Samodzielny Publiczny Zakład Opieki Zdrowotnej w Puławach
ul. Józefa Bema 1, 24-100 Puławy, Tel: (81) 450 22 74, Fax (81) 470 83 01, , Infolinia dla Pacjentów (81) 450 25 01

Puławy, dnia 29.10.2024 r.

DZP.26.118.2024

ZAPROSZENIE DO SKŁADANIA OFERT NR ZSO 59/2024

1. Opis przedmiotu zamówienia: W ramach zamówienia zaplanowane są usługi doradcze z cyberbezpieczeństwa, RODO i Sygnalistów, Audyt KSC i MZ, miesięczne raporty ze skanów płatności na ataki na sieć IT SP ZOZ:
- Doradztwo w zakresie cyberbezpieczeństwa dla operatora usługi kluczowej
- Bieżące wsparcie w wykonywaniu obowiązków operatora usługi kluczowej
- Wsparcie/doradztwo dla Inspektora Ochrony Danych (IOD)
- Wdrożenie i zarządzanie wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów
2. Wymagany termin realizacji przedmiotu zamówienia: 12 miesięcy od podpisania umowy.

3. Przy wyborze oferty do realizacji Zamawiający będzie kierował się kryterium: 100 % cena.

4. Wykluczenie z postepowania.
a. Na podstawie art. 7 ust. 1 Ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, z postępowania wyklucza się:
1. wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 Ustawy;
2. wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 Ustawy;
3. wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 Ustawy.
b. Wykluczenie następuje na okres trwania okoliczności określonych w ust. 1 Ustawy.
c. W przypadku wykonawcy lub uczestnika konkursu wykluczonego na podstawie ust. 1 Ustawy, zamawiający odrzuca wniosek o dopuszczenie do udziału w postępowaniu o udzielnie zamówienia publicznego lub ofertę takiego wykonawcy lub uczestnika konkursu, nie zaprasza go do złożenia oferty wstępnej, oferty podlegającej negocjacjom, oferty dodatkowej, oferty lub oferty ostatecznej, nie zaprasza go do negocjacji lub dialogu, a także nie prowadzi z takim wykonawcą negocjacji lub dialogu, odrzuca wniosek o dopuszczenie do udziału w konkursie, nie zaprasza do złożenia pracy konkursowej lub nie przeprowadza oceny pracy konkursowej, odpowiednio do trybu stosowanego do udzielenia zamówienia publicznego oraz etapu prowadzonego postępowania o udzielenie zamówienia publicznego

5. Wykonawca, składając ofertę, zobowiązany jest złożyć następujące dokumenty:
1) formularz oferty wg załączonego wzoru – Załącznik nr 1
2) aktualny wpis do ewidencji działalności gospodarczej lub odpis KRS-u,
3) opis przedmiotu zamówienia potwierdzający wymagania zamawiającego – Załącznik nr 2,
4) oświadczenie RODO – Załącznik nr 3
5) parafowany projekt umowy – Załącznik nr 4.

6. Opis sposobu obliczenia ceny w składanej ofercie:
Cena powinna zawierać:
1) wartość dostawy/usługi/roboty budowlanej* określoną w oparciu o przedmiot zamówienia,
2) obowiązujący podatek od towarów i usług VAT,
3) cena podana przez wykonawcę za świadczoną usługę/dostawę/robotę budowlaną* jest obowiązująca przez okres ważności umowy i nie będzie podlegała waloryzacji w okresie jej trwania.

7. Opis sposobu przygotowania oferty:
1) Ofertę należy ją złożyć w nieprzejrzystej i zamkniętej kopercie,
2) Cena podana w złożonej ofercie ma być podana cyfrowo i słownie. Oferta cenowa winna być sporządzona wyłącznie w języku polskim i musi obejmować całość zamówienia. Formularz należy wypełnić czytelną i trwałą techniką.

8. Miejsce i termin złożenia oferty:
1) Ofertę należy złożyć w terminie do dnia 07.11.2024 r., do godz. 08:00 w siedzibie Zamawiającego, budynek administracyjny, ul. Bema 1, Puławy, I piętro, Sekretariat lub na adres e-mail: zp@szpitalpulawy.pl. Formularz ofertowy wraz z załącznikami podpisuje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym w formie PAdES typ wewnętrzny(w przypadku ofert przesłanych drogą e- mail).
2) Oferta otrzymana przez Zamawiającego po terminie podanym powyżej zostanie wykonawcy zwrócona bez otwierania na jego żądanie lub po upływie 60 dni od złożenia zniszczona.

9. Miejsce i termin otwarcia oferty:
Otwarcie złożonych ofert nastąpi w dniu 07.11.2024r. o godz. 08:15 w siedzibie Zamawiającego, budynek administracyjny, ul. Bema 1, Puławy, parter, pokój nr 5.

10. Osobami uprawnionymi do kontaktów z wykonawcami są:
- w sprawie procedury zamówienia –Justyna Gawęda, tel. 81 45 02 389
- w sprawie przedmiotu zamówienia – Grzegorz Czech tel. 81 45 02 297

[*imię i nazwisko, nr tel.*]

12. Zamawiający zastrzega sobie prawo odstąpienia od wyboru ofert bez podania przyczyny.

p.o. DYREKTOR
Samodzielnego Publicznego Zakładu
Opieki Zdrowotnej w Puławach
mgr inż. Krzysztof Siejka

.....

[*data i podpis Zamawiającego*]

*niepotrzebne skreślić

Załącznik nr 1 do ZSO 58/2024

.....
[*nazwa, adres, tel. wykonawcy*]

OFERTA

Nawiązując do zaproszenia do składania ofert na: Usługi doradztwa w zakresie Cyberbezpieczeństwa, RODO i Sygnalistów dla SP ZOZ w Puławach

1. Oferuję wykonanie przedmiotu zamówienia za:
   cenę netto: ..... zł. podatek VAT: ..... %
   cenę brutto: ..... zł. (słownie: ..... złotych).

2. Termin realizacji zamówienia: 12 miesięcy od dnia podpisania umowy.
- adres email Wykonawcy.....

3. Kryterium oceny oferty: cena 100%.

4. Wyrażam zgodę na warunki płatności określone w zaproszeniu do składania ofert.

5. Oświadczam, że zapoznałem się z treścią klauzuli stanowiącej Zał. Nr 3 do zaproszenia do składania ofert o znaku ZSO 58/2024 na administrowanie siecią komputerową Zleceniodawcy, w tym z informacją o celu i sposobach przetwarzania danych osobowych oraz prawie dostępu do treści swoich danych i prawie ich poprawiania, który to fakt potwierdzam własnoręcznym podpisem opisem oraz opisem przedmiotu zamówienia oraz projektem umowy i nie wnoszę do nich zastrzeżeń. Jednocześnie oświadczam, iż wszystkie podane dane osobowe są prawdziwe i aktualne.

6. Oświadczam, że spełniam warunki określone przez Zamawiającego.

7. Załącznikami do niniejszego formularza oferty stanowiącego integralną część oferty są:
1) aktualny wpis do ewidencji działalności gospodarczej lub odpis z KRS-u
2) druk Oferta – Załącznik nr 1
3) opis przedmiotu zamówienia – Załącznik nr 2
4) oświadczenie RODO – Załącznik nr 3
5) parafowany projekt umowy – Załącznik nr 4

.....
[*pieczątka i podpis osoby uprawnionej*]

Załącznik nr 2 do ZSO 58/2024

Opis przedmiotu zamówienia

Doradztwo w zakresie cyberbezpieczeństwa dla operatora usługi kluczowej obejmujące:

1. Bieżącą aktualizację, przy ścisłej współpracy z Operatorem Usługi Kluczowej (OUK), dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymogami norm PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301;
2. Przygotowanie przy ścisłej współpracy z OUK corocznej Analizy Ryzyka (oszacowania ryzyka) wystąpienia incydentu, rozumianego jako zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo świadczonej Usługi Kluczowej;
3. Doradztwo w sprawach związanych z zarządzaniem oszacowanym ryzykiem;
4. Przeprowadzenie corocznego szkolenia z zakresu cyberbezpieczeństwa dla kadry zarządzającej oraz pracowników jednostki – szkolenie stacjonarne 1 dzień roboczy wraz z udostępnieniem platformy szkoleniowej online na okres 30 dni kalendarzowych;
5. Przeprowadzenie warsztatów w zakresie cyberbezpieczeństwa, skierowanych do kadry zarządzającej jednostki;
6. Przeprowadzenie wymaganego przepisem art. 15 ust. 1 Ustawy KSC Audytu Bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej zakończonego raportem z audytu przez wyspecjalizowana kadrę spełniającą wymogi Ustawy KSC oraz Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r., poz. 1999) tj. przynajmniej dwóch audytorów legitymujących się odpowiednimi certyfikatami – w celu spełnienia obowiązku prawnego przeprowadzenia audytu co najmniej raz na 2 lata.

Bieżące wsparcie w wykonywaniu obowiązków operatora usługi kluczowej poprzez:

1. Doradztwo osobie wyznaczonej przez operatora usługi kluczowej i będącej odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w sprawach wymagających wykonywania obowiązków wobec tych podmiotów;
    a. doradztwo wobec powołanej przez operatora usługi kluczowej wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo w podejmowanych czynnościach i wykonywanych zadaniach nałożonych obowiązkami prawnymi Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077) – zwanej dalej „Ustawą KSC" – t.j. w zakresie dotyczącym:
        i. zarządzania incydentami oraz obsłudze incydentów, w szczególności poprzez pomoc merytoryczną w:
            1. – wyszukiwaniu powiązań między incydentami,
            2. – usuwaniu przyczyn wystąpienia incydentów,
            3. – opracowywaniu wniosków wynikających z obsługi incydentu,
            4. – dokonaniu prawidłowej rejestracji zaistniałego incydentu;
        ii. eliminacji podatności systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej w celu ograniczenia zagrożeń cyberbezpieczeństwa, które doprowadziły lub mogłyby doprowadzić do incydentu;

iii. współdziałania wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo z właściwym CSIRT w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia;

2. W przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia -świadczenie pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT,
3. Świadczenie pomocy w przygotowaniu zgłoszenia informacji o innych incydentach, zagrożeniach cyberbezpieczeństwa, szacowaniu ryzyka, podatnościach lub wykorzystywanych technologiach – zgodnie z postanowieniem art. 13 ust. 1 Ustawy KSC – do właściwego CSIRT (lub sektorowego zespołu cyberbezpieczeństwa) w przypadku woli operatora usługi kluczowej dokonania takiego zgłoszenia;
4. Doradztwo w zakresie przekazanych operatorowi usługi kluczowej zaleceń pokontrolnych dotyczących usunięcia stwierdzonych nieprawidłowości, wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa;
5. Przygotowanie projektów informacji do organu właściwego do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń pokontrolnych wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa, o których mowa w punkcie powyżej;
6. Sporządzanie informacji w wymiarze nieprzekraczającym dwóch w miesiącu, w sprawach dotyczących prawnych zagadnień cyberbezpieczeństwa;
7. Pomoc w realizacji wynikającego z Ustawy KSC obowiązku operatora usługi kluczowej w zakresie zapewnienia osobom, na rzecz których zadanie publiczne jest realizowane, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, poprzez przygotowanie, a następnie - w przypadku zaistnienia prawnej konieczności -aktualizację, odpowiedniej informacji w postaci broszury dostosowanej do umieszczenia na stronie internetowej operatora usługi kluczowej.
8. Wsparcia i doradztwo dla Działu IT OUK w zakresie rozwiązań technologicznych dotyczących zabezpieczeń systemów informatycznych przetwarzających dane osobowe; wydawanie zaleceń w ramach konsultacji dotyczących wyposażenia operatora usługi kluczowej w urządzenia do bezpiecznego przechowywania i zabezpieczenia danych osobowych poprzez opiniowanie przedstawionych przez operatora usługi kluczowej ofert wyposażenia sprzętowego;
9. Konsultacje działu informatycznego operatora usługi kluczowej w sprawach związanych z przetwarzaniem danych osobowych w systemie informatycznym;
10. Wykonanie AUDYTU BEZPIECZEŃSTWA INFORMACJI zgodnie z wymaganiami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024, poz. 773), lub innych przepisów wydanych w miejsce tego rozporządzenia;
11. Wykonanie kwartalnych testów podatności infrastruktury teleinformatycznej uznanymi narzędziami wraz z przygotowaniem raportu z opisem podatności oraz rekomendacjami dotyczącymi ich usunięcia w języku polskim.

Wsparcie/doradztwo dla Inspektora Ochrony Danych (IOD) poprzez:

1. Wykonywanie audytów dotyczących przestrzegania przepisów o ochronie danych osobowych;
2. Pomoc w aktualizacji dokumentacji tj. rejestru czynności przetwarzania danych osobowych, rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora oraz polityki ochrony danych osobowych – w przypadku zaistnienia zmiany przepisów prawa w w/w zakresie lub z wniosku klienta;
3. Wykonanie corocznej analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych;
4. Przeprowadzenie corocznych szkoleń z zakresu przetwarzania danych osobowych dla kadry zarządzającej oraz pracowników jednostki – szkolenie stacjonarne 1 dzień roboczy wraz z udostępnieniem platformy szkoleniowej online na okres 30 dni kalendarzowych.
5. Bieżące wsparcie w wykonywaniu obowiązków Inspektora Ochrony Danych:
    a. informowanie o obowiązkach spoczywających na jednostce klienta na mocy przepisów o ochronie danych oraz doradztwo w tym zakresie;
    b. monitorowanie przestrzegania przepisów wewnętrznych, polityk i procedur stosowanych przez jednostkę klienta w zakresie ochrony danych osobowych;
    c. podejmowanie działań zwiększających świadomość prawną jednostki, jej pracowników i osób wykonujących pracę w oparciu o umowy cywilnoprawne
    d. wchodzących w skład kadry pracowniczej, w zakresie przetwarzania i ochrony danych osobowych;
    e. udzielanie jednostce zaleceń co do oceny skutków dla ochrony danych oraz nadzorowanie realizacji zaleceń pokontrolnych;
    f. doradztwo w przypadku wystąpienia wymaganej na podstawie przepisów prawa współpracy z Prezesem Urzędu Ochrony Danych Osobowych, będącym organem nadzorczym w sprawach z zakresu ochrony danych osobowych;
    g. wsparcie Inspektora Ochrony Danych w pełnieniu przez niego funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych oraz w stosownych przypadkach – w prowadzeniu konsultacji w sprawach dotyczących danych osobowych.

Wdrożenie i zarządzanie wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów.

1. Opracowanie wewnętrznego aktu normatywnego pod nazwą „procedura zgłoszeń wewnętrznych" ustanawiającego procedurę zgłoszeń wewnętrznych, zgodną z wymogami art. 25 ustawy o ochronie sygnalistów:
    a. przygotowanie projektu „procedury zgłoszeń wewnętrznych",
    b. wsparcie w toku konsultacji z zakładową organizacją związkową lub przedstawicielami pracowników, o których mowa w art. 24 ust. 3 ustawy o ochronie sygnalistów oraz ewentualną, korektę „procedury" w wyniku tych konsultacji,
    c. pomoc we wprowadzeniu „procedury zgłoszeń wewnętrznych" do stosowania.
2. Wdrożenie sposobów przyjmowania zgłoszeń od sygnalistów, o których mowa w art. 26 ustawy o ochronie sygnalistów, w tym:
    a. doradztwo w zakresie wyboru sposobów przyjmowania zgłoszeń, o których mowa w art. 26 ust. 1 i 2 ustawy o ochronie sygnalistów,
    b. wsparcie we wprowadzeniu, wybranych przez Zamawiającego, sposobów przyjmowania zgłoszeń, uwzględniających wymagane środki bezpieczeństwa informacji oraz poufności tożsamości sygnalisty i innych osób chronionych,

c. przyjęcie przez Wykonawcę obsługi elektronicznych (e-mail) sposobów przyjmowania zgłoszeń, potwierdzania przyjęcia zgłoszenia, przekazywania informacji zwrotnej oraz dostarczania informacji na temat procedury zgłoszeń wewnętrznych z zastosowaniem rozwiązań technicznych i organizacyjnych zapewniających zgodność z ustawą o ochronie sygnalistów), zgodnie z art. 28 ustawy o sygnalistach;

3. Opracowanie wymaganego na podstawie art. 29 ustawy o ochronie sygnalistów, Rejestru zgłoszeń wewnętrznych:
   a. w formie papierowej (tradycyjnej) lub elektronicznej (uwzględniającej środki bezpieczeństwa teleinformatycznego zapewniające ochronę informacji oraz poufności tożsamości sygnalisty i innych osób chronionych),
   b. stanowiskowe przeszkolenie osób upoważnionych (zobowiązanych) do prowadzenia Rejestru.
4. Realizację obowiązków wynikających z przepisów prawa ochrony danych osobowych (RODO), w zakresie wynikającym z ustawy o ochronie sygnalistów:
   a. przeprowadzenie analizy ryzyka procesów przetwarzania danych osobowych sygnalistów i innych osób, których dane podlegać będą przetwarzaniu,
   b. ocena skutków przetwarzania danych osobowych (DPIA), w ramach procedury zgłoszeń wewnętrznych,
   c. opracowanie wzorów obowiązków informacyjnych z art. 13 i art. 14 RODO, uwzględniających wyłączenia i ograniczenia prawne, wynikające z prawa ochrony sygnalistów,
   d. wsparcie w aktualizacji i uzupełnianiu dokumentacji RODO: polityki ochrony danych oraz rejestru czynności przetwarzania.
5. Przeprowadzenie szkolenia dedykowanego kadrze zarządzającej (kierownictwu), obejmującego zagadnienia:
   a. kim jest sygnalista i jaką rolę pełni w organizacji,
   b. wymogi prawne w zakresie ochrony sygnalistów w Polsce,
   c. korzyści i zagrożenia związane z systemami przyjmowania zgłoszeń od sygnalistów,
   d. rola kierownictwa organizacji w zapewnieniu efektywnego i skutecznego systemu zgłaszania nieprawidłowości,
   e. ryzyka zarządzania personelem, w odniesieniu do nowych obowiązków wynikających z przepisów prawa ochrony sygnalistów,
   f. metodyka zapobiegania działaniom odwetowym (za podejmowanie których grozi odpowiedzialność karna z art. 55 ustawy o ochronie sygnalistów, nawet do 3 lat pozbawienia wolności).
6. Przeszkolenie pracowników, w zakresie prawa ochrony sygnalistów, obejmujące zagadnienia:
   a. kim jest sygnalista i jaką rolę pełni w organizacji,
   b. wymogi prawne w zakresie ochrony sygnalistów w Polsce,
   c. o czym mówi procedura zgłaszania nieprawidłowości,
   d. w jaki sposób zgłaszać nieprawidłowość w organizacji.
7. Coroczny przegląd oraz aktualizację procedury zgłoszeń wewnętrznych, do wymogów wynikających ze zmian w obszarze prawa ochrony sygnalistów oraz metodologii i metodyki w tym zakresie.

8. Organizacja i przeprowadzenia spotkania bezpośredniego z sygnalistą, w przypadku złożenia takiego wniosku (zgodnie z art. 26 ust. 6 ustawy o ochronie sygnalistów, zgłaszający może złożyć wniosek o przyjęcie zgłoszenia ustnego, za pomocą bezpośredniego spotkania zorganizowanego w terminie 14 dni od dnia otrzymania takiego zgłoszenia), w szczególności:
    a. zorganizowanie i przeprowadzenie spotkania zapewniającego zachowanie tajemnicy w zakresie informacji i danych osobowych,
    b. udokumentowanie przedsiębranych działań i uzyskanych informacji.
9. Doradztwo w zakresie prowadzenia działań następczych, obejmujące:
    a. ocenę, czy przekazane przez sygnalistę zgłoszenie, stanowi informację o naruszeniu prawa, w rozumieniu przepisów ustawy o ochronie sygnalistów,
    b. rekomendacje odnośnie procedury weryfikacji prawdziwości informacji oraz przeciwdziałania naruszeniu prawa będącego przedmiotem zgłoszenia, w tym dokumentowania podejmowanych czynności,
    c. wsparcie w zakresie zamknięcia procedury działań następczych i informacji zwrotnej w sprawie ujawnionych zagrożeń;
10. Doradztwo w zakresie identyfikowania i oceny działań odwetowych oraz przeciwdziałania takim działaniom, w tym:
    a. ocenę, czy ujawnione bądź zgłoszone działanie lub zaniechanie, stanowi działanie odwetowe albo próbę lub groźbę zastosowania działania odwetowego, w rozumieniu przepisów ustawy o sygnalistach,
    b. rekomendacje odnośnie wdrożenia procedury ochrony sygnalisty przed działaniami odwetowymi oraz adekwatnych środków ochrony, w tym dokumentowania podejmowanych czynności,
    c. wsparcie w zakresie informacji zwrotnej w sprawie ujawnionych zagrożeń.

.....
miejscowość, data

.....
podpis upoważnionego przedstawiciela

Dział Zamówień Publicznych
Justyna Gawęda
Tel: 81 450 23 89
zp@szpitalpulawy.pl

NIP 7162238942
REGON: 431205731
KRS: 0000026256
BDO: 000041779
ePUAP:/SPZOZPULAWY/SkrytkaESP

spzoz@szpitalpulawy.pl
www. szpitalpulawy.pl,
Nr księgi Rejestrowej: 000000002932
Bank Millennium SA - 12 1160 2202 0000 0000 6018 9573

Załącznik nr 3 do ZSO 58/2024

Oświadczenie wymagane od Wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu – ZSO 58/2024 Oświadczam, że nie przekazuję danych osobowych innych niż bezpośrednio mnie/reprezentowanego przeze mnie podmiotu dotyczących/ Oświadczam, że wobec mnie/reprezentowanego przeze mnie podmiotu zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO (niepotrzebne skreślić).

.....
Miejscowość, data

.....
podpis osoby upoważnionej

Dział Zamówień Publicznych
Justyna Gawęda
Tel: 81 450 23 89
zp@szpitalpulawy.pl

NIP 7162238942
REGON: 431205731
KRS: 0000026256
BDO: 000041779
ePUAP:/SPZOZPULAWY/SkrytkaESP

spzoz@szpitalpulawy.pl
www. szpitalpulawy.pl,
Nr księgi Rejestrowej: 000000002932
Bank Millennium SA - 12 1160 2202 0000 0000 6018 9573

Załącznik nr 4 do ZSO 58/2024

Wzór umowy

Umowa .....
usługi doradztwa w zakresie obowiązków dotyczących cyberbezpieczeństwa przypisanych operatorowi usługi kluczowej, doradztwa w zakresie ochrony danych osobowych oraz doradztwa informatycznego
(zwana dalej „Umową")

zawarta w dniu ..... r. w Puławach,

pomiędzy:

Samodzielnym Publicznym Zakładem Opieki Zdrowotnej w Puławach, z siedzibą przy ul. Bema 1, 24-100 Puławy, wpisanym przez Sąd Rejonowy Lublin - Wschód w Lublinie z siedzibą w Świdniku, VI Wydział Gospodarczy Krajowego Rejestru Sądowego do Rejestru Stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz Samodzielnych Publicznych Zakładów Opieki Zdrowotnej pod nr KRS: 0000026256, REGON: 431205731, NIP: 7162238942, (wydruk z Centralnej Informacja Krajowego Rejestru Sądowego z dnia zawarcia Umowy stanowi Załącznik nr 1)
- reprezentowanym przez: –
zwanym w dalszej części Umowy **„Zleceniodawcą"**
a
....., prowadzącym jednoosobową działalność gospodarczą pod firmą..... z siedzibą ....., ..., NIP: .....,
zwanym w dalszej części Umowy **„Zleceniobiorcą".**

§ 1
Przedmiot Umowy

Zleceniodawca zleca a Zleceniobiorca przyjmuje zlecenie dotyczące świadczenia usługi doradztwa w zakresie obowiązków dotyczących cyberbezpieczeństwa przypisanych operatorowi usługi kluczowej na podstawie Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2023 r., poz. 913 ze zm.; dalej jako: **„Ustawa KSC"**), doradztwa w zakresie ochrony danych osobowych oraz doradztwa informatycznego, w zamian za co Zleceniodawca zobowiązuje się do zapłaty umówionego wynagrodzenia. Zakres czynności ujętych w paragrafach § 2 - § 4 zwany będzie w dalszej części Umowy **„Usługą".**

§ 2

Szczegółowy zakres świadczonej przez Zleceniobiorcę usługi – doradztwo w zakresie cyberbezpieczeństwa dla operatora usługi kluczowej

1. Zleceniobiorca w ramach świadczonej usługi doradztwa w zakresie obowiązków dotyczących cyberbezpieczeństwa przypisanych operatorowi usługi kluczowej na podstawie regulacji Ustawy KSC zobowiązuje się do wykonania następujących czynności:
   1) doradztwa na rzecz Zleceniodawcy w przystosowaniu do wdrożenia i obowiązywania u Zleceniodawcy dokumentacji dotyczącej:
      a) systemu zarządzania bezpieczeństwem informacji, wytworzonej zgodnie z wymaganiami normy PN-EN ISO/IEC 27001,
      b) systemu zarządzania ciągłością działania usługi Zleceniodawcy, wytworzonej zgodnie z wymaganiami normy PN-EN ISO 22301;
   2) doradztwa osobie wyznaczonej przez Zleceniodawcę i będącej odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w sprawach wymagających wykonywania obowiązków wobec tych podmiotów;
   3) doradztwa wobec powołanej przez operatora usługi kluczowej wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo - o której mowa w art. 14 ust. 1 Ustawy KSC, powołanej przez Zleceniodawcę będącego operatorem usługi kluczowej - w podejmowanych czynnościach i wykonywanych zadaniach nałożonych obowiązkami prawnymi Ustawą KSC – tj. w zakresie dotyczącym:
      a) zarządzania incydentami oraz obsłudze incydentów;
         - wyszukiwaniu powiązań między incydentami,
         - usuwaniu przyczyn wystąpienia incydentów,
         - opracowywaniu wniosków wynikających z obsługi incydentu,
         - dokonaniu prawidłowej rejestracji zaistniałego incydentu;
      b) eliminacji podatności systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
      c) współdziałania wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo z właściwym CSIRT w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia;
   4) świadczenia pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT – w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia;
   5) świadczenia pomocy w przygotowaniu zgłoszenia informacji o innych incydentach, zagrożeniach cyberbezpieczeństwa, szacowaniu ryzyka, podatnościach lub wykorzystywanych technologiach – zgodnie z postanowieniem art. 13 ust. 1 Ustawy KSC – do właściwego CSIRT (lub sektorowego zespołu cyberbezpieczeństwa) w przypadku woli operatora usługi kluczowej dokonania takiego zgłoszenia;
   6) doradztwa w zakresie przekazanych operatorowi usługi kluczowej zaleceń pokontrolnych dotyczących usunięcia stwierdzonych nieprawidłowości, wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa oraz przygotowanie projektów informacji do organu właściwego do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń pokontrolnych;

7) przygotowania oszacowania ryzyka wystąpienia incydentu, rozumianego jako zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo świadczonej usługi kluczowej;
8) doradztwa w sprawach związanych z zarządzaniem oszacowanym ryzykiem;
9) pomocy w realizacji wynikającego z Ustawy KSC obowiązku operatora usługi kluczowej w zakresie zapewnienia osobom, na rzecz których usługa kluczowa jest realizowana, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, poprzez przygotowanie, a następnie - w przypadku zaistnienia prawnej konieczności - aktualizację, odpowiedniej informacji w postaci broszury dostosowanej do umieszczenia na stronie internetowej operatora usługi kluczowej;
10) sporządzania informacji w wymiarze nieprzekraczającym dwóch w miesiącu, w sprawach dotyczących prawnych zagadnień cyberbezpieczeństwa, w terminie 7 dni roboczych (rozumianych jako dni od poniedziałku do piątku) od daty wpłynięcia zapytania na adres poczty elektronicznej osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa – liczonych zgodnie z przepisami ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (t. j. Dz. U. z 2022 r., poz.1360 ze zm.; dalej, jako: **„Kodeks cywilny"**) ;
11) przeprowadzenia w trybie on-line szkolenia pracowników Zleceniodawcy z zakresu obowiązków operatorów usługi kluczowej wynikających z przepisów Ustawy KSC oraz dotyczącego zagadnień przestrzegania bezpieczeństwa informacji;
12) przeprowadzenia w trybie stacjonarnym w siedzibie Zleceniodawcy szkolenia kadry kierowniczej Zleceniodawcy z zakresu obowiązków operatora usługi kluczowej wynikających z przepisów Ustawy KSC, zagadnień przestrzegania bezpieczeństwa informacji i ochrony danych osobowych;
13) przeprowadzenia wymaganego przepisem art. 15 ust. 1 Ustawy KSC audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez wyspecjalizowana kadrę spełniającą wymogi Ustawy KSC oraz Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r., poz. 1999) tj. przynajmniej dwóch audytorów legitymujących się certyfikatem audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami Ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t. j. Dz. U. z 2022 r., poz.1854 ze zm.) w zakresie certyfikacji osób.
14) comiesięcznego wykonywania testów podatności infrastruktury teleinformatycznej z przygotowaniem raportu w języku polskim z opisem podatności oraz rekomendacjami dotyczącymi ich usunięcia.

2. Przeprowadzenie czynności, o których mowa w § 2 ust. 1 pkt 13) i 14) Umowy, wykonywanych z użyciem oprogramowania audytującego następuje po zalogowaniu się administratora systemu informatycznego („ASI") lub osoby wyznaczonej przez Zleceniodawcę na urządzenia brzegowe. Strony zgodnie postanawiają, że ASI lub osoba wyznaczona, o ile nie ma takiej konieczności, nie udostępnia haseł dostępu Zleceniobiorcy.

3. Zleceniobiorca oświadcza, iż dane gromadzone przez oprogramowanie audytujące, przesyłane są protokołem szyfrowanym na serwer należący do Zleceniobiorcy, celem uniemożliwienia ingerencji w nie osobom nieuprawnionym. Najpóźniej w terminie miesiąca po zakończeniu obowiązywania Umowy dane zgromadzone przez oprogramowanie audytujące zostaną trwale usunięte przez Zleceniobiorcę – Zleceniobiorca na wniosek Zleceniodawcy przekaże oświadczenie o usunięciu danych zgromadzonych przez oprogramowanie audytujące. W przypadku mogącego zaistnieć sporu w związku z realizacją Umowy, Zleceniobiorca jest uprawniony do przetwarzania tych danych (danych osobowych jak i danych nieosobowych) w okresie po zakończeniu obowiązywania niniejszej Umowy w celu ewentualnego wykonywania roszczeń z tytułu jej niewykonania lub niewłaściwego wykonania, albo obrony przed takimi roszczeniami.
4. Przypadkowe awarie, jakie mogą powstać w związku z analizą urządzeń podczas wykonywania czynności, o których mowa w § 2 ust. 1 pkt 13) i 14) Umowy oraz ewentualnym wykonywaniem innych czynności składających się realizację świadczenia Umowy, nie rodzą po stronie Zleceniobiorcy odpowiedzialności odszkodowawczej, o ile nie powstały z przyczyn leżących po stronie Zleceniobiorcy.

§ 3
Szczegółowy zakres świadczonej przez Zleceniobiorcę usługi – doradztwo w zakresie ochrony danych osobowych

1. W ramach części Umowy dotyczącej doradztwa w zakresie ochrony danych osobowych, Strony zgodnie postanawiają, iż obejmuje ona doradztwo wobec Inspektora Ochrony Danych powołanego przez Zleceniodawcę będącego administratorem danych osobowych, w rozumieniu art. 4 pkt 7 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 - t. j. Dz.U.UE.L.2016.119.1 (w dalszej części niniejszej Umowy zwanego **„RODO"**), a które to dane osobowe przetwarzane są ramach prowadzonej przez niego działalności.
Doradztwo obejmuje:

1) informowanie o obowiązkach spoczywających na Zleceniodawcy na mocy przepisów dotyczących ochrony danych osobowych (w szczególności RODO oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781 ze zm.), oraz doradztwo w tym zakresie,
2) monitorowanie przestrzegania przepisów wewnętrznych, polityk i procedur stosowanych przez Zleceniodawcę w zakresie ochrony danych osobowych,
3) podejmowanie działań zwiększających świadomość prawną Zleceniodawcy, jego pracowników i osób wykonujących pracę w oparciu o umowy cywilnoprawne wchodzących w skład kadry pracowniczej, w zakresie przetwarzania i ochrony danych osobowych,
4) przeprowadzanie w trybie on-line szkoleń pracowników i innych wskazanych przez Zleceniodawcę osób wchodzących w skład kadry pracowniczej i przetwarzających dane osobowe,

5) wykonywanie audytów dotyczących przestrzegania przepisów o ochronie danych osobowych,
6) wykonywanie analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych,
7) udzielanie Zleceniodawcy zaleceń co do oceny skutków dla ochrony danych oraz nadzorowanie realizacji zaleceń pokontrolnych,
8) pomoc w aktualizacji dokumentacji tj. rejestru czynności przetwarzania danych osobowych, rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Zleceniodawcy jako administratora danych osobowych oraz polityki ochrony danych osobowych – w przypadku zaistnienia zmiany przepisów prawa w w/w zakresie lub z wniosku Zleceniodawcy;
9) doradztwo w przypadku wystąpienia wymaganej na podstawie przepisów prawa współpracy z Prezesem Urzędu Ochrony Danych Osobowych będącym organem nadzorczym w sprawach z zakresu ochrony danych osobowych,
10) wsparcie Inspektora Ochrony Danych w pełnieniu przez niego funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych oraz w stosownych przypadkach w prowadzeniu konsultacji w sprawach dotyczących danych osobowych.

§ 4

Szczegółowy zakres świadczonej przez Zleceniobiorcę usługi – doradztwo informatyczne

1. Zleceniobiorca w ramach świadczonej usługi w zakresie doradztwa informatycznego, obejmującej przedmiot niniejszej Umowy, o którym mowa w §1 Umowy, zobowiązuje się do wykonywania następujących czynności:
   1) ścisłej współpracy z Inspektorem Ochrony Danych;
   2) doradztwa w określeniu zasad i procedur (we współpracy z działem obsługi informatycznej Zleceniodawcy) zapewniających bezpieczeństwo systemu informatycznego przetwarzającego dane osobowe;
   3) wsparcia i doradztwa działu obsługi informatycznej Zleceniodawcy w zakresie – adekwatnych do potrzeb i możliwości Zleceniodawcy – rozwiązań technologicznych dotyczących zabezpieczeń systemów informatycznych przetwarzających dane osobowe;
   4) wydawania zaleceń w ramach konsultacji dotyczących wyposażenia Zleceniodawcy w urządzenia do bezpiecznego przechowywania i zabezpieczenia danych osobowych poprzez opiniowanie przedstawionych przez Zleceniodawcę ofert wyposażenia sprzętowego;
   5) konsultacje działu informatycznego Zleceniodawcy w sprawach związanych z przetwarzaniem danych osobowych w systemie informatycznym.

§ 5

Rozpoczęcie realizacji poszczególnych czynności z Umowy

1. Strony zgodnie ustalają, iż **od dnia ..... r.** Wykonawca rozpocznie realizację i świadczyć będzie wyłącznie czynności, o których mowa w następujących przepisach:
   a) §2 ust. 1 pkt 1);
   b) §2 ust. 1 pkt 9);

c) §2 ust. 1 pkt 11);
d) §2 ust. 1 pkt 12);
e) §3 ust. 1 pkt 4);
f) §3 ust. 1 pkt 5);
g) §3 ust. 1 pkt 8).

2. Strony zgodnie ustalają, iż **od dnia ..... r.** Wykonawca rozpocznie realizację i świadczyć będzie również pozostałe czynności (tj. obok czynności, oznaczonych w ust. 1 powyżej), o których mowa w przepisach §2-§4 Umowy.

§ 6
Obowiązki i oświadczenia Zleceniobiorcy

1. Zleceniobiorca zobowiązuje się do wykonania Umowy z zachowaniem zasad należytej staranności, wynikających z zawodowego charakteru prowadzonej przez siebie działalności.
2. Zleceniobiorca zobowiązuje się, że w toku wykonywania czynności używał będzie programów, materiałów, narzędzi oraz informacji, do których posiada stosowne uprawnienie i które nie naruszają praw osób trzecich, w szczególności zaś nie naruszają przepisów Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. j. Dz. U. z 2022 r., poz. 2509 ze zm.).
3. Zleceniobiorca ponosi odpowiedzialność w zakresie winy za każde naruszenie praw osób trzecich w związku z wykonywaniem Umowy, w tym w szczególności – za ujawnienie informacji, jakie uzyskane zostały przez niego w trakcie realizacji Umowy.
4. Zleceniobiorca oświadcza, że dane gromadzone na jego serwerach zabezpieczone są zgodnie z wymogami międzynarodowej normy standaryzującej systemy zarządzania bezpieczeństwem informacji PN-EN ISO/IEC 27001:2017-06 oraz, że Zleceniobiorca posiada ważny, wydany przez jednostkę akredytowaną przez Polskie Centrum Akredytacji certyfikat w tym zakresie.

§ 7
Obowiązki i oświadczenia Zleceniodawcy

1. Zleceniodawca zobowiązuje się do zapewnienia Zleceniobiorcy dostępu do pomieszczeń, komputerów, urządzeń oraz do systemów informatycznych znajdujących się w siedzibie Zleceniodawcy niezbędnych do realizacji Umowy, jeśli taki dostęp będzie konieczny.
2. W przypadku potrzeby uzyskania przez Zleceniobiorcę informacji koniecznych do wykonania czynności tworzącej część usługi objętej Umową, Zleceniodawca zobowiązuje się do przekazywania niezwłocznie, osobiście lub za pośrednictwem wyznaczonego pracownika, w terminie nie dłuższym niż 5 dni roboczych, liczonym od dnia przedłożenia stosownego wniosku (przekazanego w formie pisemnej lub formie elektronicznej za pośrednictwem poczty e-mail lub formie ustnej – przy czym forma ta zostanie potwierdzona w formie pisemnej lub za pośrednictwem poczty e-mail) żądanych przez Zleceniobiorcę informacji niezbędnych do wykonania Umowy. Przekazanie żądanych informacji może nastąpić w dowolnej formie, nie wyłączając przesłania ich z wykorzystaniem poczty elektronicznej e-mail lub tradycyjnej, ustnie lub poprzez konsultacje telefoniczne. W przypadku przekazania przez Zleceniodawcę informacji, o których mowa w niniejszym ustępie w formie ustnej lub poprzez konsultację telefoniczną, forma ta zostanie następnie potwierdzona pisemnie bądź za pośrednictwem poczty e-mail. Postanowienie zdania pierwszego nie dotyczy sytuacji, w których przepisy prawa

wskazują konkretne, w tym krótsze, terminy wykonania ustawowych czynności przez Zleceniodawcę lub Zleceniobiorcę – wówczas Zleceniobiorca zobowiązuje się do przekazania informacji niezwłocznie, tj. w takim czasie i w taki sposób, by nie został naruszony termin wskazany przepisem powszechnie obowiązującego prawa.

3. W sytuacji powstania przeszkód w wykonaniu Umowy, leżących po stronie Zleceniodawcy, niezwłocznie poinformuje on Zleceniobiorcę o powyższym, w formie o której mowa w § 15 ust. 1 i ust. 2 Umowy. Okres czasowej przeszkody w wykonaniu Umowy powstały po stronie Zleceniodawcy powoduje przesunięcie ustalonych między Stronami terminów o ilość dni, w trakcie których Zleceniobiorca nie był w stanie – pozostając przy tym bez swojej winy – wykonywać Umowy lub czynności z niej wynikającej w związku z trwaniem tej przeszkody.
4. Przed przystąpieniem Zleceniobiorcy do realizacji czynności wskazanych w Umowie, gdy zaistnieje taka potrzeba – w tym, w szczególności w przypadku czynności, o których mowa w § 2 ust. 1 pkt 13) i 14) Umowy – Zleceniodawca zobowiązuje się do przygotowania kserokopii wszelkich wymaganych przez Zleceniobiorcę dokumentów i ich przekazania.
5. Zleceniodawca oświadcza, że wyraża zgodę na wykonanie audytów mogących obejmować testy i analizy podatności w związku z realizacją czynności, o których mowa w § 2 ust. 1 pkt 13) i 14) Umowy. Zleceniodawca oświadcza, iż został poinformowany i jest świadomy ryzyka związanego z przeprowadzeniem w/w testów i analiz podatności, polegających na niemożliwym do przewidzenia zakłóceniu pracy systemu teleinformatycznego Zleceniodawcy, mogącym skutkować m.in. czasowym ograniczeniu dostępu do sieci teleinformatycznej oraz wynikającymi z tego konsekwencjami. Przed, jak i w trakcie wykonywania wskazanych testów i analiz, Zleceniodawca zobowiązuje się do wyznaczenia osób z obsługi informatycznej w celu zarządzania i obsługi ewentualnych incydentów, związanych z ryzykiem, o których mowa w zdaniu poprzedzającym.
6. Zleceniodawca zobowiązany jest każdorazowo do wyznaczenia pracownika, który będzie obecny przy przeprowadzaniu przez Zleceniobiorcę czynności wymagających bezpośredniej realizacji w siedzibie Zleceniodawcy oraz osoby odpowiedzialnej za jego obsługę informatyczną (np. administratora systemu informatycznego) lub bezpieczeństwo informacji Zleceniodawcy.
7. Niezapewnienie przez Zleceniodawcę obecności wyznaczonego pracownika lub osoby odpowiedzialnej za jego obsługę informatyczną, lub bezpieczeństwo informacji Zleceniodawcy, lub administratora systemu informatycznego – o ile nie będzie to niezbędne do prawidłowej realizacji czynności wynikających z Umowy – nie wstrzymuje wykonywania przez Zleceniobiorcę umownych obowiązków, przy czym może skutkować zobowiązaniem Zleceniodawcy do świadczenia zwrotu uzasadnionych kosztów dojazdu pracowników Zleceniobiorcy do siedziby Zleceniodawcy w przypadku, w którym nieobecność w/w osób uniemożliwi wykonanie czynności określonych w Umowie.
8. Zleceniodawca wyraża zgodę na przetwarzanie przez Zleceniobiorcę danych nieosobowych zgromadzonych podczas wykonywanych czynności przy czym Zleceniobiorca zobowiązany jest do:
   a) przetwarzania w/w danych jedynie w zakresie i celu wykonania Umowy;
   b) zachowania ich w poufności, przy czym okres poufności rozciąga się tak na czas realizacji Umowy, jak i bezterminowo po jej ustaniu z jakiejkolwiek przyczyny (tj. po jej wygaśnięciu, wypowiedzeniu, odstąpieniu, rozwiązaniu, upływu okresu na jaki została zawarta etc.);

obowiązek, o którym mowa w zdaniu poprzedzającym, nie dotyczy danych jawnych, czy też stanowiących informację ogólnodostępną, w szczególności – informację publiczną;

c) na wniosek Zleceniodawcy – do informowania o zasadach przetwarzania przez Zleceniobiorcę danych;

d) podjęcia niezbędnych i adekwatnych środków technicznych i organizacyjnych w celu ochrony w/w danych oraz bezpieczeństwa ich przetwarzania.

§ 8
Oświadczenia dotyczące monitorowania

1. Mając na uwadze, iż część wykonywanej przez Zleceniobiorcę usługi – w tym czynności, o których mowa w § 2 ust. 1 pkt 13) i 14) Umowy – lub innych czynności obejmujących audyt może zostać przeprowadzona z wykorzystaniem monitoringu pracowniczego, o którym mowa w art. 22^3 Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 2022 r., poz. 1510 ze zm.), Zleceniodawca zobowiązuje się do odebrania od wszystkich osób zatrudnionych w jego jednostce, niezależnie od podstawy takiego zatrudnienia (umowy o pracę, umowy cywilnoprawnej, stażu, praktyki itp.) – co do zasady będących użytkownikami stacji roboczych znajdujących się w sieci komputerowej Zleceniodawcy – pisemnego oświadczenia o poinformowaniu o fakcie dokonywania monitorowania wykorzystania sprzętu i legalności oprogramowania znajdującego się na tym sprzęcie.
2. W związku z postanowieniem ust. 1 powyżej, Zleceniodawca zobowiązuje się do przedłożenia Zleceniobiorcy pisemnego oświadczenia o poinformowaniu użytkowników stacji roboczych znajdujących się w sieci komputerowej Zleceniodawcy o fakcie dokonywania monitorowania wykorzystania sprzętu i legalności oprogramowania znajdującego się na tym sprzęcie. Przedłożenie Zleceniobiorcy pisemnego oświadczenia powinno nastąpić każdorazowo przed wykonaniem czynności z wykorzystaniem monitoringu pracowniczego. Wzór oświadczenia, o którym mowa w zdaniu poprzednim stanowi Załącznik nr 2 do Umowy.
3. W przypadku nieprzedłożenia przez Zleceniodawcę oświadczenia, o którym mowa w ust. 2, Zleceniobiorca nie będzie uprawniony do wykonania czynności z uwzględnieniem wykorzystania monitoringu pracowniczego lub po uzyskaniu od Zleceniodawcy polecenia sporządzonego w formie pisemnej pod rygorem nieważności, Zleceniobiorca wykona w/w czynności z wykluczeniem m.in. danych dotyczących inwentaryzacji sprzętu i oprogramowania oraz aktywności użytkowników stacji roboczych.
4. Zleceniodawca przyjmuje do wiadomości, że odebranie oświadczenia, o którym mowa w ust. 2, stanowi podstawę legalności przeprowadzenia monitorowania wykorzystania sprzętu i legalności oprogramowania znajdującego się na stacjach roboczych sieci komputerowej Zleceniodawcy oraz wygenerowania w tym zakresie raportów poaudytowych.
5. W przypadku niewykonania przez Zleceniodawcę obowiązku poinformowania użytkowników stacji roboczych znajdujących się w sieci komputerowej Zleceniodawcy i wprowadzenia w tym zakresie Zleceniobiorcy w błąd przedkładając mu nieprawdziwe oświadczenie, o którym mowa w ust. 2, Zleceniodawca ponosi wyłączną odpowiedzialność w pełnej wysokości za ewentualną szkodę, jaką z tego tytułu może ponieść Zleceniobiorca, przy czym Zleceniobiorcy przysługiwać będzie w takim wypadku uprawnienie do rozwiązania niniejszej Umowy ze skutkiem natychmiastowym (bez wypowiedzenia).

6. Zleceniodawca oświadcza, że w celu umożliwienia prawidłowego wykonania Umowy w zakresie uprzednio każdorazowo ustalanych między Stronami czynności wymaganych przez Zleceniodawcę lub koniecznych do przeprowadzania w związku ze świadczoną usługą – wyraża zgodę na instalację oprogramowania audytującego posiadającego funkcje monitorujące, którym dysponuje Zleceniobiorca. W przypadku wycofania przez Zleceniodawcę zgody, o której mowa w zdaniu poprzedzającym, Zleceniobiorca wykona w/w czynności, z wykluczeniem danych dotyczących inwentaryzacji sprzętu i oprogramowania oraz aktywności użytkowników stacji roboczych. Pomimo wyrażonej zgody na instalację oprogramowania monitorującego, wykluczenie danych, o których mowa powyżej może nastąpić również w przypadku zdarzenia losowego jakim jest niekompatybilność w/w oprogramowania audytującego posiadającego funkcje monitorujące z systemem teleinformatycznym Zleceniodawcy, skutkiem czego system ten może nie działać prawidłowo w zakresie dziedzinowych rozwiązań działających w technologii Web. Mając powyższe na uwadze, zespół audytorski Zleceniobiorcy we współpracy z obsługą informatyczną Zleceniodawcy, na żądanie Zleceniodawcy wyrażone pod rygorem nieważności w formie pisemnej lub formie elektronicznej za pośrednictwem poczty e-mail, może wykonać próbę instalacyjną na jego systemie teleinformatycznym, przy czym na podstawie wykonanej próby obie Strony podejmą decyzję czy podczas jej trwania działanie zainstalowanego oprogramowania nie wpływa w sposób powodujący zakłócenia na działanie infrastruktury systemu teleinformatycznego i aplikacji dziedzinowych.
7. W dniu rozpoczęcia wykonywania czynności ustalonych pomiędzy Stronami, Zleceniobiorca na żądanie Zleceniodawcy wyrażone pod rygorem nieważności w formie pisemnej lub formie elektronicznej za pośrednictwem poczty e-mail,, przekaże wersje instalacyjną oprogramowania monitorującego do zainstalowania przez Zleceniodawcę. Instalacja powinna zostać dokonana po spełnieniu obowiązków, o których mowa w ust. 1 i ust. 2 niniejszego paragrafu.
8. Oprogramowanie audytujące posiadające funkcje monitorujące zostanie odinstalowane bez zbędnej zwłoki w sposób zdalny przez Zleceniobiorcę po wykonaniu czynności, do których przeprowadzania zostało zainstalowane lub w innym terminie zgodnie przez Strony ustalonym. W przypadku problemów z odinstalowaniem oprogramowania Zleceniobiorca ustali ze Zleceniodawcą termin i sposób usunięcia oprogramowania. Kompletność odinstalowania powinna być zweryfikowana przez Zleceniodawcę, po przekazaniu mu kluczy dezinstalacyjnych przez Zleceniobiorcę.
9. W przypadku problemów z odinstalowaniem oprogramowania, o którym mowa w ust. 8, Zleceniobiorca będzie uprawniony do przetwarzania danych, w tym danych osobowych, gromadzonych przez oprogramowanie ze stacji roboczych Zleceniodawcy przez czas do dnia jego skutecznego odinstalowania.

§ 9
Upoważnienie

1. W celu prawidłowego wykonywania obowiązków, na podstawie niniejszej Umowy, Zleceniodawca udziela Zleceniobiorcy upoważnienia do osobistego lub poprzez jego pracowników (w tym osoby zatrudnione na podstawie umów cywilnoprawnych) przeprowadzenia czynności realizujących świadczoną usługę, w tym udziela również upoważnienia swoim zakresem obejmującego: uprawnienie do przetwarzania danych osobowych i nieosobowych przetwarzanych przez Zleceniodawcę, oraz – w obecności lub za

wiedzą Zleceniodawcy – uprawnienie do wstępu do pomieszczeń siedziby Zleceniodawcy, uprawnienie do dostępu do urządzeń, komputerów oraz systemów informatycznych znajdujących się w siedzibie Zleceniodawcy oraz wykonywania wszelkich innych niezbędnych czynności faktycznych w celu realizacji obowiązków umownych.

2. Zleceniobiorca lub w jego imieniu – pełnomocnik, Dyrektor Operacyjny lub Dyrektor Handlowy firmy „Centrum Bezpieczeństwa Informatycznego", zobowiązuje się do udzielenia na piśmie audytującemu pracownikowi (lub pracownikom) upoważnienia do przeprowadzenia czynności z zakresu świadczonej Umowy. Upoważnienie jest ważne przez cały okres trwania Umowy, chyba że Zleceniobiorca cofnie upoważnienie, o czym niezwłocznie powiadomi Zleceniodawcę.

§ 10
Przetwarzanie danych osobowych

1. Na podstawie art. 28 RODO Zleceniodawca, zwany dalej na potrzeby regulacji dotyczącej powierzenia przetwarzania danych osobowych również **„Administratorem"**, powierza Zleceniobiorcy, zwanemu w dalszej części niniejszego paragrafu **„Procesorem"** dane osobowe do przetwarzania, na zasadach określonych w niniejszej Umowie oraz w celu i zakresie niezbędnym do realizacji jej przedmiotu.
2. Przetwarzanie przez Procesora powierzonych danych osobowych będzie obejmowało czynności na danych osobowych takie jak: pobieranie, utrwalanie, przeglądanie, wykorzystywanie, dopasowywanie lub łączenie w związku z charakterem poszczególnych czynności tworzących usługę, a także przechowywanie nie będące tworzeniem kopii zapasowych danych przynależnych Zleceniodawcy. Przetwarzanie następować będzie w sposób ciągły w formie elektronicznej lub papierowej
3. Przetwarzanie dotyczyć będzie:
   Kategoria osób, których dane będą przetwarzane: osoby zatrudnione w zakładzie pracy Zleceniodawcy niezależnie od podstawy takiego zatrudnienia, pacjenci i usługobiorcy Zleceniodawcy.
   Rodzaj danych, które będą przetwarzane: imię, nazwisko, numery PESEL, adres zamieszkania lub adres do korespondencji, a także inne dane osobowe zwykłe znajdujące się w systemach informatycznych Zleceniodawcy oraz dane osobowe szczególnych kategorii ujawniające dane medyczne dotyczące zdrowia.
4. Czas trwania przetwarzania powierzonych Procesorowi danych osobowych będzie zgodny z czasem obowiązywania Umowy.
5. Procesor zobowiązany jest do przetwarzania danych osobowych wyłącznie w celach związanych z wykonywaniem niniejszej Umowy oraz uprawniony jest do przetwarzania danych osobowych wyłącznie w takim zakresie, w jakim zostało mu to powierzone przez Zleceniodawcę.
6. Procesor nie ma prawa do wykorzystania zgromadzonych na podstawie niniejszej Umowy danych osobowych w jakimkolwiek celu po jej rozwiązaniu, niezależnie od podstawy takiego rozwiązania, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
7. Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, przez które Strony rozumieją niniejsza Umowę lub indywidualne polecenia i instrukcje

przekazywane przez Zleceniodawcę w sposób, o którym mowa w § 15 ust. 1 i ust. 2 Umowy lub ustnie oraz:

a) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
b) podejmuje odpowiednie środki techniczne oraz organizacyjne, mające na celu zapewnienia bezpieczeństwa danych osobowych zgodnie z art. 32 RODO;
c) nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody Administratora;
d) w miarę możliwości pomaga Administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 12-23 RODO;
e) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO;
f) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, w tym również te, zawarte na nośnikach danych i potwierdza powyższe przekazaniem Administratorowi protokołu, którego wzór określa Załącznik nr 3, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
g) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia Administratorowi (lub upoważnionemu przez niego audytorowi) przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich,
h) zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Procesora danych osobowych, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Procesora, a także o wszelkich planowanych - o ile są mu wiadome - lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania przez tego Procesora danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Ochrony Danych Osobowych.

8. Jeżeli powierzone dane osobowe są przetwarzane w formie elektronicznej na serwerach i nośnikach danych Procesora, te serwery i nośniki nie mogą znajdować się poza obszarem Unii Europejskiej i Europejskiego Obszaru Gospodarczego.
9. Procesor zobowiązuje się do każdorazowego i niezwłocznego informowania Administratora o przypadkach naruszenia przepisów prawa dotyczących ochrony powierzonych danych osobowych, w tym w szczególności przepisów RODO, zaistniałych w okresie obowiązywania niniejszej Umowy. Procesor współdziała z Administratorem przy ustalaniu szczegółów związanych ze zgłoszonym mu naruszeniem, w szczególności przyczyn i skutków jego wystąpienia oraz wdraża zalecane przez Administratora środki, mające na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia danych osobowych oraz środki naprawcze.

10. W przypadku stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 RODO, Procesor zgłasza je Administratorowi bez zbędnej zwłoki. Zgłoszenie naruszenia ochrony danych osobowych Administratorowi powinno obejmować co najmniej:
    a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane osobowe dotyczą, oraz kategorie i przybliżoną liczbę wpisów, których dotyczy naruszenie;
    b) możliwe konsekwencje naruszenia ochrony danych osobowych;
    c) środki zastosowane lub proponowane przez Procesora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
11. Na wypadek zawinionego naruszenia przez Procesora zasad przetwarzania danych osobowych (określonych w przepisach powszechnie obowiązującego prawa, RODO oraz niniejszej Umowy), skutkującego zobowiązaniem Administratora na mocy prawomocnego orzeczenia sądu, ugody sądowej bądź porozumienia mediacyjnego do wypłaty odszkodowania, zadośćuczynienia lub kary pieniężnej, Procesor zobowiązuje się zrekompensować Administratorowi udokumentowane straty z tego tytułu w pełnej wysokości. Zobowiązanie Procesora, o którym mowa powyżej, powstanie pod warunkiem pisemnego powiadomienia go o każdym przypadku wystąpienia przez osoby trzecie z roszczeniem wobec Administratora z podaniem podstaw prawnych i faktycznych, w terminie 7 dni od daty dowiedzenia się Administratora o takim roszczeniu.
12. Procesor ponosi odpowiedzialność za wszelkie działania i zaniechania osób przez niego upoważnionych do przetwarzania danych osobowych oraz za takie działania i zaniechania innego podmiotu przetwarzającego, któremu powierzył przetwarzanie danych Administratora.
13. Procesor jest zwolniony z odpowiedzialności za szkody spowodowane przetwarzaniem przez niego danych osobowych jak i nieosobowych naruszającym przepisy prawa, jeżeli wykaże, że nie można mu przypisać winy za zdarzenie, które doprowadziło do powstania szkody.
14. Procesor zapewnia, że dane osobowe nie będą udostępniane jego pracownikom i zleceniobiorcom przed podpisaniem przez nich oświadczeń lub umów o zachowaniu poufności. Zachowanie poufności nie ustaje po rozwiązaniu lub wygaśnięciu stosunku pracy lub umowy cywilnoprawnej, niezależnie od przyczyny tego rozwiązania lub wygaśnięcia.
15. Procesor zobowiązuje się do monitorowania i stosowania przepisów prawa, powszechnie dostępnych wskazówek i zaleceń organu nadzorczego oraz unijnych organów doradczych, zajmujących się ochroną danych osobowych, w zakresie przetwarzania powierzonych mu danych osobowych, po uprzednim uzgodnieniu wpływu tych regulacji na przetwarzanie danych z Administratorem.
16. Administrator przez cały okres obowiązywania Umowy jest uprawniony do kontroli poprawności zabezpieczenia i przetwarzania danych powierzonych Procesorowi. Kontrola może zostać przeprowadzona m.in. w formie bezpośredniej inspekcji polegającej na dopuszczeniu przedstawicieli Administratora do wszystkich obszarów przetwarzania danych osobowych objętych niniejszą Umową we wszystkich lokalizacjach Procesora, w sposób nieutrudniający nadmiernie jego bieżącej działalności. Procesor zobowiązany jest do niezwłocznego przedstawienia odpowiednich dokumentów do kontroli oraz wyjaśnień na piśmie na każde wezwanie Administratora.

17. Administrator realizować będzie prawo kontroli z minimum siedmiodniowym (7 dni kalendarzowych) jego uprzedzeniem dokonanym w sposób, o którym mowa w § 15 ust. 1 i ust. 2 Umowy, w godzinach pracy Procesora. W przypadku powzięcia przez Administratora uzasadnionego podejrzenia naruszenia ochrony danych osobowych przez Procesora, Administrator uprawniony jest do przeprowadzenia kontroli w jednostce Procesora w sposób natychmiastowy bez zachowania terminów, o których mowa w zdaniu poprzednim, lecz po uprzednim poinformowaniu o takowym zamiarze.
18. W przypadku, gdy kontrola, o której mowa w ust. 16 i ust. 17, wykaże jakiekolwiek nieprawidłowości Administrator ma prawo żądać od Procesora niezwłocznego wdrożenia zaleceń Administratora wynikających z ustaleń pokontrolnych. Zalecenia te przedstawiane będą w formie pisemnej lub elektronicznej.
19. Zgodnie z przepisem ust. 7 pkt c) niniejszego paragrafu Procesor może na podstawie niniejszej Umowy powierzać przetwarzanie powierzonych mu danych osobowych objętych Umową innym podmiotom (w szczególności osobom prowadzącym jednoosobowe działalności gospodarcze wykonującym pracę w oparciu o umowy cywilnoprawne) stałe współpracującym z Procesorem (tzw. podpowierzenie). Podpowierzenie podmiotom innym niż te, o których mowa w zdaniu poprzednim może nastąpić wyłącznie po uprzedniej pisemnej zgodzie Administratora.
20. Podpowierzając przetwarzanie danych osobowych innym podmiotom, Procesor jest obowiązany zapewnić w dalszej umowie powierzenia spełnienie przez ten podmiot wszelkich wymogów w zakresie ochrony danych osobowych na poziomie, co najmniej takim samym jak przewidziany w niniejszej Umowie.
21. Procesor zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych, informacji i materiałów przekazanych lub udostępnionych mu lub o których wiedzę powziął w związku z realizacją Umowy, a także powstałych w wyniku jej wykonania informacji i materiałów w formie pisemnej, graficznej lub jakiejkolwiek innej formie. Informacje i materiały są objęte tajemnicą i nie mogą być bez uprzedniej pisemnej zgody Administratora udostępniane jakiejkolwiek osobie trzeciej, ani też ujawnione w inny sposób, chyba że w dniu ich ujawnienia były powszechnie znane albo muszą być ujawnione zgodnie z powszechnie obowiązującymi przepisami prawa, orzeczeniem sądu lub organu państwowego.
22. Strony ustalają, że podczas realizacji Umowy, będą ze sobą ściśle współpracować, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie powierzenia danych osobowych.
23. Strony zobowiązują się, że wszelkie decyzje dotyczące pozasądowego zakończenia sporu z osobą fizyczną na skutek naruszenia ochrony jej danych osobowych, w szczególności fakt i wysokość wypłaty ewentualnego odszkodowania, podejmą wspólnie.
24. Administrator ma prawo wypowiedzieć Umowę w trybie natychmiastowym (bez okresu wypowiedzenia), w przypadku rażącego naruszenia postanowień Umowy w zakresie ochrony danych osobowych przez Procesora, który:
    a) wykorzystał dane osobowe w sposób niezgodny z Umową, w szczególności przetwarzał je dla własnych celów lub celów innych podmiotów, a także celów niezgodnych z powszechnie obowiązującymi przepisami prawa lub postanowieniami niniejszej Umowy;
    b) wykonuje Umowę niezgodnie z obowiązującymi w tym zakresie przepisami prawa lub instrukcjami Administratora w tym zakresie;

c) nie zaprzestał niewłaściwego przetwarzania danych osobowych mimo uprzedniego wezwania Administratora do usunięcia naruszeń i bezskutecznego upływu wyznaczonego terminu 14 dni na zaniechanie naruszeń.

§ 11
Licencja w zakresie wykorzystania raportu z audytu

1. Zleceniobiorca udziela Zleceniodawcy nieodpłatnej licencji na czas oznaczony 20 lat na korzystanie z egzemplarzy wszelkich raportów, które zostaną ewentualnie wykonane z przeprowadzonych czynności usługi, w tym audytów, na następujących polach eksploatacji, tj. w zakresie:
   a) utrwalania i zwielokrotniania na wszelkich nośnikach w celu wewnętrznego wykorzystania przez Zleceniodawcę;
   b) wprowadzenia do pamięci komputera i sieci multimedialnych, w szczególności takich jak Internet, w celu realizacji zadań ustawowych Zleceniodawcy, jak również w celach dydaktycznych, edukacyjnych lub szkoleniowych i jedynie na wewnętrzny jego użytek;
   c) wykorzystania raportów w celach ustawowych, a także wszelkich czynności, do których raporty mogą stać się wymagane w ramach przepisów prawa, w tym przekazywania ich wszelkim podmiotom uprawnionym na mocy tych przepisów.

§ 12
Wynagrodzenie

1. Z tytułu realizacji niniejszej Umowy Zleceniobiorcy przysługiwać będzie wynagrodzenie ujęte w sposób następujący (zwane dalej **„Wynagrodzeniem"**):
   1) w okresie ..... **r.**, za realizację czynności, o których mowa w § 5 ust 1 Umowy – **ryczałtowe wynagrodzenie miesięczne, płatne z dołu za każdy miesiąc obowiązywania Umowy, w wysokości ..... zł netto** (słownie: dwa tysiące złotych netto) plus należny podatek VAT wedle stawki obowiązującej w danym miesiącu;
   2) w okresie ..... **r.**, za realizację czynności, o których mowa w § 5 ust. 2 Umowy – **ryczałtowe wynagrodzenie miesięczne, płatne z dołu za każdy miesiąc obowiązywania Umowy, w wysokości..... zł netto** (słownie: pięć tysięcy pięćset złotych netto) plus należny podatek VAT wedle stawki obowiązującej w danym miesiącu;
2. W przypadku, gdy usługa będzie wykonywana przez okres niepełnego miesiąca – w tym w przypadku ziszczenia się przesłanki, o której mowa w § 10 ust. 24 – wynagrodzenie za ten miesiąc będzie należne w wysokości proporcjonalnej do ilości dni kalendarzowych, przez które obowiązywała Umowa w danym okresie rozliczeniowym.
3. Wynagrodzenie będzie płatne w terminie 14 dni od daty dostarczenia Zleceniodawcy prawidłowo wystawionej faktury VAT, przelewem na rachunek Zleceniobiorcy podany na fakturze. W przypadku opóźnienia w zapłacie Wynagrodzenia Zleceniobiorcy przysługuje uprawnienie naliczania Zleceniodawcy odsetek ustawowych za opóźnienie. Faktura VAT wystawiona zostanie najpóźniej do 7-go dnia każdego miesiąca obowiązywania Umowy. Faktura VAT w przypadku pierwszego niepełnego miesiąca winna zostać uregulowana przez Zleceniodawcę w terminie w jej treści wskazanym.

4. W przypadku wystawienia przez którąkolwiek ze Stron dokumentów korygujących do faktury VAT, termin o którym mowa w ust. 4 liczony będzie od daty wpływu ostatniego dokumentu korygującego.
5. Za datę spełnienia świadczenia pieniężnego uznaje się dzień wpływu Wynagrodzenia na rachunek bankowy Zleceniobiorcy.
6. Zleceniodawca oświadcza, że wyraża zgodę na przesłanie drogą elektroniczną faktur, faktur korygujących, jak również duplikatów tych faktur wystawionych przez Zleceniobiorcę zgodnie z powszechnie obowiązującymi przepisami, w formacie PDF, na adres e-mail: **faktury_dfp@szpitalpulawy.pl**
7. Zleceniobiorca oświadcza, że faktury, faktury korygujące, jak również duplikaty tych faktur będą przesyłane z adresu e-mail: .....
8. Strony oświadczają, iż zmiana adresów e-mail określonych w ust. 6 i 7 nie stanowi zmiany Umowy i nie wymaga zgody drugiej Strony. O zmianie adresów e-mail określonych w w/w przepisach Strony będą sobie przekazywać informacje niezwłocznie w formie pisemnej lub elektronicznej oraz potwierdzenia telefonicznego.
9. Faktury VAT, faktury korygujące, jak również duplikaty tych faktur Strony uznają za skutecznie doręczone z dniem ich wysłania przez Zleceniobiorcę na adres e-mail określony w ust. 6 niniejszego paragrafu.
10. Zleceniobiorca oświadcza, że jest czynnym podatnikiem VAT oraz potwierdza, że nazwa firmy, adres prowadzenia działalności, NIP oraz nr rachunku bankowego podany na fakturze są zgodne z wykazem podatników VAT prowadzonym przez Szefa Krajowej Administracji Skarbowej.
11. Faktury VAT, na których będzie figurował rachunek bankowy spoza „Białej listy", będą traktowane, jako faktury nieprawidłowe, niepodlegające zapłacie do czasu dokonania stosownych korekt. W przypadku, gdy pomiędzy wystawieniem faktury VAT, a terminem płatności Zleceniobiorca dokona zmiany rachunku bankowego w „Białej liście" i na dzień zapłaty nie dokona on stosownej korekty, taka faktura VAT również będzie uznana za nieprawidłową, co skutkować będzie wstrzymaniem płatności. Żaden z powyższych przypadków nie stanowi opóźnienia uprawniającego Zleceniobiorcę do odsetek ustawowych za opóźnienie lub jakichkolwiek innych.
12. Jeżeli w momencie zapłaty przez Zleceniodawcę numer rachunku bankowego wskazany przez Zleceniobiorcę, podwykonawcę lub dalszego podwykonawcę w fakturze VAT nie jest numerem rachunku bankowego Zleceniodawcy wskazanym w "Białej liście" podatników VAT, Zleceniodawca wstrzyma się z płatnością na rzecz Zleceniobiorcy, bez konsekwencji wynikających z niewykonania zobowiązania lub opóźnienia w zapłacie, do momentu, w którym numer rachunku bankowego wskazany w fakturze VAT i tzw. „Białej liście" podatników VAT będą zgodne.
13. W tym miejscu Strony określają dane potrzebne do wystawienia faktury VAT:
    NABYWCA: Samodzielny Publiczny Zakład Opieki Zdrowotnej w Puławach, z siedzibą przy ul. Bema 1, 24-100 Puławy, KRS: 0000026256, REGON: 431205731, NIP: 7162238942;
    ODBIORCA: Samodzielny Publiczny Zakład Opieki Zdrowotnej w Puławach, z siedzibą przy ul. Bema 1, 24-100 Puławy, KRS: 0000026256, REGON: 431205731, NIP: 7162238942;

§ 13
Okres obowiązywania Umowy oraz możliwość jej wypowiedzenia

1. Okres świadczenia usług wynikających z Umowy strony ustalają jako termin od dnia…….. **2024 r.**
2. Każdej ze Stron przysługuje uprawnienie do wypowiedzenia niniejszej Umowy z zachowaniem trzymiesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca. Strony zastrzegają, iż wypowiedzenie Umowy winno przyjąć formę pisemną przesłaną pod adres siedziby drugiej ze Stron wskazany w komparycji Umowy lub formę elektroniczną (o której mowa w art. 78^1 § 1 Kodeksu cywilnego) zgodnie z § 15 ust. 2 Umowy, zastrzegając przy tym obydwie formy pod rygorem nieważności.

§ 14
Kary umowne

1. Zleceniobiorca zapłaci Zleceniodawcy karę umowną za każdy przypadek niewykonania lub nienależytego wykonania usługi w wysokości 10% wartości brutto usługi niewykonanej/nienależycie wykonanej.
2. Zleceniobiorca zapłaci Zleceniodawcy karę umowną w przypadku odstąpienia od umowy/jej rozwiązania przez Zleceniobiorcę lub Zleceniodawcę z przyczyn leżących po stronie Zleceniobiorcy w wysokości 10% wartości umowy brutto.
3. Kary umowne płatne będą w terminie 7 dni od dnia wezwania do ich zapłaty. Zleceniodawcy przysługuje prawo potrącania kar umownych z należnościami Zleceniobiorcy. Zleceniodawca ma prawo dochodzenia odszkodowania uzupełniającego w przypadku, gdy kara umowna nie pokryje szkody Zleceniodawcy.
4. Zleceniodawcy przysługuje prawo do rozwiązania umowy ze skutkiem natychmiastowym w razie niewykonania lub nienależytego wykonania umowy przez Zleceniobiorcę.
5. Poza przypadkiem określonym w ust. 4 powyżej Zleceniodawcy przysługuje prawo odstąpienia od umowy w razie wystąpienia istotnej zmiany okoliczności, powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy; odstąpienie od umowy w tym przypadku może nastąpić w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim przypadku Zleceniobiorca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.
6. Rozwiązanie i odstąpienie od umowy nastąpi w formie pisemnej pod rygorem nieważności.

§ 15
Siła wyższa

1. W czasie trwania siły wyższej, Strony Umowy zwolnione będą od wszelkiej odpowiedzialności za jej niewykonanie lub nienależyte wykonanie, jeżeli tylko okoliczności zaistnienia siły wyższej będą stanowiły przeszkodę w wykonaniu Umowy. Postanowienie ze zdania poprzedzającego będzie miało zastosowanie również w okresie bezpośrednio poprzedzającym lub bezpośrednio następującym po wystąpieniu siły wyższej, jeżeli tylko we wskazanym okresie dalsze oddziaływanie siły wyższej będzie stanowiło przeszkodę w wykonaniu Umowy.

2. Przez „siłę wyższą", o której mowa w ust. 1, należy rozumieć zdarzenie o charakterze przypadkowym lub naturalnym, całkowicie niezależne od woli i działania Zleceniobiorcy lub Zleceniodawcy, którego nie można było przewidzieć i niemożliwe było jego zapobieżenie, w szczególności takie zdarzenia jak: powódź, włamanie, długotrwały zanik energii elektrycznej wywołany awarią dostawcy energii, zaprzestanie funkcjonowania sieci Internet, wojna, akt terroru, wprowadzenie stanu wyjątkowego, stany pandemii lub epidemii w zakresie uniemożliwiającym przemieszczanie się, o ile taka konieczność do wykonania Umowy byłaby niezbędna, a także inne zdarzenia które obiektywnie mogą zakłócić (uniemożliwić lub znacznie utrudnić) realizację czynności wynikających z Umowy.
3. Strona Umowy uprawniona będzie do powoływania się na siłę wyższą jednie w sytuacji, w której niezwłocznie poinformuje o powyższym drugą Stronę, w sytuacji w której posiądzie przekonanie, że zdarzenie to uniemożliwia lub znacznie utrudnia wykonanie Umowy.

§ 16
Postanowienia końcowe

1. Strony zgodnie ustalają, że formą kontaktu wiążącą przy realizacji Umowy, jest kontakt w formie pisemnej tj. kontakt listowny (na adresy korespondencyjne podane w komparycji Umowy), bądź kontakt za pośrednictwem poczty elektronicznej e-mail, wskazane w ustępach poniżej – chyba że inaczej zastrzeżono w poszczególnych postanowieniach Umowy.
2. Wymiana informacji, wzajemne powiadomienia, przesyłanie dokumentacji, zgłoszenia naruszeń, a także wszelkie inne ustalenia lub zgłoszenia, które winny odbywać się w trakcie obowiązywania Umowy, dokonywać się będą pomiędzy Stronami poprzez osoby upoważnione do kontaktu w celu jej realizacji, o których mowa w ust. 3 i ust. 4 poniżej. Postanowienie uregulowane w zdaniu poprzednim nie dotyczy przypadków, w których w Umowie wprost wskazano inne dane kontaktowe lub inne osoby do kontaktu w konkretnych przypadkach w niej określonych.
3. Osoby upoważnione do kontaktu ze strony **Zleceniodawcy**:
   a) .....
   b) .....
4. Osoby upoważnione do kontaktu ze strony **Zleceniobiorcy**:
   a) .....
   b) .....
5. W przypadku stwierdzenia przez Zleceniodawcę nienależytego wykonania Umowy, wyznaczy on Zleceniobiorcy termin na ich usunięcie, jednakże termin ten nie może być krótszy niż 14 dni kalendarzowych, liczonych od potwierdzenia przez Zleceniobiorcę uzyskania informacji od Zleceniodawcy o wadzie lub usterce przekazanych w formie, o której mowa w ust. 1 lub ust. 2 pod rygorem nieważności. Potwierdzenia przez Zleceniobiorcę uzyskania informacji od Zleceniodawcy winno nastąpić niezwłocznie.
6. Niniejsza Umowa nie stanowi umowy zawartej z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa, o której mowa przepisach Ustawy KSC.
7. Każdorazowo, gdy Umowa stanowi o Zleceniodawcy, Strony zgodnie postanawiają, iż w zależności od kontekstu rozumieją przez to również pracowników lub inne osoby pozostające w strukturze Zleceniodawcy odpowiedzialne za poszczególne elementy świadczenia

usług Zleceniodawcy oraz innych zadań i obowiązków zleconych im w ramach obowiązków pracowniczych lub umów cywilnoprawnych, pozostających w zakresie przedmiotowym i ścisłym związku z usługą ujętą w treści Umowy, oddelegowane przez Zleceniodawcę do celu, którego dotyczy stosowny przepis lub czynność stanowiąca przedmiot Umowy.

8. Nieważność lub bezskuteczność któregokolwiek z postanowień Umowy nie powoduje nieważności lub bezskuteczności pozostałych postanowień Umowy. W takim przypadku Strony są zobowiązane przystąpić do negocjacji w dobrej wierze w celu zastąpienia takiego nieważnego lub bezskutecznego postanowienia ważnym i skutecznym postanowieniem najbardziej zbliżonym do pierwotnego zgodnego zamiaru Stron w tym zakresie.
9. Zmiana postanowień Umowy wymaga formy pisemnej pod rygorem nieważności.
10. Wszelkie załączniki do Umowy stanowią jej integralną część.
11. W kwestiach nieuregulowanych mają zastosowanie przepisy z Kodeksu cywilnego.
12. Strony ustalają, że sądem właściwym do rozstrzygania sporów mogących w przyszłości powstać na tle Umowy będzie sąd miejscowo właściwy dla siedziby Zleceniodawcy.
13. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

(Zleceniodawca)	(Zleceniobiorca)

Załączniki:

1) Wydruk z Centralnej Informacji Krajowego Rejestru Sądowego dot. Zleceniodawcy z dnia 01.06.2023 r.
2) Oświadczenie Zleceniodawcy o poinformowaniu wszystkich użytkowników stacji roboczych znajdujących się w sieci komputerowej o zainstalowaniu oprogramowania monitorującego;
3) Protokół usunięcia/zwrotu danych osobowych powierzonych do przetwarzania na podstawie Umowy.

Załącznik nr 2 do umowy

Oświadczenie Zleceniodawcy
o poinformowaniu wszystkich użytkowników stacji roboczych znajdujących się w sieci komputerowej o zainstalowaniu oprogramowania monitorującego

Oświadczam, iż poinformowano wszystkich użytkowników stacji roboczych znajdujących się w sieci komputerowej Zleceniodawcy o zamiarze zainstalowania oprogramowania monitorującego w zakresie ilościowego i jakościowego wykorzystania sprzętu pracowniczego i legalności oprogramowania, w związku z czym Zleceniodawca uprawnia Zleceniobiorcę do realizacji czynności monitorowania koniecznego do wykonania części Umowy CBI/……/2024/……., z dnia ……

……
(data i podpis Zleceniodawcy)

Dział Zamówień Publicznych
Justyna Gawęda
Tel: 81 450 23 89
zp@szpitalpulawy.pl

NIP 7162238942
REGON: 431205731
KRS: 0000026256
BDO: 000041779
ePUAP:/SPZOZPULAWY/SkrytkaESP

spzoz@szpitalpulawy.pl
www. szpitalpulawy.pl,
Nr księgi Rejestrowej: 000000002932
Bank Millennium SA - 12 1160 2202 0000 0000 6018 9573

Załącznik nr 3 do umowy

PROTOKÓŁ USUNIĘCIA/ZWROTU DANYCH OSOBOWYCH
powierzonych do przetwarzania na podstawie
Umowy CBI/……/2024/……., z dnia ……

ADMINISTRATOR:

……..

ul. ……

NIP ……., reprezentowany przez: ……..

przy kontrasygnacie:

……..

W imieniu PROCESORA oświadczamy, iż dane osobowe przetwarzane na podstawie Umowy oraz wszelkie ich istniejące kopie wytworzone zarówno w wersji papierowej jak i elektronicznej, zostały w dniu …….. roku trwale usunięte zarówno z nośników elektronicznych oraz dokumentów tradycyjnych / zwrócone powierzającemu.

Usunięcie danych osobowych nastąpiło w formie: ……

Poprzez trwałe usunięcie danych osobowych należy rozumieć takie zniszczenie tych danych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (art. 4 pkt. 1Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; Dz. U. UE. L. 2016, poz. 119.1),).

Członkowie komisji nadzorującej usuwanie danych osobowych:

……..
Imię i nazwisko, stanowisko — data, podpis

……..
Imię i nazwisko, stanowisko — data, podpis

……..
Imię i nazwisko, stanowisko — data, podpis