Puławy, dn. 28.04.2025 r.

**Zapytanie ofertowe nr ZO 17/2025**

na zamówienie pn.

**„Świadczenie usługi doradztwa w zakresie cyberbezpieczeństwa, ochrony danych osobowych, informatycznego oraz ochrony sygnalistów w SPZOZ w Puławach”**

1. **ZAMAWIAJĄCY:**

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Puławach

ul. Bema 1, 24-100 Puławy

KRS 0000026256, NIP 716-22-38-942, REGON 431205731

tel. 814502274

[www.szpitalpulawy.pl](http://www.szpitalpulawy.pl)

1. **OPIS PRZEDMIOTU ZAMÓWIENIA:**

**Przedmiotem zamówienia jest świadczenie usługi doradztwa w zakresie obowiązków dotyczących cyberbezpieczeństwa przypisanych operatorowi usługi kluczowej, doradztwa w zakresie ochrony danych osobowych, doradztwa informatycznego oraz doradztwa w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń sygnalistów zgodnie z przedstawionym zakresem czynności.**

1. W przedmiocie doradztwa w zakresie cyberbezpieczeństwa dla operatora usługi kluczowej:
2. bieżącą aktualizację przy ścisłej współpracy z operatorem usługi kluczowej, dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymogami norm PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301;
3. przygotowanie przy ścisłej współpracy z operatorem usługi kluczowej corocznej Analizy Ryzyka (oszacowania ryzyka) wystąpienia incydentu, rozumianego jako zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo świadczonej usługi kluczowej;
4. doradztwo w sprawach związanych z zarządzaniem oszacowanym ryzykiem;
5. 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;
6. przeprowadzenie warsztatów w zakresie cyberbezpieczeństwa, skierowanych do kadry zarządzającej jednostki;
7. 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.
8. 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;
9. doradztwo wobec powołanej przez operatora usługi kluczowej wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo w podejmowanych czynności i wykonywanych zadaniach nałożonych obowiązkami prawnymi Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. 2023 r., poz. 913) – zwanej dalej „Ustawą KSC” – t.j. w zakresie dotyczącym:
10. zarządzania incydentami oraz obsłudze incydentów, w szczególności poprzez pomoc merytoryczną w:
* wyszukiwaniu powiązań między incydentami,
* usuwaniu przyczyn wystąpienia incydentów,
* opracowywaniu wniosków wynikających z obsługi incydentu,
* dokonaniu prawidłowej rejestracji zaistniałego incydentu;
1. eliminacji podatności systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej w celu ograniczenia zagrożeń cyberbezpieczeństwa, które doprowadziły lub mogłyby doprowadzić do incydentu;
2. współdziałania wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo z właściwym CSIRT w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia;
3. w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia - świadczenie pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego - CSIRT;
4. 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;
5. doradztwo w zakresie przekazanych operatorowi usługi kluczowej zaleceń pokontrolnych dotyczących usunięcia stwierdzonych nieprawidłowości, wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa;
6. 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;
7. sporządzanie informacji w wymiarze nieprzekraczającym dwóch w miesiącu, w sprawach dotyczących prawnych zagadnień cyberbezpieczeństwa;
8. 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.
9. W przedmiocie doradztwa dla Inspektora Ochrony Danych (IOD) poprzez:
10. wykonywanie audytów dotyczących przestrzegania przepisów o ochronie danych osobowych;
11. 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;
12. wykonanie corocznej analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych;
13. 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;
14. informowanie o obowiązkach spoczywających na jednostce klienta na mocy przepisów o ochronie danych oraz doradztwo w tym zakresie;
15. monitorowanie przestrzegania przepisów wewnętrznych, polityk i procedur stosowanych przez jednostkę klienta w zakresie ochrony danych osobowych;
16. podejmowanie działań zwiększających świadomość prawną jednostki, jej pracowników i osób wykonujących pracę w oparciu o umowy cywilnoprawne wchodzących w skład kadry pracowniczej, w zakresie przetwarzania i ochrony danych osobowych;
17. udzielanie jednostce zaleceń co do oceny skutków dla ochrony danych oraz nadzorowanie realizacji zaleceń pokontrolnych;
18. 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;
19. 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.
20. W przedmiocie doradztwa Informatycznego:
21. doradztwo w określeniu zasad i procedur (we współpracy z działem obsługi informatycznej operatora usługi kluczowej) zapewniających bezpieczeństwo systemu informatycznego przetwarzającego dane osobowe;
22. wsparcie i doradztwa działu obsługi informatycznej operatora usługi kluczowej w zakresie – adekwatnych do potrzeb i jego możliwości – rozwiązań technologicznych dotyczących zabezpieczeń systemów informatycznych przetwarzających dane osobowe;
23. 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;
24. konsultacje działu informatycznego operatora usługi kluczowej w sprawach związanych z przetwarzaniem danych osobowych w systemie informatycznym;
25. wykonanie comiesięcznych testów podatności infrastruktury teleinformatycznej uznanymi narzędziami wraz z przygotowaniem raportu z opisem podatności oraz rekomendacjami dotyczącymi ich usunięcia w języku polskim;
26. coroczne 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.
27. Udostępnienie SYMULATORA ZAGROŻEŃ INTERNETOWYCH dedykowanego podmiotom sektora medycznego, gwarantującego:
28. Czytelne zasady obsługi - przedstawione w ramach zorganizowanego szkolenia oraz opisane w dołączonej instrukcji.
29. Bezpieczny sposób sprawdzenia oraz poznania typowych zagrożeń występujących w obszarze przestrzeni internetowej na dedykowanej platformie dostępnej na stronie www. dostosowanej do standardu WCAG 2.1, bez możliwości zapisu oraz archiwizacji wprowadzonych danych.
30. Realizację minimum ośmiu scenariuszy zagrożeń popularnych przestępstw internetowych typu: Phishing Clone, PhishingSpear, PhishingSpear Chat, PhishingWhaling, Pharming, Malware Post, Malware Email.
31. Możliwość tworzenia nowych scenariuszy zagrożeń w obszarze cyberbezpieczeństwa.
32. Nieograniczony dostępu do modułów spełniających poniższe możliwości:
* Moduł podstron (fałszywych witryn) do tworzenia witryn nakłaniających do pobierania zainfekowanych załączników, podawania wrażliwych danych lub dokonywania płatności internetowych.
* Moduł czatu z botami, symulujący wyłudzenia danych osobowych i numerów kart kredytowych.
* Moduł e-mail do przeglądania wiadomości z linkami lub załącznikami, symulującymi działanie malware.
* Moduł edukacyjny z informacjami o cyberprzestępstwach, identyfikacji zagrożeń, sposobach zapobiegania i działania po oszustwie.
* Moduł postów społecznościowych, prezentujący potencjalne ataki phishingowe lub pharmingowe.
1. Opracowanie oraz przekazanie zestawu testowego potwierdzającego funkcjonalność SYMULATORA poprzez:
* dokonanie prezentacji oferowanego Systemu Symulatora zagrożeń internetowych w obszarach proponowanych scenariuszy.
1. Wsparcie zabezpieczeniami technologicznymi w postaci:
	1. monitorowania CYBERBEZPIECZEŃSTWA w sposób ciągły i proaktywny - monitorowanie od strony sieci Internet otwartych portów i usług;
	2. wykrywania podatności w czasie rzeczywistym - indeksowanie podatności w urządzeniach podłączonych do Internet;
	3. analizy zagrożeń związanych z IoT;
	4. powiadomień o zmianach w infrastrukturze;
	5. wsparcia dla proaktywnej obrony.
2. Testy socjotechniczne kierowane na adresy e-mail w tym realizacja testów phishingowych zawierających różnorodne scenariusze, aby jak najlepiej odzwierciedlać realne zagrożenia, z jakimi mogą spotkać się pracownicy.
3. W przedmiocie doradztwa w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń sygnalistów:
4. Doradztwo w aktualizacji wprowadzonej „procedury zgłoszeń wewnętrznych”.
5. Doradztwo w realizacji obowiązków wynikających z przepisów prawa ochrony danych osobowych (RODO) w zakresie wynikającym z ustawy o ochronie sygnalistów:
6. przeprowadzeniu analizy ryzyka procesów przetwarzania danych osobowych sygnalistów i innych osób, których dane podlegać będą przetwarzaniu,
7. ocenie skutków przetwarzania danych osobowych (DPIA), w ramach procedury zgłoszeń wewnętrznych,
8. opracowanie wzorów obowiązków informacyjnych z art. 13 i art. 14 RODO, uwzględniających wyłączenia i ograniczenia prawne, wynikające z prawa ochrony sygnalistów,
9. wsparcie w aktualizacji i uzupełnianiu dokumentacji RODO: polityki ochrony danych oraz rejestru czynności przetwarzania.
10. Opcjonalne przeprowadzenie szkolenia dedykowanego kadrze zarządzającej (kierownictwu), obejmującego zagadnienia:
11. kim jest sygnalista i jaką rolę pełni w organizacji,
12. wymogi prawne w zakresie ochrony sygnalistów w Polsce,
13. korzyści i zagrożenia związane z systemami przyjmowania zgłoszeń od sygnalistów,
14. rola kierownictwa organizacji w zapewnieniu efektywnego i skutecznego systemu zgłaszania nieprawidłowości,
15. ryzyka zarządzania personelem, w odniesieniu do nowych obowiązków wynikających z przepisów prawa ochrony sygnalistów,
16. metodyka zapobiegania działaniom odwetowym (za podejmowanie których grozi odpowiedzialność karna z art. 55 ustawy o ochronie sygnalistów, nawet do 3 lat pozbawienia wolności).
17. Opcjonalne przeszkolenie pracowników, w zakresie prawa ochrony sygnalistów, obejmujące zagadnienia:
18. kim jest sygnalista i jaką rolę pełni w organizacji,
19. wymogi prawne w zakresie ochrony sygnalistów w Polsce,
20. czym mówi procedura zgłaszania nieprawidłowości,
21. w jaki sposób zgłaszać nieprawidłowość w organizacji.
22. 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:
23. zorganizowanie i przeprowadzenie spotkania zapewniającego zachowanie tajemnicy w zakresie informacji i danych osobowych,
24. udokumentowanie przedsiębranych działań i uzyskanych informacji.
25. Doradztwo w zakresie prowadzenia działań następczych, obejmujące:
26. ocenę, czy przekazane przez sygnalistę zgłoszenie, stanowi informację o naruszeniu prawa, w rozumieniu przepisów ustawy o ochronie sygnalistów,
27. rekomendacje odnośnie procedury weryfikacji prawdziwości informacji oraz przeciwdziałania naruszeniu prawa będącego przedmiotem zgłoszenia, w tym dokumentowania podejmowanych czynności,
28. wsparcie w zakresie zamknięcia procedury działań następczych i informacji zwrotnej w sprawie ujawnionych zagrożeń;
29. Doradztwo w zakresie identyfikowania i oceny działań odwetowych oraz przeciwdziałania takim działaniom, w tym:
* ocenę, czy ujawnione bądź zgłoszone działanie lub zaniechanie, stanowi działanie odwetowe albo próbę lub groźbę zastosowania działania odwetowego, w rozumieniu przepisów ustawy o sygnalistach,
* rekomendacje odnośnie wdrożenia procedury ochrony sygnalisty przed działaniami odwetowymi oraz adekwatnych środków ochrony, w tym dokumentowania podejmowanych czynności,
* wsparcie w zakresie informacji zwrotnej w sprawie ujawnionych zagrożeń.
1. Adres świadczenia usługi: Ul. Bema 1, 24-100 Puławy.
2. **TERMIN, SPOSÓB I WARUNKI WYKONANIA ZAMÓWIENIA**
3. Termin wykonania przedmiotu zamówienia**: 12 miesięcy od dnia podpisania umowy.**
4. **WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY ICH SPEŁNIANIA**
5. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące posiadania odpowiedniej sytuacji ekonomicznej, posiadania wiedzy i doświadczenia, dysponowania odpowiednimi narzędziami i osobami zdolnymi do wykonania zamówienia.
6. Sposób dokonania oceny spełniania przez Wykonawców warunków udział w postępowaniu zostanie wykonany metodą spełnia / nie spełnia na podstawie złożonych wraz z ofertą oświadczeń lub dokumentów.
7. Niepełnienie warunku określonego w pkt 1 skutkować będzie wykluczeniem Wykonawcy z postępowania.
8. Oferta Wykonawcy wykluczonego z postępowania zostanie odrzucona.
9. Wykonawca spełni warunek, o którym mowa w ust 1, jeżeli:
10. Dysponuje osobami posiadającymi uprawnienia do wykonywania przedmiotu zamówienia tj.:
11. co najmniej dwiema osobami posiadającymi odpowiednie umiejętności i uprawnienia, legitymującymi się certyfikatem uprawniającym do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, określonych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r., poz. 1999),
12. co najmniej dwiema osobami (w celu zachowania ciągłości działania) z minimum dwuletnim doświadczeniem w zakresie pełnienia funkcji Inspektora Ochrony Danych bądź realizacji usług doradczych na rzecz Inspektora Ochrony Danych podmiotu publicznego z czego jedna z nich wykaże posiadanie doświadczenia
w realizacji powyższych czynności na rzecz podmiotu / podmiotów sektora medycznego (szpitala / szpitali). Zakres realizowanych usług zgodny z przedmiotem zapytania lub szerszy.
13. co najmniej dwiema osobami posiadającymi certyfikat - Certified Ethical Hacker (CEH),
14. co najmniej trzy osoby posiadające certyfikaty w zakresie stosowania normy ISO/IEC 19011:2002
15. co najmniej jedną osobą posiadającąkompetencje Audytora bezpieczeństwa informacji potwierdzone certyfikatem **CISA**;
16. co najmniej jedną osobą posiadającąkompetencje Managera bezpieczeństwem informacji potwierdzone certyfikatem **CISM**;
17. posiada minimum 2 lata doświadczenia (popartego referencjami lub innymi dokumentami poświadczającymi należyte wykonanie) w zakresie pełnienia funkcji Inspektora Ochrony Danych bądź realizacji usług doradczych na rzecz Inspektora Ochrony Danych podmiotu sektora medycznego, którego zasoby kadrowe stanowią minimum 1.000 osób (osoby wykonujące prace w oparciu o stosunek pracy lub inne formy zatrudnienia – kontrakty, umowy zlecenia itp.). Zakres realizowanych usług zgodny z przedmiotem zapytania lub szerszy;
18. posiada minimum 2 lata doświadczenia (popartego referencjami lub innymi dokumentami poświadczającymi należyte wykonanie) w realizacji usługi doradczej w zakresie Krajowego Systemu Cyberbezpieczeństwa oraz przepisów i praktyk dotyczących ochrony danych osobowych świadczonej na rzecz operatora usługi kluczowej sektora medycznego, którego zasoby kadrowe stanowią minimum 1.000 osób (osoby wykonujące prace w oparciu o stosunek pracy lub inne formy zatrudnienia – kontrakty, umowy zlecenia itp.). Zakres realizowanych usług zgodny z przedmiotem zapytania lub szerszy;
19. aktualnie realizuje usług doradcze w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów w minimum **10 podmiotach publicznych** w tym co najmniej jednym podmiocie sektora medycznego pełniącego funkcję szpitala publicznego. Zakres realizowanych usług zgodny z przedmiotem zapytania lub szerszy.
20. wykonał co najmniej **10 Audytów Bezpieczeństwa** podmiotów medycznych mających na celu wskazanie podniesienie poziomu cyberbezpieczeństwa zgodnie z wymogami Zarządzeń Prezesa Narodowego Funduszu Zdrowia nr 68/2022/BBIICD lub nr 8/2023/BBIICD Prezesa Narodowego Funduszu Zdrowia;
21. wykonał co najmniej **4 usług** polegających na opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w podmiotach medycznych zgodnie z wymogami Zarządzeń Prezesa Narodowego Funduszu Zdrowia nr 68/2022/BBIICD lub nr 8/2023/BBIICD Prezesa Narodowego Funduszu Zdrowia;
22. posiada certyfikaty potwierdzające spełnienie wymagań działalności wykonawcy w zakresie stosowania norm **ISO/IEC 27001:2022** (System Zarządzania Bezpieczeństwem Informacji) oraz **PN-EN ISO 22301:2020** (System Zarządzania Ciągłością Działania) wydane przez jednostkę akredytowaną przez Polskie Centrum Akredytacji;
23. dysponuje profesjonalnym, komercyjnym skanerem podatności służącym wykrywaniu i usuwaniu zagrożeń na różnych poziomach infrastruktury zamawiającego;
24. posiada polisę ubezpieczeniową od **zawodowej odpowiedzialności cywilnej na min. 6 000 000 zł** dotyczącą wykonywania audytów i usługi doradczej w zakresie cyberbezpieczeństwa dla operatora usługi kluczowej, wykonywania u klientów funkcji inspektora ochrony danych/pełnienia funkcji doradczej dla inspektora ochrony danych oraz obejmującą monitorowanie, wdrażanie, nadzorowanie systemu bezpieczeństwa informacji w zakresie przepisów o ochronie danych osobowych, wykonywanie audytów KRI zgodnie z rozporządzeniem 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, a w przypadku podmiotów nie realizujących zadań publicznych - wykonanie audytów bezpieczeństwa.
25. **DOKUMENTY WYMAGANE NA POTWIERDZENIE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU**
	* 1. Na potwierdzenie spełniania warunków, o którym mowa w pkt IV.1 zapytania Zamawiający wymaga złożenie przez Wykonawcę oświadczenia stanowiącego załącznik nr 2 do niniejszego zapytania, wykazu usług stanowiącego załącznik nr 3 do niniejszego zapytania oraz dołączenia do oferty następujących dokumentów.
26. kopię certyfikatów potwierdzających uprawnienia osób wskazanych do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, określonych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r., poz. 1999),
27. kopię certyfikatów - Certified Ethical Hacker (CEH);
28. kopię certyfikatów - ISO/IEC 19011:2002;
29. kopię certyfikatów **CISA**;
30. kopię certyfikatów **CISM**;
31. oświadczenie oraz referencje (lub inne dokumenty poświadczające należyte wykonanie) potwierdzające doświadczenie wykonawcy z zakresie realizacji zadań Inspektora Ochrony Danych lub usług doradczych w tym zakresie w podmiotach medycznych których zasoby kadrowe stanowią minimum 1 000 osób;
32. oświadczenie oraz referencje (lub inne dokumenty poświadczające należyte wykonanie) potwierdzające doświadczenie w realizacji usług doradczych w zakresie Krajowego Systemu Cyberbezpieczeństwa w podmiotach medycznych których zasoby kadrowe stanowią minimum 1 000 osób;
33. wykaz minimum 10 podmiotów publicznych w których wykonawca realizuje usługi doradcze w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów;
34. wykaz podmiotów (popartego referencjami lub innymi dokumentami poświadczającymi należyte wykonanie usługi) w których wykonawca zrealizował minimum 10 usług polegających na przeprowadzeniu Audytów Bezpieczeństwa podmiotów medycznych zgodnie wymogami określonymi we wskazanych Zarządzeniach Prezesa NFZ;
35. wykaz podmiotów (poparty referencjami lub innymi dokumentami poświadczającymi należyte wykonanie usługi) w których wykonawca zrealizował minimum 5 usług polegających na opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w podmiotach medycznych zgodnie wymogami określonymi we wskazanych Zarządzeniach Prezesa NFZ;
36. kopię certyfikatów potwierdzającą spełnienie wymagań działalności wykonawcy w obszarze stosowania norm **ISO/IEC 27001:2022;**
37. kopię certyfikatów potwierdzającą spełnienie wymagań działalności wykonawcy w obszarze stosowania norm **PN-EN ISO 22301:2020;**
38. kopię polisy ubezpieczenia odpowiedzialności cywilnej zawodowej**.**
39. **OPIS SPOSOBU OBLICZENIA CENY OFERTY**
40. Cena powinna być podana w złotych polskich i obejmować cenę w rozumieniu art. 3 ustawy z 9 marca 2014 r. o informowaniu o cenach towarów i usług. (Dz. U. z 2023 r. poz. 168). Cena oferty powinna być podana w PLN cyfrowo i słownie z zaokrągleniem do dwóch miejsc po przecinku.
41. Cena podana w ofercie powinna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia oraz z warunkami stawianymi przez Zamawiającego.
42. Cenę należy podać zgodnie z wzorem zawartym w formularzu ofertowym, stanowiącym załącznik nr 1 do niniejszej zapytania.
43. Wszelkie rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w złotych polskich.
44. Zamawiający informuje, że jeżeli zostanie złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, ma obowiązek poinformować Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
45. Jeżeli ofertę złoży osoba fizyczna nieprowadząca działalności gospodarczej w cenie oferty należy wliczyć składki na ubezpieczenie społeczne i zdrowotne oraz zaliczkę na podatek dochodowy, które to Zamawiający, zgodnie z obowiązującymi przepisami, zobowiązany byłby naliczyć i odprowadzić.
46. **OCENA OFERT I INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY**
47. Kryterium oceny ofert:
48. Cena (C) – waga 100%
49. Opis sposobu przyznania punktacji w kryterium: Cena (C).

Kryterium „Cena” będzie rozpatrywane na podstawie ceny brutto za wykonanie przedmiotu zamówienia podanej przez Wykonawcę w formularzu ofertowym. Ilość punktów w tym kryterium zostanie obliczona na podstawie poniższego wzoru:

C = (Cena brutto oferty najtańszej / Cena brutto oferty badanej) \* 100 pkt

1. Przyznane punkty zostaną zaokrąglone do dwóch miejsc po przecinku.
2. W przypadku rozbieżności w wyliczeniach ceny netto, podatku VAT i ceny brutto, podstawą do dokonywania poprawek będzie cena netto.
3. Jeżeli wybór oferty najkorzystniejszej będzie niemożliwy z uwagi na to, że dwie lub więcej ofert uzyska taką samą liczbę punktów, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie przez niego określonym ofert dodatkowych.
4. Wykonawcy składający oferty dodatkowe nie mogą zaoferować wyższych cen jak zaoferowane w złożonych wcześniej ofertach.
5. Informację o wyborze najkorzystniejszej oferty Zamawiający przekaże wszystkim Wykonawcom, którzy złożyli oferty.
6. W przypadku odmowy podpisania umowy przez wybranego Wykonawcę, Zamawiający może zawrzeć umowę z Wykonawcą, który spełnia wymagania zapytania ofertowego i którego oferta uzyskała kolejno najwyższą ilość punktów.
7. **OPIS SPOSOBU PRZYGOTOWANIA OFERTY**
8. Wykonawca może złożyć tylko jedną ofertę, w której musi być zaoferowana tylko jedna cena. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert.
9. Na etapie składania ofert, na ofertę składa się:
10. Formularz ofertowy stanowiący zał. nr 1 do zapytania ofertowego.
11. Oświadczenie o spełnianiu warunków stanowiące zał. nr 2 do zapytania ofertowego.
12. Wykaz usług, o których mowa w pkt V.1.8)-10) zapytania na potwierdzenie spełniania warunków stanowiący zał. nr 3 do zapytania ofertowego.
13. aktualny wpis do CEIDG lub odpis z KRS-u.
14. Parafowany wzór umowy stanowiący zał. nr
15. Ofertę należy sporządzić w języku polskim zgodnie z treścią załączników do niniejszego zapytania. Zaleca się jej sporządzenie pismem maszynowym, komputerowym lub ręcznie długopisem lub nieścieralnym atramentem.
16. Oferta powinna być podpisana przez osobę uprawnioną/osoby uprawnione do reprezentowania Wykonawcy.
17. Wszystkie miejsca, w których Wykonawca naniósł zmiany powinny być podpisane przez osobę uprawnioną do występowania w imieniu Wykonawcy wraz z datą naniesienia zmiany.
18. Zamawiający uznaje, że podpisem jest:
19. podpis elektroniczny lub
20. własnoręcznie podpis – językowy znak graficzny umożliwiający identyfikację osoby składającej ofertę.
21. **MIEJSCE I TERMIN ZŁOŻENIA OFERTY:**
22. Termin składania ofert upływa dnia: **08.05.2025 r. o godz. 10:00.**
23. Ofertę można złożyć w jeden z następujących sposobów:
24. w formie papierowej: osobiście, za pośrednictwem Poczty Polskiej, kuriera, posłańca itp w kancelarii Zamawiającego - budynek administracyjny, ul. Bema 1, 24-100 Puławy

lub

1. w formie elektronicznej poprzez wysyłkę na adres e-mail: zp@szpitalpulawy.pl
2. Za formę elektroniczną oferty uznaje się ofertę:
3. Podpisaną podpisem elektronicznym.
4. Za datę złożenia oferty uznaje się datę faktycznego wpływu oferty do Zamawiającego.
5. W przypadku złożenia oferty po terminie określonym w ust. 1 oferta nie będzie rozpatrywana.
6. Oferta otrzymana przez Zamawiającego po terminie składania ofert, w sposób określony w ust. 2 pkt 1, zostanie wykonawcy zwrócona bez otwierania na jego żądanie lub po upływie 60 dni od złożenia zniszczona.
7. Wykonawca, w przypadku woli zachowania poufności oferty, może:
8. sporządzić ofertę w wersji papierowej i zamieścić ofertę w zamkniętej, nieprzejrzystej kopercie. W takim przypadku koperta powinna być zaadresowana na adres Zamawiającego: SPZOZ w Puławach, ul. Bema 1, 24-100 Puławy. Ponadto na kopercie należy umieścić w widocznym miejscu i czytelnym drukiem: „Oferta na usługę doradczą SPZOZ” lub
9. przesłać ofertą na adres e-mail wskazany w ust. 2 pkt 2 zapytania ofertowego w formie pliku zaszyfrowanego (np. plik pdf z hasłem) i najpóźniej do terminu otwarcia ofert przesłać hasło do otwarcia pliku zawierającego ofertę. Nieprzesłanie hasła będzie uznane za niezłożenie oferty w terminie.
10. Oferty złożone w sposób określony w ust. 7 będą jawne od terminu otwarcia ofert.
11. W przypadku złożenia oferty z pominięciem zasad poufności określonych w ust. 7 oferty będą jawne przed terminem otwarcia ofert jedynie dla Zamawiającego.
12. Wykonawca może wprowadzić zmiany lub wycofać ofertę złożoną przed upływem terminu składania ofert.
13. Wykonawcy będą związani swoimi ofertami 14 dni od końca terminu składania ofert.
14. **MIEJSCE I TERMIN OTWARCIA OFERT:**

Otwarcie złożonych ofert nastąpi w dniu 08.05.2025 r. o godz. 11:00 w siedzibie Zamawiającego.

1. **OSOBA UPRAWNIONA DO KONTATKÓW Z WYKOWCAMI:**

W sprawach związanych z przedmiotem zamówienia – p. Rafał Stachyra – Kierownik Działu Informatycznego, rstachyra@szpitalpulawy.pl , 81 45 02 297.

W sprawach związanych z postępowaniem – p. Maciej Goławski – Kierownik Działu Zamówień Publicznych, tel. 604113446, e:mail: mgolawski@szpitalpulawy.pl

1. **KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH**
	* 1. Na podstawie art. 19 ust. 1 Ustawy Pzp w związku z art. art. 13 ust. 1-3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej „RODO”, Zamawiający informuje, że:
	1. Wykonawca składając ofertę wyraża zgodę na gromadzenie i przetwarzanie swoich danych osobowych przez Zamawiającego w zakresie niezbędnym do przeprowadzenie postępowania i udzielenia zamówienia.
	2. administratorem danych osobowych jest Samodzielny Publiczny Zakład Opieki Zdrowotnej w Puławach, ul. Bema 1, 24-100 Puławy, NIP: 7162238942, REGON: 431205731.
	3. administrator wyznaczył Inspektora Ochrony Danych Osobowych, z którym można kontaktować się pocztą elektroniczną na adres e-mail: odo@szpitalpulawy.pl, telefonicznie na numer 814502274 lub pocztą tradycyjną na adres wskazany w punkcie 2
	4. Dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego, które jest prowadzone w trybie podstawowym;
	5. Odbiorcami danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 Ustawy Pzp;
	6. Dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 Ustawy Pzp przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy (art. 78 ust. 4 Ustawy Pzp);
	7. Obowiązek podania danych osobowych bezpośrednio dotyczących Wykonawcy jest wymogiem określonym w przepisach Ustawy Pzp, związanym z udziałem w niniejszym postępowaniu;
	8. w odniesieniu do danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do postanowień art. 22 RODO;
	9. Wykonawcy posiadają:
		1. zgodnie z art. 15 RODO - prawo dostępu do danych osobowych dotyczących (z zastrzeżeniem, że w sytuacji, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku, Wykonawcy mogą zostać zobowiązani do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego albo sprecyzowania nazwy lub daty zakończonego postępowania o udzielenie zamówienia);
		2. zgodnie z art. 16 RODO - prawo do sprostowania danych osobowych (z tym, że skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z Ustawą Pzp oraz nie może naruszać integralności protokołu z postępowania oraz załączników do niego);
		3. zgodnie z art. 18 RODO - prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego oraz przypadków, o których mowa w art. 18 ust. 2 RODO (prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
		4. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznają, że przetwarzanie danych osobowych narusza przepisy RODO;
		5. Wykonawcom nie przysługuje:
		6. zgodnie z art. 17 ust. 3 lit. b, d lub e RODO - prawo do usunięcia danych osobowych;
		7. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
		8. zgodnie z art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO.
		9. Jednocześnie Zamawiający przypomina o ciążącym na Wykonawcy obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od Wykonawcy.
2. **ZAŁĄCZNIKI DO ZAPYTANIA OFERTOWEGO.**
3. Formularz ofertowy.
4. Oświadczenie.
5. Wykaz usług.
6. Wzór umowy.

 Maciej Goławski

 Kierownik Działu Zamówień Publicznych

 SPZOZ w Puławach

Zał. nr 1 do Zapytania ofertowego nr ZO 17/2025

……………………………………………….

 Miejscowość, data

………………………………………………………

………………………………………………………

[*Nazwa lub pieczęć wykonawcy*]

**Formularz ofertowy**

Nawiązując do zaproszenia do złożenia oferty w zapytaniu ofertowym nr ZO 17/2025 z dnia 28.04.2025 r. pn. **„Świadczenie usługi doradztwa w zakresie cyberbezpieczeństwa, ochrony danych osobowych, informatycznego oraz ochrony sygnalistów w SPZOZ w Puławach”**,

ja niżej podpisany, działając w imieniu i na rzecz Wykonawcy:

…………………………………………………………………………………………………………………………………………..

(nazwa Wykonawcy)

……………………………………………………………………………………………………………………………………………

(adres Wykonawcy)

NIP …………………………………………………….. Regon ………………………………………………….

Nr telefonu ………………………………………… e-mail: ………………………………………………….

* + - 1. Oferuję realizację zamówienia zgodnie z wszystkimi postanowieniami Zapytania ofertowego za łączną cenę:

NETTO: ……………………………………. zł (słownie: …………………………………………………………………………… zł)

PODATEK VAT (……….%) - ……………………………….. zł,

BRUTTO: …………………………………. zł (słownie: …………………………………………………………………………… zł)

* + - 1. Zapoznałem się z zapytaniem ofertowym oraz jego załącznikami, nie wnoszę do ich treści zastrzeżeń i uznaję się za związanego określonymi w niej postanowieniami i zasadami postępowania.
			2. Oświadczam, że przedmiot oferty jest zgodny z zapisami w zapytaniu ofertowym.
			3. Oświadczam, że wszystkie informacje podane w ofercie są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.
			4. Zapoznałem się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych zawartą w zapytaniu ofertowym i ją akceptuję.
			5. Załącznikami do niniejszego formularza ofertowego stanowiącego integralną część oferty są:
1. …………………………………………………………
2. …………………………………………………………

…………………………………………………………

 .............................................................

 [*Podpis osoby uprawnionej*]

Zał. nr 2 do Zapytania ofertowego nr ZO 17/2025

……………………………………………….

 Miejscowość, data

………………………………………………………

………………………………………………………

[*Nazwa lub pieczęć wykonawcy*]

**OŚWIADCZENIE**

**O SPEŁNIANIU WARUNKÓW**

Składając ofertę do zapytania ofertowego nr ZO 17/2025 z dnia 28.04.2025 r. pn. **„Świadczenie usługi doradztwa w zakresie cyberbezpieczeństwa, ochrony danych osobowych, informatycznego oraz ochrony sygnalistów w SPZOZ w Puławach”**, ja niżej podpisany, działając w imieniu i na rzecz Wykonawcy:

…………………………………………………………………………………………………………………………………………..

(nazwa Wykonawcy)

……………………………………………………………………………………………………………………………………………

(adres Wykonawcy)

NIP …………………………………………………….. Regon ………………………………………………….

1. Oświadczam, że spełniam wszystkie warunki udziału w postępowaniu dotyczące odpowiedniej sytuacji ekonomicznej, posiadania wiedzy i doświadczenia, dysponowania odpowiednimi narzędziami i osobami zdolnymi do wykonania zamówienia zgodnie z wymogami pkt IV.5 Zapytania ofertowego.
2. Na potwierdzenie spełniania warunków, o którym mowa w ust. 1 przedkłada stosowne dowody.

 .............................................................

 [*Podpis osoby uprawnionej*]

Zał. nr 3 do Zapytania ofertowego nr ZO 17/2025

……………………………………………….

 Miejscowość, data

………………………………………………………

………………………………………………………

[*Nazwa lub pieczęć wykonawcy*]

**Wykaz usług doradczych**

Wykaz podmiotów publicznych, w których aktualnie realizuję usługi doradcze w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów:

1. …………………………………………………………………………………………………………
2. …………………………………………………………………………………………………………
3. …………………………………………………………………………………………………………
4. …………………………………………………………………………………………………………
5. …………………………………………………………………………………………………………
6. …………………………………………………………………………………………………………
7. …………………………………………………………………………………………………………
8. …………………………………………………………………………………………………………
9. …………………………………………………………………………………………………………
10. …………………………………………………………………………………………………………

Wykaz podmiotów medycznych, w których zrealizowane zostały usługi wykonania Audytów Bezpieczeństwa zgodnie wymogami określonymi we wskazanych Zarządzeniach Prezesa NFZ:

1. …………………………………………………………………………………………………………
2. …………………………………………………………………………………………………………
3. …………………………………………………………………………………………………………
4. …………………………………………………………………………………………………………
5. …………………………………………………………………………………………………………
6. …………………………………………………………………………………………………………
7. …………………………………………………………………………………………………………
8. …………………………………………………………………………………………………………
9. …………………………………………………………………………………………………………
10. …………………………………………………………………………………………………………

Wykaz podmiotów medycznych w których zrealizowane zostały usługi polegające na opracowaniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie wymogami określonymi we wskazanych Zarządzeniach Prezesa NFZ:

1. …………………………………………………………………………………………………………
2. …………………………………………………………………………………………………………
3. …………………………………………………………………………………………………………
4. …………………………………………………………………………………………………………
5. …………………………………………………………………………………………………………

 .............................................................

 [*Podpis osoby uprawnionej*]

Zał. nr 4 do zapytania ofertowego nr ZO 17/2025

/WZÓR/

**Umowa**

**usługi doradztwa w zakresie obowiązków dotyczących cyberbezpieczeństwa przypisanych operatorowi usługi kluczowej, doradztwa w zakresie ochrony danych osobowych, doradztwa informatycznego oraz doradztwa w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów**

**(zwana dalej „Umową”)**

zawarta w dniu ………………………w ……………………, pomiędzy:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, z siedzibą przy \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_NIP: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

reprezentowany przez:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zwanym w dalszej części Umowy **„Zleceniodawcą”**

a

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, z siedzibą przy \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_NIP: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

reprezentowany przez:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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. 2023 r., poz. 913), doradztwa w zakresie ochrony danych osobowych oraz doradztwa informatycznego, w zamian za co Zleceniodawca zobowiązuje się do zapłaty umówionego wynagrodzenia. Zakres czynności ujętych w przepisach § 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 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. 2023 r., poz. 913), – zwanej dalej „Ustawą KSC”) zobowiązuje się do wykonania następujących czynności:
2. Bieżącą aktualizację przy ścisłej współpracy z operatorem usługi kluczowej, dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymogami norm PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301;
3. doradztwo osobie wyznaczonej przez Zleceniodawcę i będącej odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w sprawach wymagających wykonywania obowiązków wobec tych podmiotów;
4. doradztwo 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:
5. zarządzania incydentami oraz obsłudze incydentów;
* wyszukiwaniu powiązań między incydentami,
* usuwaniu przyczyn wystąpienia incydentów,
* opracowywaniu wniosków wynikających z obsługi incydentu,
* dokonaniu prawidłowej rejestracji zaistniałego incydentu;
1. eliminacji podatności systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
2. współdziałania wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo z właściwym CSIRT w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia;
3. świadczenie pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT – w przypadku wystąpienia incydentu wymagającego stosownego zgłoszenia;
4. 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;
5. doradztwo 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;
6. przygotowanie oszacowania ryzyka wystąpienia incydentu, rozumianego jako zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo świadczonej usługi kluczowej;
7. doradztwo w sprawach związanych z zarządzaniem oszacowanym ryzykiem;
8. pomoc 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;
9. sporządzanie 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 Kodeksu Cywilnego;
10. 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;
11. przeprowadzenie warsztatów w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej jednostki;
12. przeprowadzenie 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 2019 r. poz. 544) w zakresie certyfikacji osób.
13. comiesięczne wykonywanie testów podatności infrastruktury teleinformatycznej
z przygotowaniem raportu w języku polskim z opisem podatności oraz rekomendacjami dotyczącymi ich usunięcia.
14. 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.
15. 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.
16. 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 były przez niego zawinione.

**§ 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 (w dalszej części niniejszej Umowy zwanego „RODO”), a które to dane osobowe przetwarzane są ramach prowadzonej przez niego działalności.
Doradztwo obejmuje:
2. 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), oraz doradztwo w tym zakresie,
3. monitorowanie przestrzegania przepisów wewnętrznych, polityk i procedur stosowanych przez Zleceniodawcę w zakresie ochrony danych osobowych,
4. 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,
5. 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;
6. wykonywanie audytów dotyczących przestrzegania przepisów o ochronie danych osobowych,
7. wykonywanie analizy zagrożeń i ryzyka przy przetwarzaniu danych osobowych,
8. udzielanie Zleceniodawcy zaleceń co do oceny skutków dla ochrony danych oraz nadzorowanie realizacji zaleceń pokontrolnych,
9. 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;
10. 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,
11. 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 zobowiązuje się do wykonywania następujących czynności:
2. ścisłej współpracy z Inspektorem Ochrony Danych;
3. doradztwa w określeniu zasad i procedur (we współpracy z działem obsługi informatycznej Zleceniodawcy) zapewniających bezpieczeństwo systemu informatycznego przetwarzającego dane osobowe;
4. wsparcia i doradztwa działu obsługi informatycznej Zleceniodawcy w zakresie – adekwatnych do potrzeb i możliwości Zleceniodawcy – rozwiązań technologicznych dotyczących zabezpieczeń systemów informatycznych przetwarzających dane osobowe;
5. 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;
6. konsultacje działu informatycznego Zleceniodawcy w sprawach związanych z przetwarzaniem danych osobowych w systemie informatycznym.
7. udostępnienie symulatora zagrożeń internetowych dedykowanego podmiotom sektora medycznego, gwarantującego:
8. Czytelne zasady obsługi - przedstawione w ramach zorganizowanego szkolenia oraz opisane w dołączonej instrukcji.
9. Bezpieczny sposób sprawdzenia oraz poznania typowych zagrożeń występujących w obszarze przestrzeni internetowej na dedykowanej platformie dostępnej na stronie www. dostosowanej do standardu WCAG 2.1, bez możliwości zapisu oraz archiwizacji wprowadzonych danych.
10. Realizację minimum ośmiu scenariuszy zagrożeń popularnych przestępstw internetowych typu: Phishing Clone, PhishingSpear, PhishingSpear Chat, PhishingWhaling, Pharming, Malware Post, Malware Email.
11. Możliwość tworzenia nowych scenariuszy zagrożeń w obszarze cyberbezpieczeństwa.
12. Nieograniczony dostępu do modułów spełniających poniższe możliwości:
* Moduł podstron (fałszywych witryn) do tworzenia witryn nakłaniających do pobierania zainfekowanych załączników, podawania wrażliwych danych lub dokonywania płatności internetowych.
* Moduł czatu z botami, symulujący wyłudzenia danych osobowych i numerów kart kredytowych.
* Moduł e-mail do przeglądania wiadomości z linkami lub załącznikami, symulującymi działanie malware.
* Moduł edukacyjny z informacjami o cyberprzestępstwach, identyfikacji zagrożeń, sposobach zapobiegania i działania po oszustwie.
* Moduł postów społecznościowych, prezentujący potencjalne ataki phishingowe lub pharmingowe.
1. Opracowanie oraz przekazanie zestawu testowego potwierdzającego funkcjonalność symulatora poprzez dokonanie prezentacji oferowanego Systemu Symulatora zagrożeń internetowych w obszarach proponowanych scenariuszy.
2. Wsparcie Zleceniodawcy systemem, który zapewnia zaawansowane zabezpieczenie technologiczne, w postaci:
3. monitorowania cyberbezpieczeństwa w sposób ciągły i proaktywny poprzez monitorowanie od strony sieci Internet otwartych portów i usług, które mogą stać się celem ataków – funkcja monitorowania umożliwia szybkie wykrycie, jeśli porty zostaną otwarte bez autoryzacji lub jeśli usługi zostaną uruchomione na urządzeniach, co może sugerować naruszenie bezpieczeństwa;
4. wykrywania podatności w czasie rzeczywistym – indeksowanie podatności w urządzeniach podłączonych do Internetu – funkcja umożliwia użytkownikom usługi możliwość natychmiastowego otrzymywania powiadomień o nowych podatnościach wykrytych w ich infrastrukturze, co pozwala na szybkie działania zapobiegawcze, takie jak instalacja poprawek bezpieczeństwa lub ograniczenie dostępu do podatnych urządzeń;
5. analizy zagrożeń związanych z IoT – funkcja monitorowania urządzeń Internetu Rzeczy (IoT) za pomocą usługi, przyczynia się do skutecznego zarządzania ryzykiem jakie niesie ze sobą IoT, a także minimalizowania potencjalnych wektorów ataku;
6. powiadomień o zmianach w infrastrukturze – funkcja polegająca na wysyłaniu przez system powiadomień, gdy do sieci zostają dodane nowe urządzenia, co może sygnalizować potencjalne zagrożenia lub naruszenia, w konsekwencji czego umożliwia szybkie zbadanie i ewentualne zabezpieczenie ww. nowych elementów;
7. wsparcia dla proaktywnej obrony – funkcja umożliwia stosowanie proaktywnych środków bezpieczeństwa poprzez regularne analizy danych pomagających zidentyfikować anomalie lub potencjalne ataki, zanim te doprowadzą do rzeczywistych szkód;
8. dostarczania dokładnych i bieżących danych o stanie bezpieczeństwa infrastruktury IT Zleceniodawcy – funkcja umożliwia utrzymanie organizacji Zleceniodawcy w zgodności z przepisami prawa, z uwagi na uzyskiwanie danych pozwalających na weryfikację stanu faktycznego z regulacjami dotyczącymi ochrony danych osobowych, bezpieczeństwa informacji i cyberbezpieczeństwa, wymagań interoperacyjności, co dostarcza użyteczny informacji w czynnościach audytowych bezpieczeństwa w zakresie dokumentacji zmian i zagrożeń.
9. Coroczne 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.
10. Zleceniodawca zobowiązuje się do przekazania Zleceniobiorcy listy zewnętrznych numerów IP sprzętu objętego usługą o której mowa w § 4 ust. 1 pkt 7) Umowy pod adres osoby upoważnionej do kontaktu ze strony Zleceniobiorcy, o której mowa w § 15 ust. 4 pkt a) Umowy. Brak przekazania zewnętrznych numerów IP nie stanowi przesłanki braku realizacji Umowy przez Zleceniobiorcę.
11. Zawiadomienia (tzw. alerty) w ramach usługi wskazanej § 4 ust. 1 pkt 7) Umowy generowane przez system będą przekazywane Zleceniodawcy przez Zleceniobiorcę pod adres poczty elektronicznej e-mail osoby upoważnionej do kontaktu ze strony Zleceniodawcy, o której mowa w § 15 ust. 3 pkt a) Umowy.

**§ 5**

**Szczegółowy zakres świadczonej przez Zleceniobiorcę usługi – doradztwo w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów**

1. Zleceniobiorca w ramach świadczonej usługi w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów zobowiązuje się do wykonywania następujących czynności:
2. Doradztwo w aktualizacji wprowadzonej „procedury zgłoszeń wewnętrznych”.
3. Doradztwo w realizacji obowiązków wynikających z przepisów prawa ochrony danych osobowych (RODO) w zakresie wynikającym z ustawy o ochronie sygnalistów:
* przeprowadzeniu analizy ryzyka procesów przetwarzania danych osobowych sygnalistów i innych osób, których dane podlegać będą przetwarzaniu,
* ocenie skutków przetwarzania danych osobowych (DPIA), w ramach procedury zgłoszeń wewnętrznych,
* opracowanie wzorów obowiązków informacyjnych z art. 13 i art. 14 RODO, uwzględniających wyłączenia i ograniczenia prawne, wynikające z prawa ochrony sygnalistów,
* wsparcie w aktualizacji i uzupełnianiu dokumentacji RODO: polityki ochrony danych oraz rejestru czynności przetwarzania.
1. Opcjonalne przeprowadzenie szkolenia dedykowanego kadrze zarządzającej (kierownictwu), obejmującego zagadnienia:
* kim jest sygnalista i jaką rolę pełni w organizacji,
* wymogi prawne w zakresie ochrony sygnalistów w Polsce,
* korzyści i zagrożenia związane z systemami przyjmowania zgłoszeń od sygnalistów,
* rola kierownictwa organizacji w zapewnieniu efektywnego i skutecznego systemu zgłaszania nieprawidłowości,
* ryzyka zarządzania personelem, w odniesieniu do nowych obowiązków wynikających z przepisów prawa ochrony sygnalistów,
* metodyka zapobiegania działaniom odwetowym (za podejmowanie których grozi odpowiedzialność karna z art. 55 ustawy o ochronie sygnalistów, nawet do 3 lat pozbawienia wolności).
1. Opcjonalne przeszkolenie pracowników, w zakresie prawa ochrony sygnalistów, obejmujące zagadnienia:
* kim jest sygnalista i jaką rolę pełni w organizacji,
* wymogi prawne w zakresie ochrony sygnalistów w Polsce,
* czym mówi procedura zgłaszania nieprawidłowości,
* w jaki sposób zgłaszać nieprawidłowość w organizacji.
1. 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:
* zorganizowanie i przeprowadzenie spotkania zapewniającego zachowanie tajemnicy w zakresie informacji i danych osobowych,
* udokumentowanie przedsiębranych działań i uzyskanych informacji.
1. Doradztwo w zakresie prowadzenia działań następczych, obejmujące:
* ocenę, czy przekazane przez sygnalistę zgłoszenie, stanowi informację o naruszeniu prawa, w rozumieniu przepisów ustawy o ochronie sygnalistów,
* rekomendacje odnośnie procedury weryfikacji prawdziwości informacji oraz przeciwdziałania naruszeniu prawa będącego przedmiotem zgłoszenia, w tym dokumentowania podejmowanych czynności,
* wsparcie w zakresie zamknięcia procedury działań następczych i informacji zwrotnej w sprawie ujawnionych zagrożeń;
1. Doradztwo w zakresie identyfikowania i oceny działań odwetowych oraz przeciwdziałania takim działaniom, w tym:
* ocenę, czy ujawnione bądź zgłoszone działanie lub zaniechanie, stanowi działanie odwetowe albo próbę lub groźbę zastosowania działania odwetowego, w rozumieniu przepisów ustawy o sygnalistach,
* rekomendacje odnośnie wdrożenia procedury ochrony sygnalisty przed działaniami odwetowymi oraz adekwatnych środków ochrony, w tym dokumentowania podejmowanych czynności,
* wsparcie w zakresie informacji zwrotnej w sprawie ujawnionych zagrożeń.

**§ 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 2021 r., poz.1062).
3. Zleceniobiorca ponosi odpowiedzialność w zakresie winy za 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 ISO/IEC 27001:2022 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 tworzącą część usługi objętej Umową, Zleceniodawca zobowiązuje się do przekazywania niezwłocznie, osobiście lub za pośrednictwem wyznaczonego pracownika, w terminie nie dłuższym niż 5 dni robocze liczonym od dnia przedłożenia stosownego wniosku (przekazanego w formie pisemnej lub formie elektronicznej za pośrednictwem poczty e-mail lub formie ustnej – przy czym dla celów dowodowych forma ta powinna zostać potwierdzona przynajmniej jedną z dwóch pozostałych wymienionych form) 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. 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:
9. przetwarzania w/w danych jedynie w zakresie i celu wykonania Umowy;
10. 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;
11. na wniosek Zleceniodawcy – do informowania o zasadach przetwarzania przez Zleceniobiorcę danych;
12. 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. 223 Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 2022 r., poz. 1510), 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, 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 niebędące 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.

1. Czas trwania przetwarzania powierzonych Procesorowi danych osobowych będzie zgodny z czasem obowiązywania Umowy.
2. 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.
3. 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.
4. 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:
5. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
6. podejmuje odpowiednie środki techniczne oraz organizacyjne, mające na celu zapewnienia bezpieczeństwa danych osobowych zgodnie z art. 32 RODO;
7. nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody Administratora;
8. 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;
9. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO;
10. 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;
11. 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,
12. 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.
13. 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.
14. 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.
15. 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:
	1. 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;
	2. możliwe konsekwencje naruszenia ochrony danych osobowych;
	3. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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
27. 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.
28. Strony zobowiązują się, że wszelkie decyzje dotyczące polubownego zakończenia sporu z osobą fizyczną na skutek naruszenia ochrony jej danych osobowych, w szczególności fakt i wysokość wypłaty ewentualnego odszkodowania, podejmą wspólnie.
29. Administrator ma prawo wypowiedzieć Umowę w trybie natychmiastowym, w przypadku rażącego naruszenia postanowień Umowy w zakresie ochrony danych osobowych przez Procesora, który:
30. 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;
31. wykonuje Umowę niezgodnie z obowiązującymi w tym zakresie przepisami prawa lub instrukcjami Administratora w tym zakresie;
32. 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:
2. utrwalania i zwielokrotniania na wszelkich nośnikach w celu wewnętrznego wykorzystania przez Zleceniodawcę;
3. 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.

**§ 12**

**Wynagrodzenie**

1. Z tytułu realizacji niniejszej Umowy Zleceniobiorcy przysługiwać będzie ryczałtowe **wynagrodzenie miesięczne, płatne z dołu, w wysokości ……………… zł netto**
(słownie: …………………..) plus należny podatek VAT wedle stawki obowiązującej w danym miesiącu (w dalszej części niniejszej Umowy zwane również jako „Wynagrodzenie”).
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: ……………………………………………….
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:** …………………………………………….

**ODBIORCA:** …………………………………………….

**§ 13**

**Okres obowiązywania Umowy oraz możliwość jej wypowiedzenia**

* + 1. Umowa obowiązuje od dnia ……………………… do ……………………….
		2. Każdej ze Stron przysługuje uprawnienie do wypowiedzenia niniejszej Umowy z zachowaniem trzymiesięcznego okresu wypowiedzenia ze skutkiem na koniec trzeciego miesiąca, następującego po miesiącu, w którym oświadczenie o wypowiedzeniu zostało złożone drugiej Stronie. 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. 781  § 1 Kodeksu cywilnego) zgodnie z § 15 ust. 2 Umowy, zastrzegając przy tym obydwie formy pod rygorem nieważności.

**§ 14**

**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.

**§ 15**

**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**:
	1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , tel.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; e- mail:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .
	2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , tel.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , e- mail:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .
4. Osoby upoważnione do kontaktu ze strony **Zleceniobiorcy**:
	1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , tel.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; e- mail:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .
	2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , tel.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , e- mail:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .
5. W przypadku stwierdzonych przez Zleceniodawcę wad i usterek w przedmiocie 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 z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. 2020 r., poz.1369).
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. Zmiana postanowień Umowy wymaga formy pisemnej pod rygorem nieważności.
9. Wszelkie załączniki do Umowy stanowią jej integralną część.
10. W kwestiach nieuregulowanych mają zastosowanie przepisy z Kodeksu cywilnego.
11. Strony ustalają, że sądem właściwym do rozstrzygania sporów mogących w przyszłości powstać na tle Umowy będzie sąd miejscowo właściwy dla siedziby Zleceniodawcy.
12. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

|  |  |
| --- | --- |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **(Zleceniodawca)** | **(Zleceniobiorca)** |

Załączniki:

1. Wydruk z Centralnej Informacja Krajowego Rejestru Sądowego Zleceniodawcy z dnia …………………
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 z dnia …………………. **usługi doradztwa w zakresie obowiązków dotyczących cyberbezpieczeństwa przypisanych operatorowi usługi kluczowej, doradztwa w zakresie ochrony danych osobowych, doradztwa informatycznego oraz doradztwa w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów**

…………………………….

(data i podpis Zleceniodawcy)

Załącznik nr 3 do umowy

**PROTOKÓŁ USUNIĘCIA/ZWROTU DANYCH OSOBOWYCH**

**powierzonych do przetwarzania na podstawie
Umowy z dnia ………………… usługi doradztwa w zakresie obowiązków dotyczących cyberbezpieczeństwa przypisanych operatorowi usługi kluczowej, doradztwa w zakresie ochrony danych osobowych, doradztwa informatycznego oraz doradztwa w zakresie zarządzania wewnętrzną procedurą przyjmowania zgłoszeń od sygnalistów**

ADMINISTRATOR:

……………………………………………..

ul. ………………………………………….

NIP ………………………………., reprezentowany przez: …………………………………..

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