnia Podmiotu przetwarzajacego z odpowiedzialności za powierzone do przetwarzania dane.

C.8 Wymagania dotyczące komunikacji pomiędzy serwerami (jednostki wysyłajacej i opisujacej) z użyciem serwera centralnego (do wyboru i uzupełnienia w przypadku pozytywnej odpowiedzi).

Strony przewidują/ nie przewidują w komunikacji pomiędzy serwerami Administratora i Podmiotu przetwarzającego użycia serwera centralnego, do przekierowywania badań do innej jednostki.

C.9 Wymagania dotyczące rozwiązań opartych na «Chmurze» (do wyboru i uzupełnienia w przypadku pozytywnej odpowiedzi).

Umowa przewiduje/ nie przewiduje korzystania przez Podmiot przetwarzający z usług opartych na chmurze.

Dane osobowe podlegające ustawowemu obowiązkowi zachowania poufności mogą być udostępniane dostawcom usług chmurowych, o ile dla takich danych nie istnieje bariera prawna outsourcingu i pozwalają na to odpowiednie przepisy prawa. Podmiot przetwarzający zobowiązany jest regularnie odnotowywać zagrożenia, ponieważ usługi w chmurze stale się rozwijają a zmiany mogą prowadzić do niedopuszczalnego ryzyka, z powyższym w przypadku korzystania z rozwiązań chmurowych innych podwykonawców Podmiot przetwarzający podejmuje odpowiednie środki bezpieczeństwa oparte na analizie ryzyka specyficznego dla danego rozwiązania chmurowego lub o ile to możliwe rezygnuje z usługi w chmurze.

Załącznik D Pozostałe uzgodnienia Stron.

Nr Załącznika	Wersja	Nr Umowy Głównej	Wprowadzone zmiany	Czas trwania powierzenia przetwarzania	Data aktualizacji
D.	0.1				
	1.0				

D.1 Zasady dostępu do danych osobowych/informacji poprzez połączenie VPN.

1. Podmiot przetwarzający dostarczy zewnętrzną adresację IP, z której będzie możliwe zestawienie Zdalnego dostępu do sieci teleinformatycznej Administratora oraz zapewni po swojej stronie możliwość realizacji bezpiecznego połączenia VPN.
2. Połączenie VPN musi być skonfigurowane w sposób gwarantujący zachowanie poufności i rozliczalności dostępu do danych za pomocą systemu monitorowania i logowania działań pracowników Zleceniobiorcy.
3. Połączenie VPN do zasobów Administratora odbywa się wyłącznie za pośrednictwem firmowej sieci Podmiotu przetwarzającego.
4. Dostęp do zdalnego połączenia VPN możliwy jest wyłącznie dla pracowników upoważnionych przez Podmiot przetwarzający.
5. Zdalny dostęp do danych osobowych/informacji Administratora jest realizowany wyłącznie za pomocą sprzętu należącego do Podmiotu przetwarzającego zabezpieczonego systemem antywirusowym.
6. Pracownicy Podmiotu przetwarzającego korzystający z komputerów przenośnych zobowiązani są do zachowania zabezpieczeń kryptograficznych dysków twardych, do zachowania szczególnej ostrożności podczas transportu oraz nieudostępniania sprzętu osobom nieupoważnionym.

D.2 Nadzór

Prace wdrożeniowe i serwisowe odbywają się pod nadzorem uprawnionych pracowników Szpitala.

D.3 Sprawdzenie Podmiotu przetwarzającego w zakresie spełnienia wymogów rozporządzenia o ochronie danych oraz wdrożonych zasad bezpieczeństwa.

«*Ankieta dla podmiotów przetwarzających dane*». Sprawdzenia Podmiotu przetwarzajacego są powtarzane według planu sprawdzeń realizowanego przez Administratora.

Podmiot przetwarzający posiadający certyfikat ISO/IEC 27001 jest zwolniony ze sprawdzenia.

D4. Pozostałe zabezpieczenia:

1).....,

2).....,

3) .....

D.3 Ankieta dla Podmiotu przetwarzającego dane / Survey for entities processing data

Nazwa podmiotu: ……..

Bezpieczeństwo procesowe / Process safety

Wiedza fachowa Professional knowledge			
1.	Czy Podmiot przetwarzający posiada **doświadczenie** w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? (Prosimy o **udokumentowanie** świadczenia przedmiotowych usług w komentarzu. *) Does the processor have experience in providing services related with entrusting data processing? (If yes, how long? Please document providing subject services in comments.)* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
2.	Czy dany podmiot przetwarzający wyznaczył inspektora ochrony danych? *Has the processor appointed a data protection inspector?* **Uwagi** / *Comments*:	art. 37 RODO	☐ Tak / *Yes* ☐ Nie / *No*
1.	Czy Podmiot przetwarzający wyznaczył inspektora ochrony danych, mimo że nie wymagają tego przepisy prawa lub też inną osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji? *Has the processor appointed a data protection inspector despite the fact that it is not required under legal provisions or other person/team responsible for supervisingpersonal data protection in the organisation?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
2.	Czy osoby po stronie Podmiotu przetwarzającego dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane? *Have the persons dedicated by the processor to provide services to the data administrator been trained and familiarised with data protection provisions?Is it documented?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
3.	Czy osoby zatrudnione w Podmiocie przetwarzającym przy przetwarzaniu danych zostały przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemu informatycznego, jeżeli jest on stosowany do przetwarzania danych przez podmiot przetwarzający? *Have the persons employed by the processor at data processing been trained in the scope of the services, including safe use of the IT system, if used,for data processing by the processor?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
Wiarygodność Credibility			

4.	Czy Podmiot przetwarzający posiada referencje od innych podmiotów, które obsługuje/obsługiwał w zakresie przetwarzania danych osobowych na ich zlecenie? Jeśli tak, to prosimy o przedstawienie takich referencji lub co najmniej wskazanie podmiotów. *Does the processor have credentialsfrom other entities to whomhe provides/has provided services in the scope of ordered personal data processing? If yes, please submit such credentials orat least enumerate the relevant entities.* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
5.	Czy stwierdzono prawomocną decyzją UODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający? Prosimy o podanie daty. *Has apersonal data protection infringement by the processor been stated with a valid decision of UODO or other supervisory authority, or with a valid judgement of the court? Please provide a date.* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
8.	Czy Podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów podstępowania?/ planuje przystąpić – podać organizację branżową, izbę lub inną instytucję przygotowująca kodeks? *Does the processor follow codes of conduct adopted by the supervisory authority?/plans to join –please give an industry organisation, chamber or other institution drawing up a code?* **Uwagi** / *Comments*:	art. 40 RODO	☐ Tak / *Yes* ☐ Nie / *No*
9.	Czy Podmiot przetwarzający otrzymał/ planuje wystąpić o - certyfikat zgodności z RODO? *Has the processor received/plans to apply for-a GDPR compliance certificate?* **Uwagi** / *Comments*:	art. 42 RODO	☐ Tak / *Yes* ☐ Nie / *No*
Zasoby Resources			
10.	Czy Podmiot przetwarzający opracował i wdrożył politykę bezpieczeństwa danych osobowych oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych? (bądź: Politykę ochrony danych zgodną z RODO) Jeśli tak, prosimy o udostępnienie dokumentacji na wezwanie. *Has the processor drawn up and implemented the Personal Data Protection Policy and the IT System Management Guide regarding personal data processing?(or:the Data Protection Policy compliant with GDPR) If yes, please provide the documentation upon request.* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
11.	Czy podmiot Przetwarzający opracował i wdrożył politykę ochrony danych lub podobną procedurę? Jeśli tak, prosimy o jej przedstawienie lub informację kiedy zostanie wdrożona. *Has the processor drawn up and implemented the Data Protection Policy or a similar procedure? If yes, please submit such procedure or provide information, when it shall be implemented.* **Uwagi** / *Comments*:	art. 24 RODO	☐ Tak / *Yes* ☐ Nie / *No*
12.	Czy Podmiot przetwarzających wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych? *Has the processor implemented operational instructions regarding a case of personal data protection infringement?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

13.	Czy Podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych? *Does the processor keep a record of infringements of personal data protection provisions, including data security infringements?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
14.	Czy Podmiot przetwarzający prowadzi/ przygotowuje rejestry czynności przetwarzania danych osobowych (jako ADO oraz jako procesor)? *Does the processor keep/drawup registers of personal data processing activities (as a controller and as a processor)?* **Uwagi** / *Comments*:	art. 30 RODO	☐ Tak / *Yes* ☐ Nie / *No*
15.	Czy Podmiot przetwarzający wdrożył zasady zarządzania bezpieczeństwem informacji, w tym: *Has the processor implemented the information security management, including:*		
	system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? Czy posiada certyfikat? *information security management system pursuant to ISO 27001?Doeshe have a certificate?*		☐ Tak / *Yes* ☐ Nie / *No*
	zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002? *information security management principles with elements of applying ISO 27002?*		☐ Tak / *Yes* ☐ Nie / *No*
	[dla podmiotów publicznych] zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami Krajowych Ram Interoperacyjności? *[for public entities] information security management principles compliant with requirements of the National Interoperationality Framework?*		☐ Tak / *Yes* ☐ Nie / *No*
	[dla podmiotów podlegających pod Komisję Nadzoru Finansowego] zasady zarządzania bezpieczeństwem informacji zgodne z odpowiednimi wytycznymi KNF? *for entities subject to the Polish Financial Supervision Authority] information security management principles compliant with relevant KNF guidelines?*		☐ Tak / *Yes* ☐ Nie / *No*
	Czy podmiot wdrożył inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji, itp.? *Has the entity implemented other information protection principles e.g. the Information Security Policy etc.?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

16.	Czy Podmiot przetwarzający dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? (na podstawie szacowania ryzyka pod kątem ochrony prywatności - Privacy Impact Assessment)? *Has the processor selected securities ensuring security of processed personal data with regard to the impact assessment of processing thereof on the rights and freedoms of data subjects?(on the grounds of risk estimation with regard to the privacy protection -Privacy Impact Assessment)?* **Uwagi** / *Comments*:	Odn. do Art. 24, 25, 32 RODO	☐ Tak / *Yes* ☐ Nie / *No*
17.	Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania (Statement of Applicability)? *Has risk estimation been documented e.g. has a Risk Management Plan or a Statement of Applicability been drawn up?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
18.	Czy Podmiot przetwarzający okresowo przeprowadza/ planuje kolejne działania związane z szacowaniem ryzyka pod kątem ochrony prywatności? Czy w przypadku zmiany poziomu ryzyka dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy? *Has the processor been periodically conducting/plans another measures related with estimating the risk with regard to the privacy protection?Does the processor select new technical and organisational measures securing data and relevant to the analysis results in the case of a risk level change?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
19.	Czy Podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym: *Has the processor implemented relevant technical and organisational measures so as to ensurethe security level relevant to the risk related with processing thereof, including:*	Art. 32 ust. 1 lit a)-c) RODO	
	a) pseudonimizację i szyfrowanie danych, *pseudonymization and data encryption,*		☐ Tak / *Yes* ☐ Nie / *No*
	b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, *ability to continuously ensure confidentiality, integrity, accessibility and resilience of processing systems and services,*		☐ Tak / *Yes* ☐ Nie / *No*
	c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, *ability to promptly restore accessibility of personal data and access thereto in case of a physical or technical incident,*		☐ Tak / *Yes* ☐ Nie / *No*
	d) inne środki *other measures* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

20.	Czy Podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa danych osobowych, w tym oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? *Does the processor conduct regular auditson the personal data security principles, including technical and organisational measures effectiveness assessment aimed at ensuring processing security?* **Uwagi** / *Comments*:	Art. 32 ust. 1 lit d) RODO	☐ Tak / *Yes* ☐ Nie / *No*
21.	Czy wnioski z audytów zostały udokumentowane, np. w raport audytowy? *Have the audit conclusions been documented e.g. in an audit report?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
22.	Czy audyt jest przeprowadzany wewnętrznie? Proszę podać datę ostatniego audytu. *Is the audit conducted internally? Please provide the date of the last audit.* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
23.	Czy audyt jest przeprowadzany przez podmiot zewnętrzny? Proszę podać datę ostatniego audytu i audytora (o ile pozwala na to klauzula poufności). *Is the audit conducted by an external entity?Please provide the date of the last audit and the auditor (if permitted under a confidentiality clause).* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
24.	Czy podmiot Przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez Administratora danych lub audytora upoważnionego przez Administratora danych? *Is the processor prepared to subject to the audit conducted by the data administrator or an auditor authorised by the data administrator?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
25.	Czy osoby delegowane do obsługi ADO posiadają nadane upoważnienia do przetwarzania danych? Czy zostało to udokumentowane? Prosimy o przedłożenie listy osób upoważnionych, które będą obsługiwać ADO? *Do persons delegated to provide PDA services have authorisations to process data?Has it been documented?Please submit a list of authorised persons who shall provide PDA services.* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
26.	Czy osoby upoważnione do przetwarzania danych w ramach obsługi ADO zostały obowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane? *Have persons authorised to process data within the PDA services been obliged to keep them in secret? Has it been documented?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
27.	Czy Podmiot przetwarzający wprowadził procedurę upoważniania osób uczestniczących w przetwarzaniu danych osobowych do ich przetwarzania? *Has the processor introduced a procedure of authorising persons participating in personal data processing to process them?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

28.	Czy dane są przekazywane do państw trzecich poza obszar EOG? Proszę wskazać, w którym kraju znajdują się serwery/infrastruktura. *Are data transferred to third parties outside the EEA area? Please indicate a country where servers/infrastructure are/is located.* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
29.	Czy dane są powierzane do dalszego przetwarzania? Proszę podać nazwę sub-processora. *Are data entrusted for further processing?Please give a sub-processor's name.* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

Kontrola dostępu / Access control (A.9)

Polityka kontroli dostępów *Access control policy*			
30.	Czy jest dokument określający politykę kontroli dostępów do systemów przetwarzających dane osobowe? *Is there a document stipulating the control policy of the access to personal data processing systems?* **Uwagi** / *Comments*:	A.9	☐ Tak / *Yes* ☐ Nie / *No*
31.	Czy w czasie opracowywania dokumentu została przeprowadzona analiza ryzyka? *Was a risk analysis conducted in the course of drawing up the document?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
32.	Jak często polityka jest poddawana przeglądowi i aktualizacji? *How often is the policy subjected to a review and update?* **Uwagi** / *Comments*:		
33.	Czy jest zachowana minimalizacji dostępów? *Is access minimisation preserved?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
34.	Czy jest kontrola dostępu do usług sieciowych? *Is there a network services access control?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
35.	Czy jest przeprowadzona segmentacja sieci? *Is there a network segmentation conducted?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
Zarządzanie dostępem pracowników *Employee Access management*			
36.	Czy jest wprowadzony formalny proces przydzielania praw dostępów? Has a formal process of granting access rights been introduced? **Uwagi** / Comments:	A.9	☐ Tak / *Yes* ☐ Nie / *No*
37.	Czy jest wprowadzono proces akceptacji dostępów do danych osobowych? Has a personal data access acceptance process been introduced? **Uwagi** / Comments:		☐ Tak / *Yes* ☐ Nie / *No*
38.	W jaki sposób są odbierane i dostosowywane dostępy do zmieniających się obowiązków pracowników? How is the access selected and adjusted to changing employees duties? **Uwagi** / Comments:		

Rozliczalność Accountability			
39.	Czy jest wprowadzony centralny system zarządzania tożsamością pracownika? *Is there an introduced central system of employee's identity management?* **Uwagi** / *Comments*:	A.9	☐ Tak / *Yes* ☐ Nie / *No*
40.	Czy wszystkie próby dostępu do danych są rejestrowane? *Are all data access attempts registered?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
41.	Czy jest wprowadzony system podwójnego uwierzytelnienia dla uprzywilejowanych użytkowników systemu? *Is there a system of double certification introduced for privileged system users?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

Kryptografia / Cryptography (A.10)

Polityka stosowania zabezpieczeń kryptograficznych *Cryptographic securities policy*			
42.	Czy informacje na stacjach roboczych są zaszyfrowane? *Is the information on workstations encrypted?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
43.	Czy na urządzeniach mobilnych informacje są zaszyfrowane? *Is the information on mobile devices encrypted?* **Uwagi** / *Comments*:		
44.	Czy zostały określone zasady zabezpieczeń kryptograficznych do przesyłania danych osobowych między systemami? *Have the encryption securities principles for transmitting personal data between systems been stipulated?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
Zarządzanie kluczami *Keys management*			
45.	Czy określono proces zarządzania kluczami? *Has the keys management process been stipulated?* **Uwagi** / *Comments*:	A.10	☐ Tak / *Yes* ☐ Nie / *No*

Bezpieczna eksploatacja / Safe exploitation (A.12)

Zabezpieczenie AV *AV security*			
46.	Czy oprogramowanie antywirusowe (AV) jest zainstalowane na wszystkich stacjach roboczych pracowników? *Has antivirus (AV) software been installed on all employees workstations?* **Uwagi** / *Comments*:	A.12	☐ Tak / *Yes* ☐ Nie / *No*
47.	Czy serwery mają zainstalowane oprogramowanie AV? *Do servers have AV software installed?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
48.	Czy są monitorowane anomalie sieciowe wykrywające działanie niepożądanego oprogramowania? *Are network anomalies detecting*		☐ Tak / *Yes* ☐ Nie / *No*

	unwanted software operations monitored? **Uwagi** / *Comments*:		
Kopie bezpieczeństwa Backups			
49.	Czy są wprowadzone regulacje dotyczące wykonywania kopii bezpieczeństwa? *Are there regulations regarding making backups introduced?* **Uwagi** / *Comments*:	A.12	☐ Tak / *Yes* ☐ Nie / *No*
50.	Czy istnieje instrukcja/plan odtworzenia danych z kopii bezpieczeństwa? *Is there an instruction/a plan of restoring data from backups?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
51.	Czy są przeprowadzane próby odtworzenia kopi bezpieczeństwa? *Are there trial backups recoveries?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
Zarządzanie podatnościami technicznymi i oprogramowaniem Technical vulnerabilities and software management			
52.	Czy jest zatwierdzona polityka zarządzaniami podatnościami? *Is there anapproved vulnerabilities management policy?* **Uwagi** / *Comments*:	A.12	☐ Tak / *Yes* ☐ Nie / *No*
53.	Czy jest zatwierdzona polityka aktualizacji systemów na stacjach roboczych? *Is there an approved systems update on workstations policy?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
54.	Czy jest zatwierdzona lista dozwolonego oprogramowania na stacjach roboczych? *Is there an approved list ofsoftware permitted on workstations?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
55.	Czy jest systematyczna weryfikowana lista zainstalowanych programów na stacjach roboczych? *Is therea systematically verified list of programmes installed on workstations?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

Bezpieczeństwo komunikacji / Communication security (A.13)

Bezpieczeństwo komunikacji Communication security			
56.	Czy są wprowadzone zabezpieczenia dostępowe do usług sieciowych po sieci? (Jeżeli tak to proszę wypisać jakie w komentarzu) *Are there securities introduced regarding the access to network services available "on the network"? (If yes, which ones? Put info In comments.)* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
57.	Czy są wprowadzone mechanizmy wykrywające anomalie sieciowe? *Are there introduced mechanisms detecting network anomalies?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
58.	W jaki sposób są rozdzielone grupy pracowników, systemy? *How are the employees groups and systems divided?*		☐ Tak / *Yes* ☐ Nie / *No*

	Uwagi / *Comments*:		
59.	Czy są zatwierdzone kanały przekazywania informacji w zależności od ich poufności wewnątrz organizacji? *Are there approved information transmission channels depending on the confidentiality thereof inside the organisation?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
60.	Czy są zatwierdzone kanały przekazywania informacji na zewnątrz organizacji? *Are there approved channels of forwarding information outside the organisation?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

Pozyskiwanie, rozwój i utrzymanie systemów / Soliciting, development and maintenance of systems (A.14)

Pozyskiwanie, rozwój i utrzymanie systemów			
61.	Czy wprowadzono politykę rozwoju produktów/oprogramowania? *Has the policy of products/software development been introduced?* **Uwagi** / *Comments*:	A.14	☐ Tak / *Yes* ☐ Nie / *No*
62.	Czy wprowadzono formalne mechanizmy kontroli zmiany? (Jeżeli tak to proszę wypisać jakie w komentarzu) *Has formal mechanisms of change control been introduced? (If yes, which ones? Put info In comments.)* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
63.	Czy na koniec cyklu produkcji są przeprowadzane testy? (Jeżeli tak to proszę wypisać jakie w komentarzu) *Are there tests conducted at the end of aproduction cycle? (If yes, which ones? Put info In comments.)* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*

Zarządzanie incydentami związanymi z bezpieczeństwem informacji / Management of incidents related with information security (A.16)

1.6.1 Incydenty bezpieczeństwa Security incidents			
64.	Czy są instrukcje regulujące incydenty bezpieczeństwa informacji? *Are there instructions regulating information security incidents?* **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*
65.	Czy podwykonawcy są zobowiązani do informowania o incydentach bezpieczeństwa? Are the subcontractors obliged to inform about security incidents? **Uwagi** / *Comments*:		☐ Tak / *Yes* ☐ Nie / *No*