zał. nr 1 do zapytania ofertowego nr Sp/AZP/382/13/2022

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest usługa polegająca na:

Usługa przeprowadzenia audytu oraz diagnozy poziomu bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) i rekomendacji dotyczących podniesienia tego poziomu jako dwu etapowego audytu bezpieczeństwa systemu informacyjnego i ochrony danych medycznych zgodnie z „Wymaganiami dotyczącymi audytu bezpieczeństwa", stanowiącymi załącznik nr 2 do Umowy o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, będącej załącznikiem Nr 2 do Zarządzenia Nr 68/2022/BBIICD Prezesa NFZ z dnia 20 maja 2022 r. ,z wymaganiami ustawy z dnia 13 sierpnia 2018 roku o Krajowym Systemie Cyberbezpieczeństwa , Krajowych Ram Interoperacyjności zgodnie z wymaganiami norm PN ISO IEC 27001, PN ISO IEC 22301 wraz z wykorzystaniem standardów WGITA oraz NSC

poprzez dwukrotne tożsame zadaniowo badanie

a) spełniania wymogów dokumentacyjnych obowiązujących u Zamawiającego jako regulacji wewnętrznych dokumentacji normatywnej i operacyjnej dotyczących usługi kluczowej bezpieczeństwa informacji - dokumentacja SZBI/KRI/BCM , ochrony danych osobowych dokumentacja RODO i ODO ,
b) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych
c) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych
   w zakresie:
   a) skuteczności działania infrastruktury,
   b) procesów zarządzania bezpieczeństwem informacji,
   c) monitorowania i reagowania na incydenty bezpieczeństwa,
   d) zarządzania ciągłością działania,
   e) utrzymania systemów informacyjnych,
   f) zarządzania bezpieczeństwem i ciągłością działania łańcucha usług

każdorazowe badanie:

- spełniania wymogów dokumentacyjnych obowiązujących u Zamawiającego jako regulacji wewnętrznych dokumentacji normatywnej i operacyjnej dotyczących usługi kluczowej bezpieczeństwa informacji - dokumentacja SZBI/KRI/BCM , ochrony danych osobowych dokumentacja RODO i ODO ,
- określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych
- określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych

Zakres audytu

Ocena stopnia dojrzałości i zgodności organizacyjno - technicznej infrastruktury ICT w kontekście zabezpieczeń konfiguracji, eksploatacji projektu modernizacji ICT jako Operatora usługi Kluczowej , funkcjonującego u Zamawiającego jako realizację czynności:

1. Audyt organizacyjny polegający na:

a) weryfikacji środków organizacyjnych (w tym dokumentacja SZBI) w obszarze bezpieczeństwa informacji, w tym danych osobowych;

b) weryfikacji procesów i czynności przetwarzania danych uwzględniając ich charakter, zakres, kontekst, cele przetwarzania, zasoby, aktywa i ryzyka

c) weryfikacji realizowania przez pracowników obowiązków wynikających z regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI/BCM/ODO).

Wykaz obowiązków pracowników podlegających weryfikacji (poszczególnych procedur, instrukcji, zapisów z dokumentacji SZBI) zostanie przedłożony Wykonawcy po podpisaniu umowy. Weryfikacja musi obejmować przynajmniej kierownika lub zastępcę kierownika każdej komórki organizacyjnej oraz jej pracowników (chyba, że komórka posiada mniejszą liczbę pracowników - wówczas wszystkich jej pracowników).

Audyt bezpieczeństwa fizycznego

Badanie polega na polegający na weryfikacji środków technicznych służących zabezpieczeniu informacji, w tym danych osobowych, w szczególności stanu bezpieczeństwa fizycznego i środowiskowego siedziby Zamawiającego - budynki i pomieszczenia na podstawie wizji lokalnej obszarów przetwarzania danych.

Audyt teleinformatyczny

Badanie polega na wykonaniu czynności audytowych na wybranej reprezentatywnej próbie i przeprowadzeniu nieinwazyjnych (wewnętrznych i zewnętrznych) testów penetracyjnych systemów informatycznych w szczególności odniesieniu do infrastruktury sieciowej, systemu Firewall, aplikacji, portali i wybranych serwisów www oraz poczty elektronicznej jako:

1. weryfikacji bezpieczeństwa infrastruktury sieciowej w szczególności:
    a) inwentaryzacja urządzeń sieciowych (adresy IP, konfiguracja urządzeń, konfiguracja zapory ogniowej, podział na sieci logiczne i fizyczne) w siedzibie Zamawiającego
    b) analiza urządzeń i ich parametrów technicznych zapewniających stronie Zamawiającej dostęp do sieci Internet - w tym serwera brzegowego, urządzeń UTM, Firewall, routerów;
    c) analiza konfiguracji sieci lokalnej;
    d) analiza oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia informatycznego;
    e) analiza sposobu połączenia segmentów pomiędzy sobą;
    f) analiza metody komunikacji pomiędzy segmentami sieci.
    g) analiza zabezpieczenia ciągłości działania

2. weryfikacji bezpieczeństwa infrastruktury serwerowej w szczególności:
    a) analiza bezpieczeństwa zainstalowanych usług (czy zainstalowane oprogramowanie jest aktualne, czy zainstalowane oprogramowanie posiada znane luki w bezpieczeństwie, kto ma

dostęp do udostępnionych usług);

b) analiza bezpieczeństwa serwerów pod kątem dostępu użytkowników (czy jedynie uprawnieni użytkownicy mają dostęp do usług, czy udostępnione usługi zawierają jedynie te dane które są wymagane);
c) analiza bezpieczeństwa uprawnień poszczególnych użytkowników oraz grup użytkowników;
d) analiza bezpieczeństwa fizycznego infrastruktury serwerowej,
e) analiza zabezpieczenia ciągłości działania

3. weryfikacji bezpieczeństwa poczty elektronicznej, domeny, stron internetowych Zamawiającego wg wymagań WCGA 2.1
4. weryfikacji bezpieczeństwa systemów (aplikacji) w których przetwarzane są dane osobowe
   a) analiza podatności komponentów aplikacji, w tym serwerów aplikacyjnych i baz danych - próby uzyskania dostępu do panelu administracyjnego za pomocą kont zwykłych użytkowników m. in. przez wykorzystanie bieżącej sesji, podniesienie uprawnień, próby uzyskania większych uprawnień, próby uzyskania nieautoryzowanego dostępu do danych znajdujących się w systemie;
   b) analiza szyfrowania danych dla danych przesyłanych przez sieci publiczne.
   c) Wykaz systemów w których przetwarzane są dane w tym dane osobowe w weryfikacji bezpieczeństwa stacji roboczych:
      - analiza kontroli dostępu do stacji roboczych,
      - analiza zainstalowanego oprogramowania znajdującego się na stacjach roboczych,
      - analiza bezpieczeństwa stacji roboczych pod kątem zainstalowanych usług, dostępów zdalnych do stacji roboczych, bezpieczeństwa ochrony antywirusowej.
   d) analiza zabezpieczenia ciągłości działania
5. weryfikacji zarządzania kopiami zapasowymi i ciągłością działania w szczególności:
   a) analizę poprawności wykonywanych kopii zapasowych,
   b) analiza częstotliwości wykonywania kopii zapasowych,
   c) analiza bezpieczeństwa wykonywanych kopii zapasowych,
   d) analiza testów odzyskiwania kopii zapasowych - odtwarzania danych w środowisku testowym,
   e) analiza zbierania, przechowywania i monitorowania logów systemowych,
6. weryfikacji poprawności realizacji w zakresie:
   a) zarządzania hasłami użytkowników i hasłami administracyjnymi,
   b) instalacji i aktualizacji oprogramowania,
   c) ochrony przed szkodliwym oprogramowaniem,
   d) zabezpieczania procesu pracy zdalnej,
   e) rozwoju systemów informatycznych,
   f) zarządzania zmianami w systemach informatycznych,
   g) przeglądów, konserwacji i napraw systemu informatycznego,
   h) monitorowania bezpieczeństwa systemów informatycznych w tym przy użyciu ZABBIX,
   i) zapisywanie, monitorowanie, zabezpieczanie logów systemowych,
   j) monitorowania pojemności i wydajności systemów informatycznych,
   k) bezpieczeństwa sieci,
   l) zapewnienia legalności oprogramowania,
   m) usuwania danych i niszczenia nośników,

n) synchronizacji zegarów
o) gromadzenia logów

W czasie wykonania i po wykonaniu usługi infrastruktura Zamawiającego musi pozostać w niezmienionej formie, tj. nie może zostać uszkodzona, jak również nie mogą zostać usunięte, zmienione, nadpisane dane znajdujące się w tej infrastrukturze. Zamawiający dopuszcza wykonanie audytu w formie hybrydowej.

Raport

Wynikiem przeprowadzonych obu etapów audytów i testów będzie raport po audytowy w standardzie ENISA zawierający:

1. przedmiot, cel i zakres audytu,
2. datę rozpoczęcia audytu,
3. opis przyjętej metodyki,
4. raport dla kierownictwa obejmujące syntezę wyników audytu i ocenę poziomu spełnienia wymogów RODO, KRI, regulacji wewnętrznych dot. bezpieczeństwa informacji Zamawiającego oraz ocenę bezpieczeństwa systemu informatycznego w tym podsumowanie zidentyfikowanych słabości/nieprawidłowości, a także główne rekomendacje dotyczące poprawy bezpieczeństwa informacji, danych i systemu informatycznego.

5. dokładny opis zidentyfikowanych nieprawidłowości w szczególności
   - wskazujący miejsca, w których występują realne bądź potencjalne problemy z bezpieczeństwem informacji;
   - zawierający wyniki audytów, w tym testów i ich interpretację - ustalenia musza odnosić się do konkretnych przypadków słabości/nieprawidłowości popartych zgromadzonymi dowodami audytowymi, które będą stanowiły załącznik do raportu;
   - zawierający rekomendacje w zakresie eliminacji zidentyfikowanych słabości/nieprawidłowości oraz poprawy poziomu bezpieczeństwa, w tym wskazanie działań korygujących i/lub doskonalących bez lokowania sprzętu lub oprogramowania.
6. analizę rekomendowanych zmian w treści regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI) Zamawiającego wraz z proponowaną treścią nowych (zmienionych lub dodanych) zapisów;
7. wypełniony Formularz weryfikacji dojrzałości organizacji pod kątem cyberbezpieczeństwa zgodny z wzorem Ministra Klimatu i Środowiska
8. datę sporządzenia raportu;
9. imiona i nazwiska audytorów realizujących zadanie oraz ich podpisy.

W terminie do 7 dni od dnia zakończenia audytu wstępnego (diagnostycznego) w siedzibie Zamawiającego Wykonawca prześle w formie elektronicznej w formacie edytowalnym i pdf raport, zaszyfrowany programem 7 ZIP przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 11-znakowym hasłem jednorazowym przesłanym przez alternatywny kanał komunikacji. W terminie do 10 dni od zakończenia audytu końcowego w siedzibie Zamawiającego Wykonawca prześle w formie elektronicznej w formacie edytowalnym i pdf raport, zaszyfrowany programem 7 ZIP przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 11-znakowym hasłem jednorazowym przesłanym przez alternatywny kanał komunikacji.
Wykonawca może dodatkowo przekazać raport końcowy w wersji edytowalnej w formacie A4

Zakres czasowy audytu

1. Czynności audytowe w siedzibie Zamawiającego powinny zakończyć się do 20.09.2022r. audyt wstępny, oraz do 30.11.2022 audyt końcowy w siedzibie u Zamawiającego.

Podstawowe informacje na temat systemów informatycznych Zamawiającego

liczba komputerów:

stacjonarnych - 50

przenośnych - 5

liczba serwerów:

fizycznych - 6

wirtualnych - 4

liczba serwerów:

Windows - 6

Linux - 4

liczba aplikacji bazodanowych - *systemów przetwarzających dane i dane osobowe* -

liczba serwerowni - 2

liczba urządzeń sieciowych - (drukarki, routery , switche, voip, itd.) - 40

liczba Access Point - 5

liczba drukarek sieciowych - 20

liczba podsieci - 3

liczba adresów zewnętrznych - 1

wdrożony Active Directory - nie

liczba serwisów www - 1

Formularz ofertowy

W odpowiedzi na zapytanie ofertowe:

Ja (My), niżej podpisany (ni) .....

działając w imieniu i na rzecz: .....

(pełna nazwa wykonawcy)

.....

(adres siedziby wykonawcy)

składam(y) ofertę cenową dotyczącą: przeprowadzenia audytu **Usługa przeprowadzenia audytu oraz diagnozy poziomu bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) i rekomendacji dotyczących podniesienia tego poziomu jako** dwu etapowego audytu bezpieczeństwa systemu informacyjnego i ochrony danych medycznych zgodnie z dla Operatora Usługi Kluczowej zgodnie z „Wymaganiami dotyczącymi audytu bezpieczeństwa", stanowiącymi załącznik nr 2 do Umowy o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, będącej załącznikiem Nr 2 do Zarządzenia Nr 68/2022/BBIICD Prezesa NFZ z dnia 20 maja 2022 r. ,z wymaganiami ustawy z dnia 13 sierpnia 2018 roku o Krajowym Systemie Cyberbezpieczeństwa , Krajowych Ram Interoperacyjności zgodnie z wymaganiami norm PN ISO IEC 27001, PN ISO IEC 22301

poprzez badanie

a) spełniania wymogów dokumentacyjnych obowiązujących u Zamawiającego jako regulacji wewnętrznych dokumentacji normatywnej i operacyjnej dotyczących usługi kluczowej bezpieczeństwa informacji - dokumentacja SZBI/KRI/BCM , ochrony danych osobowych dokumentacja RODO i ODO ,
b) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych
c) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych

dalej „przedmiotem zamówienia".

Lp.	Usługa	Cena netto całej usługi	Podatek VAT	Cena brutto całej usługi
1	Przeprowadzenie audytu – koszt całkowity usługi			

Termin płatności 21 dni od dostarczenia audytu końcowego

UWAGA!!! *Poniższe oświadczenie wypełniają jedynie wykonawcy mający siedzibę poza terytorium Rzeczypospolitej Polskiej, którzy nie są zarejestrowanymi podatnikami podatku VAT na terytorium RP oraz w przypadku, gdy w wyniku świadczenia usług lub realizowanej dostawy towarów na Zamawiającym będzie ciążył obowiązek odprowadzenia podatku VAT zgodnie z przepisami o podatku od towarów i usług.*

Oświadczam(y) że wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, w zakresie następujących towarów/usług:

Nazwa towaru/usługi, których dostawa/świadczenie będzie prowadzić do powstania obowiązku podatkowego	wartość bez kwoty podatku od towarów i usług.

1. Oświadczam, że***:

☐ wykonam zadanie siłami własnymi

☐ przewiduję wykonanie zadania przy pomocy podwykonawcy (ów)

Zakres zlecany Podwykonawcy	**Nazwa Podwykonawcy**

Oświadczam(y), że:

- jestem(śmy) ***

☐ mikro przedsiębiorcą,

☐ małym przedsiębiorcą

☐ średnim przedsiębiorcą

(zaznaczyć, jeżeli wykonawca jest mikro-, małym lub średnim przedsiębiorcą w rozumieniu ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców Dz. U. z 2019 r., poz. 1292 z późn. zm)

Wynagrodzenie zaspokaja wszelkie roszczenia Wykonawcy z tytułu wykonania umowy, w tym roszczenia z tytułu przeniesienia na Zamawiającego autorskich praw majątkowych do wszystkich utworów w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231, z późn. zm.), powstałych w związku z jej wykonaniem oraz z tytułu zezwolenia na wykonanie zależnego prawa autorskiego oraz przeniesienia prawa do zezwalania na wykonanie zależnego prawa audytorskiego.

1. Przedmiot zamówienia realizowany będzie zgodnie z wytycznymi określonymi w zapytaniu ofertowym oraz opisie przedmiotu zamówienia.
2. Oświadczam(y), że:
   1) posiadamy niezbędną wiedzę i doświadczenie oraz dysponujmy odpowiednimi osobami przygotowanymi do wykonania przedmiotu zamówienia,

2) w podanej cenie wliczyliśmy wszystkie koszty związane z pełną i terminową realizacją zamówienia, zgodnie z warunkami określonymi w zapytaniu ofertowym oraz opisie przedmiotu zamówienia,
3) zostaliśmy zapoznani z zakresem przedmiotu zamówienia oraz otrzymaliśmy od Zamawiającego wyczerpujące informacje i wyjaśnienia potrzebne do sporządzenia oferty,
4) jesteśmy związani niniejszą ofertą przez okres 30 dni od upływu terminu składania ofert
5) Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2022 poz. 835)

....

Miejscowość, data

Podpis osoby/osób uprawnionej/uprawnionych do reprezentowania Wykonawcy (pieczątki)

Załącznik nr 3 do Zapytania ofertowego
Sp/AZP/382/13/poza/2022

Składający ofertę:

Wykonawca (pełna nazwa albo imię i nazwisko)	
Siedziba/miejsce zamieszkania i adres jeżeli jest miejscem wykonywania działalności Wykonawcy	

Wykaz usług

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy w okresie od 01.01.2018 r. wykonali (tj. świadczyli, zrealizowali, zakończyli) co najmniej 5 usług obejmujących swoim zakresem:

- audyt bezpieczeństwa informacji zgodnie z wymaganiami SZBI/KRI (audyt SZBI/ KRI),
- audyt bezpieczeństwa systemów informatycznych, w tym testów penetracyjnych,

Lp.	Przedmiot zamówienia	Opis
1	**Zamawiający** *(podmiot, który zlecał wykonanie usługi)*	(nazwa i adres)
	Nazwa zamówienia oraz krótki opis przedmiotu zamówienia	
	Data wykonania usługi (należy podać zakończenia wskazanej usługi)	od ...../...../..... (dzień / miesiąc / rok)
	Wartość zamówienia w PLN netto	
	Dokument potwierdzający należyte wykonanie wyżej wymienionej usługi *	
2	**Zamawiający** *(podmiot, który zlecał wykonanie usługi)*	(nazwa i adres)
	Nazwa zamówienia oraz krótki opis przedmiotu zamówienia	
	Data wykonania usługi (należy podać zakończenia wskazanej usługi)	od ...../...../..... (dzień / miesiąc / rok)
	Wartość zamówienia w PLN netto	
	Dokument potwierdzający należyte wykonanie wyżej wymienionej usługi *	
3	**Zamawiający** *(podmiot, który zlecał wykonanie usługi)*	(nazwa i adres)

	Nazwa zamówienia oraz krótki opis przedmiotu zamówienia	
	Data wykonania usługi (należy podać zakończenia wskazanej usługi)	od ...../...../..... (dzień / miesiąc / rok)
	Wartość zamówienia w PLN netto	
	Dokument potwierdzający należyte wykonanie wyżej wymienionej usługi *	

Lp.	Przedmiot zamówienia	Opis
2	**Zamawiający** *(podmiot, który zlecał wykonanie usługi)*	(nazwa i adres)
	Nazwa zamówienia oraz krótki opis przedmiotu zamówienia	
	Data wykonania usługi (należy podać zakończenia wskazanej usługi)	od ...../...../..... (dzień / miesiąc / rok)
	Wartość zamówienia w PLN netto	
	Dokument potwierdzający należyte wykonanie wyżej wymienionej usługi *	

Lp.	Przedmiot zamówienia	Opis
3	**Zamawiający** *(podmiot, który zlecał wykonanie usługi)*	(nazwa i adres)
	Nazwa zamówienia oraz krótki opis przedmiotu zamówienia	
	Data wykonania usługi (należy podać zakończenia wskazanej usługi)	od ...../...../..... (dzień / miesiąc / rok)
	Wartość zamówienia w PLN netto	
	Dokument potwierdzający należyte wykonanie wyżej wymienionej usługi *	

....., dn. .....

.....
Podpis osoby/osób uprawnionej/uprawnionych
do reprezentowania Wykonawcy (pieczątki)

UWAGA
* skany referencji i/lub protokołów odbioru potwierdzających wykonanie danej usługi

Załącznik nr 4 do Zapytania ofertowego
Sp/AZP/382/13/poza/2022

Składający ofertę:

Wykonawca (pełna nazwa albo imię i nazwisko)	
Siedziba/miejsce zamieszkania i adres jeżeli jest miejscem wykonywania działalności Wykonawcy	

WYKAZ OSÓB

które będą uczestniczyć w wykonywaniu zamówienia

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy dysponują zespołem audytowym składającym się przynajmniej z 3 osób zatrudnionych o umowę o prace i które będą realizowały audyt u Zamawiającego, w tym:

W przypadku większej liczby audytorów realizujących usługę u Zamawiającego należy wykazać wszystkie osoby, które będą uczestniczyły w realizacji audytu.

Pierwsza osoba – audytor wiodący

Lp.	Doświadczenie zawodowe
1.	jedna osoba z zespołu musi posiadać certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji wg normy ISO 27001 wskazanymi jako uprawnione do audytowaniu w Rozporządzeniu Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, ukończyła studia podyplomowe bezpieczeństwa informacji lub równoważny kurs kwalifikacyjny oraz brała udział w charakterze audytora wiodącego w co najmniej 9 audytach KRI, (należy wskazać certyfikat, nazwę i adres podmiotu, który wydał certyfikat oraz datę wydania/ jego ważność): Imię nazwisko ..... Przeprowadzone audyty KRI (audytowany podmiot, data przeprowadzenia audytu): 1. ..... 2. ..... 3. ..... 4. ..... 5. ..... Informacja o podstawie dysponowania osobami w celu realizacji zamówienia .....

Druga osoba

Lp.	Doświadczenie zawodowe
1.	co najmniej jedna osoba z zespołu musi posiadać certyfikat audytora wiodącego lub wewnętrznego wg normy ISO 27701, ukończyła studia podyplomowe ochrony danych osobowych lub równoważny kurs kwalifikacyjny oraz brała udział w

	charakterze audytora wewnętrznego lub wiodącego w co najmniej 5 audytach KRI/SZBI, Imię nazwisko ..... Przeprowadzone audyty KRI (audytowany podmiot, data przeprowadzenia audytu): 1. ..... 2. ..... 3. ..... 4. ..... 5. ..... Informacja o podstawie dysponowania osobami w celu realizacji zamówienia .....

Trzecia osoba

Lp.	Doświadczenie zawodowe
1.	co najmniej jedna osoba z zespołu jest specjalistą ds. bezpieczeństwa IT, który brał udział w charakterze pentestera w co najmniej 5 audytach bezpieczeństwa IT z zastosowaniem testów penetracyjnych oraz posiada przynajmniej jeden z następujących certyfikatów: *- Certified Ethical Hacker (CEH),* *- Certified IT Security Specjalist Training (CSST)* *- Certified Penetration Testing Engineer (CPTE),* *- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN),* *- Offensive Security Certified Professional (OSCP),* *- Offensive Security Certified Expert (OSCE),* *- Certified Information Security Manager (CISM),* *- Certified in Risk and Information Systems Control (CRISC),* *- Certified in the Governance of Enterprise IT (CGEIT),* *- Certified Information Systems Security Professional (CISSP),* *- Certified IT Security Specjakist (CSP)* *- Certified Information Texchnical Securitu Specialist jako(CITSS),* *- Systems Security Certified Practitioner (SSCP)* *- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.* Imię nazwisko ..... Przeprowadzone audyty KRI (audytowany podmiot, data przeprowadzenia audytu): 1. ..... 2. ..... 3. ..... 4. ..... 5. ..... Informacja o podstawie dysponowania osobami w celu realizacji zamówienia .....

Czwarta osoba (opcja)

Lp.	Doświadczenie zawodowe
1.	Imię nazwisko ..... Przeprowadzone audyty KRI (audytowany podmiot, data przeprowadzenia audytu): 1. ..... 2. ..... 3. ..... 4. ..... 5. ..... Informacja o podstawie dysponowania osobami w celu realizacji zamówienia .....

....., dn. .....

.....

Podpis osoby/osób uprawnionej/uprawnionych do reprezentowania Wykonawcy (pieczątki)

* Podstawa do dysponowania każdą z osób wskazaną w wykazie, np. umowa o pracę, umowa zlecenia. W przypadku, gdy wykonawca polega na osobach innych podmiotów zobowiązany jest udowodnić zamawiającemu, że będzie dysponował tymi osobami, np. przedstawiając pisemne zobowiązanie innych podmiotów do udostępnienia osób zdolnych do wykonania zamówienia.

Klauzula informacyjna Oferenci

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (EU) 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 informuję, że:

Administratorem Pana/Pani danych osobowych jest Szpital w Pyskowicach Sp. z o.o. – 44-120 Pyskowice, ul . Szpitalna 2; nr.tel. 32 233-24-24

Osobą odpowiedzialną za ochronę danych osobowych w Szpitalu w Pyskowicach Sp. z o.o. jest **Inspektor Ochrony Danych** mgr. Iwona Reszka , kontakt: adres email:Iod@szpitalpyskowice.pl, telefon: 32 233-24-24

Podstawa prawna, zakres i cel przewarzania danych osobowych :

a) przetwarzanie jest niezbędne do wypełniania zobowiązań umownych wobec Państwa, jeżeli są lub będą Państwo stroną umowy zawartej ze Spółką (art. 6 ust. 1 lit. b RODO);

b) przetwarzanie jest niezbędne do podjęcia czynności przed zawarciem umowy (art. 6 ust. 1 lit. b RODO) – w zakresie danych osobowych osób prowadzących działalność gospodarczą, z którymi Spółki mogą zawrzeć umowę;

c) w zakresie danych osobowych zawartych w dokumentach podlegających archiwizacji na podstawie przepisów prawa;

d) przetwarzanie jest niezbędne dla realizacji uzasadnionych interesów Szpitala lub strony trzeciej (art. 6 ust. 1 lit. f RODO).

e) dla celów ustalania lub dochodzenia przez Szpital roszczeń cywilnoprawnych w ramach prowadzonej działalności, a także obrony przed takimi roszczeniami – przez odpowiednie okresy przedawnienia takich roszczeń, tj. co do zasady nie dłużej niż przez 10 lat od zajścia zdarzenia skutkującego powstaniem roszczenia.

F) w celach wykazania spełnienia obowiązków wynikających z rozliczenia dofinansowania ze środków publicznych - przez odpowiednie okresy wskazane w umowach oraz we właściwych przepisach regulujących udzielanie dofinansowania – co do zasady są to okresy 5-letnie.

Podczas przetwarzania danych osobowych na tej podstawie zawsze staramy się zachować równowagę między naszym uzasadnionym interesem a Państwa prywatnością.

Przykłady interesów:

- weryfikacja złożonych ofert oraz wniosków o dopuszczenie do udziału w Postępowaniu;

- umożliwienie Spółce kontaktu z Oferentami;

- weryfikacja potencjału i doświadczenia Oferenta i możliwości wykorzystania informacji w innych Postępowaniach (tworzenie bazy dostawców);

- przechowywanie dokumentacji dla celów wykazania spełnienia obowiązków wynikających z rozliczenia dofinansowania ze środków publicznych; v. zapobieganie oszustwom oraz działalności przestępczej;

Zakres zbieranych Danych.

Dane podane przez Oferenta:

a) imię i nazwisko, firma, adres prowadzenia działalności gospodarczej oraz adresy korespondencyjne,

b) numery posiadane we właściwych rejestrach (np. numer NIP lub REGON, numer PESEL),

c) dane kontaktowe, takie jak adres e-mail lub numer telefonu lub faxu,

d) stanowisko zajmowane przez Państwa w ramach Państwa organizacji lub pełnioną funkcję,

e) posiadane doświadczenie lub uprawnienia;

f) inne dane zawarte w oświadczeniach Oferenta lub referencjach przedstawianych w danym Postępowaniu, w tym w szczególności specyficzne numery identyfikacyjne niebędące numerami nadawanymi powszechnie (np. numer legitymacji służbowej lub zawodowej, numer rachunku bankowego, tytuł zawodowy, wykształcenie).

Konsekwencją niepodania danych jest brak możliwości uczestniczenia w Postępowaniu.

Dane pozyskane z innych źródeł :

Możemy pozyskiwać Państwa dane osobowe z publicznych źródeł, takich jak rejestry przedsiębiorców CEIDG lub KRS w celu weryfikacji podanych przez Państwa informacji. Zakres przetwarzanych danych będzie w takim przypadku ograniczony do danych dostępnych publicznie w odpowiednich rejestrach. Możemy również pozyskiwać Państwa dane osobowe od podmiotów, w których są Państwo zatrudnieni, lub którego są Państwo reprezentantami. Zakres przetwarzanych danych obejmie w takim przypadku informacje konieczne do prowadzenia Postępowania oraz kontaktu z Oferentem, np. informacje o ustaniu Państwa zatrudnienia u danego podmiotu lub zmianie danych kontaktowych. Możemy pozyskiwać także dane osobowe podwykonawców Oferentów od Oferentów, którzy dostarczyli Szpitalowi takie dane w ramach Postępowania.

· odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1 ustawy z dnia 11 wrzesień 2019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.), dalej „ustawa Pzp"'

· Pani/Pana 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;

· obowiązek podania przez Pani/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z

udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

· w odniesieniu do Pani/Pana danych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;

· **Posiada Pani/Pan prawo do:**

- na podstawie art. 15 RODO prawo do dostępu do danych osobowych Pani/Pana dotyczących,

- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych,

- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO,

- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO,

· **Nie przysługuje Pani/Panu prawo do:**

- w związku z art. 17 ust. 3 lit. b), d) lub e) RODO prawo do usunięcia danych osobowych,

- prawo do przenoszenia danych osobowych, o których mowa w art. 20 RODO,

- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c) RODO.

LISTA KONTROLNA DLA POTENCJALNYCH PODMIOTÓW PRZETWARZAJĄCYCH

DOTYCZĄCA STOPNIA SPEŁNIENIA WYMAGAŃ TECHNICZNYCH I ORGANIZACYJNYCH WOBEC PODMIOTÓW, KTÓRYM POWIERZA SIĘ PRZETWARZANIE DANYCH OSOBOWYCH

Szanowni Państwo!

Zwracamy się z prośbą o wypełnienie niniejszej listy kontrolnej, która pozwoli nam ocenić czy Państwa firma zapewnia wystarczającą gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, dzięki którym przetwarzanie danych osobowych będzie zgodne z przepisami RODO i będzie chroniło prawa osób, których dotyczą dane.
Jednocześnie informujemy, że dane przekazane nam przez Państwa będą dostępne wyłącznie dla osób upoważnionych. Informacje przekazane przez Państwa są traktowane jako poufne i nie będą udostępniane osobom trzecim.

Dane firmy	
Nazwa Firmy:	
Adres:	
Wypełniający ankietę	
Imię i Nazwisko:	
Stanowisko:	
Data wypełnienia:	

Lp.	PYTANIE	TAK / NIE/ NIE DOTYCZY	UWAGI
1	Czy przeprowadzają Państwo udokumentowaną analizę ryzyka i uwzględniają w niej ryzyka wynikające z przypadkowego lub niezgodnego z prawem: - zniszczenia, - utraty, - modyfikacji, - nieuprawnionego ujawnienia lub dostępu do danych?		
2	Czy w związku z przetwarzaniem danych na zlecenie Administratora zidentyfikowali Państwo zagrożenie/a mogące z dużym prawdopodobieństwem skutkować wysokim ryzykiem naruszenia praw lub wolności osób fizycznych? Jeżeli tak należy dokładnie je opisać w polu Uwagi.		
3	Czy wdrożyli Państwo odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanym przez Państwa ryzykom zgodnie z art. 32 RODO?		
4	Jakie środki techniczne stosują Państwo w celu zapewnienia odpowiedniego poziomu bezpieczeństwa dla ochrony danych? - proszę wybrać (postawić znak X) w polu Uwagi lub wpisać inne przez		[ ] pomieszczenia zabezpieczone drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi) [ ] pomieszczenia zabezpieczone drzwiami o podwyższonej odporności ogniowej >= 30 min

	Państwa stosowane. Mamy świadomość, że każda z firm dobierając zabezpieczenia uwzględnia stan wiedzy technicznej, koszt ich wdrażania, ryzyko naruszenia praw lub wolności osób fizycznych oraz charakter, zakres, kontekst i cele przetwarzania danych osobowych. Dlatego też **nie wymagamy wdrożenia wszystkich zabezpieczeń** uwzględnionych w polu Uwagi.		[ ] pomieszczenia zabezpieczone drzwiami o podwyższonej odporności na włamanie – drzwi klasy C [ ] okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej [ ] pomieszczenia, w których przetwarzane są dane wyposażone są w system alarmowy/przeciwwłamaniowy [ ] dostęp do pomieszczeń objęty jest systemem kontroli dostępu [ ] dostęp do pomieszczeń kontrolowany jest przez system monitoringu wizyjnego [ ] dostęp do pomieszczeń jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony [ ] dostęp do pomieszczeń przez całą dobę jest nadzorowany przez służbę ochrony [ ] pracownicy posiadają dostęp jedynie do pomieszczeń, do których jest to niezbędne ze względu na realizowane obowiązki [ ] dane w formie papierowej przechowywane są w zamkniętej, szafie lub sejfie, kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej szafie lub sejfie, [ ] pomieszczenia, w których przetwarzane są dane są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy [ ] dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów [ ] zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania [ ] dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła [ ] dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena [ ] zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity [ ] żyto system Firewall do ochrony dostępu do sieci komputerowej [ ] wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych w systemie informatycznym (logi) [ ] zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w systemie

			informatycznym zbioru danych osobowych [ ] dostęp do danych osobowych w systemie informatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (oprócz hasła do systemu operacyjnego) [ ] zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu służącego do przetwarzania danych [ ] systemy wymuszają jakość haseł użytkowników (różne grupy znaków, długość haseł) [ ] zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika [ ] zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji [ ] dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia [ ] firma korzysta z systemów operacyjnych, które mają aktualne wsparcie producenta [ ] firma monitoruje w aktywny sposób działanie serwerów, ruch na serwerach, nieautoryzowane próby wejścia na serwer, próby złamania zabezpieczeń [ ] firma prowadzi dziennik administracyjny systemu i prowadzi w nim ewidencję zdarzeń i czynności administracyjnych [ ] firma wykonuje kopie zapasowe danych i konfiguracji systemów teleinformatycznych oraz weryfikuje regularnie możliwość ich odtworzenia [ ] firma przechowuje kopie zapasowe systemów w innej lokalizacji niż dane produkcyjne [ ] w firmie przeprowadzane są testy penetracyjne/audyty bezpieczeństwa systemów teleinformatycznych [ ] w przypadku pracy zdalnej wykorzystuje się bezpieczne kanały komunikacji – VPN [ ] w firmie nadzoruje się wykorzystywanie pamięci USB [ ] w firmie zabronione jest wykorzystanie nieautoryzowanych nośników USB [ ] INNE – proszę wpisać jakie ....
5	Jakie środki organizacyjne stosują Państwo w celu zapewnienia odpowiedniego poziomu bezpieczeństwa dla ochrony danych? -		[ ] w firmie jest wdrożona niezbędna dokumentacja w obszarze bezpieczeństwa informacji i ochrony danych osobowych zgodnie z mającymi zastosowanie regulacjami prawnymi (polityki, procedury, instrukcje itp.) - wpisać jakie

	proszę wybrać (postawić znak X) w polu Uwagi lub wpisać inne przez Państwa stosowane. Mamy świadomość, że każda z firm dobierając zabezpieczenia uwzględnia stan wiedzy technicznej, koszt ich wdrażania, ryzyko naruszenia praw lub wolności osób fizycznych oraz charakter, zakres, kontekst i cele przetwarzania danych osobowych. Dlatego też **nie wymagamy wdrożenia wszystkich zabezpieczeń** uwzględnionych w polu Uwagi.		.... [ ] firma posiada certyfikowany system zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001 [ ] prowadzona jest ewidencja osób upoważnionych do przetwarzania danych [ ] prowadzone są regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych [ ] INNE – proszę wpisać jakie ....
6	Czy posiadają Państwo zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania powierzonych danych?		
7	Czy posiadają Państwo zdolność do szybkiego przywrócenia dostępności danych w razie incydentu?		
8	Czy prowadzą Państwo regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych zabezpieczeń?		
9	Czy Państwa pracownicy, którzy będą przetwarzać powierzone dane mają wydane upoważnienia do przetwarzania danych osobowych?		
10	Czy osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy?		
11	Czy osoby upoważnione do przetwarzania danych zostały odpowiednio przeszkolone w zakresie ochrony danych osobowych?		
12	Czy są Państwo w stanie wspomagać administratora poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw?		
13	Czy są Państwo w stanie wspomagać administratora w wywiązywaniu się z obowiązków związanych z zabezpieczaniem danych określonych w art. 32-36 RODO?		
14	Czy dysponują Państwo środkami, które pozwalają na usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie ich wszelkich istniejących kopii?		

15	Czy zamierzają Państwo przy przetwarzaniu powierzonych przez nas danych osobowych korzystać z podprocesora (podwykonawcy)? Jeżeli tak proszę w polu Uwagi wskazać jakiego/jakich i w jakim zakresie.		
16	Jeżeli korzystają Państwo z podprocesora, czy ocenili Państwo, że zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych zgodnie z art. 28 ust. 1 RODO?		
17	Jeżeli korzystają Państwo z podprocesora, czy mają Państwo podpisaną z nim umowę powierzenia danych osobowych?		
18	Czy są Państwo w stanie zrezygnować ze współpracy z którymś ze swoich podmiotów przetwarzających, jeśli administrator danych nie wyrazi na nich zgody?		
19	Czy umożliwią Państwo administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji?		
20	Czy potrafią Państwo prawidłowo identyfikować naruszenia ochrony danych osobowych zgodnie z art. 33 RODO?		
21	Czy Państwa pracownicy są świadomi spoczywającej na nich odpowiedzialności dotyczącej możliwie najszybszego zgłaszania zdarzeń związanych z bezpieczeństwem informacji, w tym danych osobowych?		
22	Czy Państwa pracownicy posiadają wiedzę komu w Państwa firmie powinni zgłaszać incydenty bezpieczeństwem informacji, w tym danych osobowych?		
23	Czy są Państwo w stanie informować administratora o naruszeniach ochrony danych osobowych, do których u Państwa dojdzie w ciągu 24 godzin od stwierdzenia naruszenia?		
24	Czy posiadają Państwo wiedzę na temat prowadzenia rejestru kategorii czynności przetwarzania zgodnie z art. 30 RODO?		
25	Czy wyznaczyli Państwo inspektora ochrony danych?		
26	Czy jesteście Państwo gotowi podpisać umowę powierzenia przygotowaną przez SP Tarnów		
27	Czy przekazujecie Państwo powierzone		

	dane do państwa trzeciego? Jeżeli tak - w oparciu o jaką podstawę prawną? (pole Uwagi)		

Załącznik nr 6 do Umowy nr .....

Umowa powierzenia przetwarzania danych osobowych

zawarta w Pyskowicach w dniu ..... r. pomiędzy:
.....
ul. ....., ..., NIP: ....., Regon: ....., reprezentowanymi przez
..... - .....
w dalszej części niniejszej umowy zwanym **„Administratorem danych"**
a

z siedzibą w .....
reprezentowaną przez:

w dalszej części niniejszej umowy zwanym **„Podmiotem przetwarzającym"**

łącznie zwanymi dalej „Stronami"

§1
Przedmiot Umowy

1. Administrator i Podmiot przetwarzający oświadczają, że w dniu ..... zawarli umowę nr ..... w przedmiocie przeprowadzenia audytu spełniania wymogów KRI, RODO, obowiązujących u Zamawiającego regulacji wewnętrznych dot. bezpieczeństwa informacji oraz systemu informatycznego Zamawiającego zwaną dalej Umową Główną, z tytułu której będą przetwarzane dane osobowe.
2. Niniejsza - akcesoryjna względem Umowy Głównej - Umowa powierzenia przetwarzania danych osobowych, zwana dalej Umową, reguluje wzajemny stosunek Stron i obowiązki w zakresie przetwarzania danych osobowych wynikających z zawartej Umowy Głównej.

§2
Definicje

Dla potrzeb niniejszej Umowy, o ile z treści i celu Umowy nie wynika inaczej, przyjmuje się następujące znaczenie dla poniżej wymienionych sformułowań:

1) **RODO** - Rozporządzenie 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;
2) **Ustawa** - obowiązująca ustawa o ochronie danych osobowych;
3) **Administrator danych** - 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;

4) **Podmiot przetwarzający** - w rozumieniu art. 4 pkt. 8 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;
5) **Inny podmiot przetwarzający** - podmiot, któremu Podmiot przetwarzający w imieniu Administratora powierzył dane osobowe do dalszego przetwarzania w całości lub częściowo.
6) **Dane osobowe** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7) **Dane zwykłe -** oznaczają dane osobowe podstawowe, inne niż dane wrażliwe;
8) **Dane wrażliwe** - oznaczają dane osobowe podlegające szczególnej ochronie, o których mowa w art. 9 ust. 1 oraz art. 10 RODO;
9) **Dane poufne** - wszelkie informacje, dane, materiały, dokumenty i dane osobowe otrzymane od Administratora i od współpracujących z nim osób oraz dane uzyskane w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej dotyczące Administratora i przedmiotu Umowy;
10) **Organ nadzorczy** - Prezes Urzędu Ochrony Danych Osobowych;
11) **Umowa** - niniejsza umowa;
12) **Przetwarzanie danych osobowych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

§3
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 RODO dane osobowe do przetwarzania, na zasadach i w celu określonym w Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe na polecenie Administratora zgodnie z Umową, RODO, Ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO i daje gwarancję wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których

   dane są przetwarzane na podstawie Umowy.
4. Podmiot przetwarzający oświadcza, że przetwarzanie powierzonych danych osobowych będzie się odbywało na terenie Europejskiego Obszaru Gospodarczego, z zastrzeżeniem § 8 ust. 2.

5. Upoważnienia do przetwarzania danych osobowych pracownikom Podmiotu przetwarzającego którymi Podmiot przetwarzający posługuje się przy wykonywaniu niniejszej umowy nadaje Podmiot przetwarzający .

§4

Zakres i cel przetwarzania danych

1. Cel i zakres powierzenia przetwarzania danych osobowych wynika bezpośrednio i ogranicza się wyłącznie do zadań wynikających z zawartej Umowy Głównej, tj.: przeprowadzenia audytu spełniania wymogów KRI, RODO, obowiązujących u Zamawiającego regulacji wewnętrznych dot. bezpieczeństwa informacji oraz systemu informatycznego Zamawiającego. podmiot przetwarzający będzie przetwarzał, powierzone na podstawie Umowy:
   a) dane zwykłe, dotyczące pracowników Zamawiającego, kontrahentów Zamawiającego, klientów Zamawiającego (w tym m.in.: uczestników imprez sportowych i rekreacyjnych, osób korzystających z bazy sportowo - rekreacyjnej, gości hotelowych), składających skargi, wnioski oraz innego rodzaju pisma do Zamawiającego, także w wersji elektronicznej w tym zawarte w jego systemach informatycznych oraz dokumentacji papierowej.
   b) dane wrażliwe, dotyczące pracowników Zamawiającego, klientów Zamawiającego (w tym m. in.: uczestników imprez sportowych i rekreacyjnych, osób korzystających z bazy sportowo - rekreacyjnej, gości hotelowych) w tym zawarte w jego systemach informatycznych oraz dokumentacji papierowej.
2. Dane osobowe będą przetwarzane w formie elektronicznej w systemie informatycznym oraz w formie papierowej.

§5

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych) poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa zgodnie art. 32 RODO. Wykaz minimalnych środków, które zobowiązany jest wdrożyć Podmiot przetwarzający został określony w załącznik nr 1 do Umowy.
2. Przetwarzanie danych osobowych przez Podmiot przetwarzający będzie odbywać się wyłącznie na udokumentowane polecenie Administratora.
3. Za udokumentowane polecenie uznaje się zadania zlecone do wykonywania Podmiotowi przetwarzającemu na podstawie Umowy oraz Umowy Głównej.
4. Podmiot przetwarzający zobowiązuje się do:
   a) nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy oraz prowadzenia ich ewidencji,
   b) zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

c) zobowiązania osób upoważnionych do przetwarzania danych osobowych do zachowania tych danych oraz sposobu ich zabezpieczenia w tajemnicy, także po zakończeniu zatrudnienia,
d) prowadzenia rejestru wszystkich kategorii czynności przetwarzania, wykonywanych w imieniu Administratora zgodnie z art. 30 ust. 2 RODO,
e) powiadamiania Administratora o każdym naruszeniu ochrony danych osobowych, nawet jeśli w jego ocenie nie jest ono na tyle poważne, by podlegać notyfikacji do Organu nadzorczego zgodnie z RODO, bez zbędnej zwłoki, jednak nie później niż w ciągu 24 godzin od jego wystąpienia. Powiadomienie nastąpi poprzez przesłanie wypełnionego formularza „Zgłoszenie naruszenia danych osobowych" stanowiącego załącznik nr 2 do Umowy oraz dołączenie do zgłoszenia wszelkiej niezbędnej dokumentacji dotyczącej naruszenia, tak by umożliwić Administratorowi spełnienie obowiązku powiadomienia Organu nadzorczego.
Jeżeli przekazanie wszystkich powyższych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji Podmiot przetwarzający przekazuje je Administratorowi bez zbędnej zwłoki.
f) wdrożenia dokumentacji dotyczącej ochrony informacji, w tym danych osobowych zgodnej z RODO i Ustawą.

5. Po zakończeniu świadczenia usługi realizowanej na podstawie Umowy Głównej Podmiot przetwarzający, w zależności od decyzji Administratora, zobowiązany jest w terminie 7 dni do zwrotu danych w formacie określonym przez Administratora lub usunięcia powierzonych danych osobowych ze wszystkich nośników, zarówno w wersji elektronicznej jak i papierowej oraz do podjęcia stosownych działań w celu wyeliminowania możliwości dalszego przetwarzania danych powierzonych na podstawie Umowy, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
W przypadku usunięcia powierzonych danych osobowych, Podmiot przetwarzający zobowiązuje się w ciągu 7 dni od daty ich usunięcia przekazać Administratorowi protokół zniszczenia powierzonych danych osobowych.
6. Biorąc pod uwagę charakter przetwarzania, Podmiot przetwarzający pomaga nieodpłatnie Administratorowi poprzez odpowiednie środki techniczne organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.
7. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga nieodpłatnie Administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO.
8. Podmiot przetwarzający zobowiązuje się przekazać Administratorowi informację o wniesieniu żądań wprost do Podmiotu przetwarzającego przez osoby, których dane są przetwarzane w związku z realizacją niniejszej Umowy w terminie do 48 godzin od otrzymania żądania.

§6
Obowiązki informacyjne Podmiotu przetwarzającego wobec Administratora

1. Podmiot przetwarzający zobowiązuje się niezwłocznie przekazywać wszelkie informacje dotyczące zobowiązań publicznych w stosunku do policji i organów ścigania oraz służb specjalnych w zakresie przekazywania im dostępu do danych osobowych powierzonych przez Administratora, a także do

niezwłocznego informowania Administratora o wszelkich pismach oraz działaniach podejmowanych przez policję, organy ścigania oraz służby specjalne pozostających w związku z realizacją Umowy.

2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o:
   a) prowadzonym postępowaniu, w szczególności administracyjnym lub sądowym, prowadzonym wobec Podmiotu przetwarzającego oraz współpracujących z nim Innych podmiotów przetwarzających w związku z przetwarzaniem danych osobowych określonych w Umowie,
   b) wydaniu decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych danych osobowych, skierowanych do Podmiotu przetwarzającego lub współpracujących z nim Innych podmiotów przetwarzających,
   c) wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych, realizowanych wobec Podmiotu przetwarzającego lub współpracujących z nim Innych podmiotów przetwarzających, w szczególności tych prowadzonych przez Organ nadzorczy, a także o każdym piśmie tego podmiotu, dotyczącym składania wyjaśnień w zakresie powierzonych danych osobowych.
3. Podmiot przetwarzający oświadcza, że w przypadku kontroli Organu nadzorczego, prowadzonej u Administratora dotyczącej przetwarzania powierzonych danych osobowych, będzie przekazywał Administratorowi niezbędne informacje i wyjaśnienia.

§7
Prawo sprawdzenia

1. Administrator ma prawo do przeprowadzania audytów, w tym inspekcji, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy.

2. Podmiot przetwarzający przyjmuje do wiadomości, iż w związku z realizacją Umowy może być poddany sprawdzeniu zgodności przetwarzania danych z obowiązującymi przepisami prawa przez uprawnione podmioty tj. personel Administratora lub niezależnego audytora działającego na zlecenie Administratora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych Podmiotu przetwarzającego.
3. Na wniosek Administratora Podmiot przetwarzający jest zobowiązany do udzielenia informacji na temat przetwarzania powierzonych danych osobowych, w tym na temat zastosowanych przy przetwarzaniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w terminie 7 dni od otrzymania wniosku.
4. Administrator realizować będzie prawo sprawdzenia, w siedzibie Podmiotu przetwarzającego i/lub miejscach przetwarzania, w godzinach pracy Podmiotu przetwarzającego i z minimum 3 dniowym jego uprzedzeniem.
5. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas realizacji prawa sprawdzenia w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.
6. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§8
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający oświadcza, że nie będzie powierzać danych osobowych objętych Umową do dalszego przetwarzania Innym podmiotom przetwarzającym, a w przypadku takiej konieczności zastosuje się do poniższych postanowień określonych przez Administratora:
   a) Podmiot przetwarzający może powierzyć dane osobowe objęte Umową do dalszego przetwarzania Innym podmiotom przetwarzającym jedynie w celu wykonania Umowy po uzyskaniu uprzedniej pisemnej zgody Administratora,
   b) Podmiot przetwarzający może powierzyć dane osobowe objęte Umową do dalszego przetwarzania wyłącznie takim Innym podmiotom przetwarzającym, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie przez te pomioty przetwarzające danych osobowych, spełniało wymogi RODO i chroniło prawa osób, których dane są przetwarzane na podstawie Umowy,
   c) Dalsze powierzenie przetwarzania danych osobowych przez Podmiot przetwarzający Innemu podmiotowi przetwarzającemu wymaga, pod rygorem nieważności, zawarcia umowy w formie pisemnej,
   d) Umowa, o której mowa w lit. b) musi zawierać wszystkie zobowiązania określone w niniejszej Umowie oraz precyzować czas, charakter i cel przetwarzania danych z uwzględnieniem zakresu (lub kategorii) przetwarzanych danych.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

Jeżeli zgodnie z §8 ust. 2 podmiot przetwarzający korzysta z usług Innego podmiotu przetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu administratora), które wiążą się z przekazywaniem danych osobowych do państw trzecich w rozumieniu rozdziału V RODO, administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V RODO za pomocą standardowych klauzul umownych przyjętych przez Komisję UE zgodnie z art. 46 ust. 2 RODO (decyzja wykonawcza Komisji UE 2021/914) pod warunkiem że spełnione są warunki stosowania tych standardowych klauzul umownych. Za warunki, o których mowa powyżej, uznaje się przeprowadzenie przez Podmiot przetwarzający szczegółowej analizy prawa państwa trzeciego, w szczególności pod kątem obowiązywania egzekwowalnych praw osób, których dane dotyczą, skutecznych środków ochrony prawnej oraz warunków dostępu do przekazywanych danych ze strony organów władzy publicznej (np. służb specjalnych) państwa trzeciego.

§9
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający ponosi odpowiedzialność za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do

przetwarzania danych osobowych osobom nieupoważnionym.

2. Podmiot przetwarzający odpowiada za szkody poniesione przez osobę, której dotyczą przetwarzane dane osobowe, Administratora oraz osoby trzecie, spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada Umowa, gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom jak i za te szkody, które powstały na skutek działań niezgodnych z przepisami RODO.
3. Podmiot przetwarzający ponosi odpowiedzialność za działania i zaniechania swoich pracowników oraz Innych podmiotów przetwarzających, którymi posługuje się przy wykonywaniu Umowy, jak za własne działania i zaniechania.
4. W przypadku naruszenia przepisów Ustawy lub RODO w ramach realizacji Umowy z przyczyn leżących po stronie Podmiotu przetwarzającego, w następstwie którego Administrator zostanie zobowiązany do wypłaty odszkodowania lub ukarany grzywną, prawomocnym wyrokiem lub decyzją właściwego organu, Podmiot przetwarzający zobowiązuje się do zwrócenia równowartości odszkodowani, kary pieniężnej lub grzywny zapłaconych przez Administratora.

§10
Czas obowiązywania umowy

1. Umowa obowiązuje od dnia jej zawarcia przez czas trwania Umowy Głównej.

§11
Rozwiązanie umowy

Administrator jest uprawniony do rozwiązania Umowy ze skutkiem natychmiastowym, w przypadku gdy:

a) Podmiot przetwarzający, pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas realizacji prawa sprawdzenia nie usunie ich w wyznaczonym terminie;
b) Podmiot przetwarzający naruszył zasady przetwarzania danych osobowych określonych w Umowie i/lub w RODO;
c) zostanie stwierdzone prawomocną decyzją administracyjną lub prawomocnym wyrokiem sądu, że Podmiot przetwarzający naruszył zasady ochrony danych osobowych, o których mowa w Umowie oraz w RODO.

Rozwiązanie Umowy stanowi podstawę rozwiązania Umowy Głównej.

§12
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy danych poufnych.
2. Podmiot przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy lub Umowy Głównej, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy lub Umowy Głównej.
3. Podmiot przetwarzający zobowiązuje się do rozstrzygania wątpliwości w przedmiocie kwalifikacji

określonych informacji uzyskanych na potrzeby wykonywania Umowy oraz Umowy Głównej, poprzez ich określenie jako informacje chronione na mocy Umowy.

§13

Administrator w roli podmiotu przetwarzającego dla innych podmiotów

1. W przypadku, gdy Administrator będzie występował jako podmiot przetwarzający dla innego podmiotu, Podmiot przetwarzający zobowiązuje się do wykonywania tych samych obowiązków, które na mocy umowy z tym innym podmiotem zostaną nałożone na Administratora.

§14

Kary umowne

1. W przypadku odstąpienia od Umowy przez którąkolwiek ze Stron z przyczyn leżących po stronie Podmiotu przetwarzającego, Administratorowi przysługuje kara umowna w wysokości 30% wynagrodzenia brutto Podmiotu przetwarzającego określonego w Umowie Głównej.
2. W przypadku niezrealizowania lub nienależytego wykonania przez Podmiot przetwarzający obowiązków objętych Umową, Podmiot przetwarzający zapłaci Administratorowi karę umowną w wysokości 30% wynagrodzenia brutto określonego w Umowie Głównej, z zastrzeżeniem ust. 3.
   W przypadku obowiązków Podmiotu przetwarzającego, co do których w Umowie wskazano konkretny termin ich realizacji, niewykonanie tych obowiązków w tym terminie pociąga za sobą zobowiązanie Podmiotu przetwarzającego do zapłacenia kary umownej w wysokości 1000 zł za każdy dzień opóźnienia.
   Zamawiający zastrzega sobie możliwość dochodzenia odszkodowania przewyższającego wysokość określonych w umowie kar umownych, na zasadach ogólnych kodeksu cywilnego.
   Zamawiający ma również możliwość potrącenia naliczonych kar umownych z należności przysługujących Podmiotowi przetwarzającemu z tytułu realizacji Umowy Głównej.

§15

Postanowienia końcowe

1. W przypadku, gdy Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
3. W sprawach nieuregulowanych Umową mają zastosowanie przepisy prawa obowiązujące na terenie Rzeczypospolitej Polskiej, w tym Kodeksu cywilnego oraz RODO.
4. Umowa ma charakter nieodpłatny.
5. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
6. Sądem właściwym dla rozpatrzenia sporów wynikających z Umowy będzie sąd właściwy dla Administratora.
7. Kontakt do Inspektora ochrony danych, wyznaczonego przez Administratora w celu realizacji

Umowy: ....., tel. .....

8. *Zgodnie z klauzulą informacyjną w załączeniu*

Administrator danych: **Podmiot przetwarzający:**

Załącznik nr 1 do Umowy powierzenia danych

Wykaz minimalnych środków technicznych i organizacyjnych, które zobowiązany jest wdrożyć Podmiot przetwarzający

I. Zabezpieczenia organizacyjne

1. Wdrożona dokumentacja w obszarze bezpieczeństwa informacji (w tym systemów informatycznych) i ochrony danych osobowych (polityki, procedury, instrukcje itp.).

2. Osoby przetwarzające dane u podmiotu przetwarzającego zostały przeszkolone w zakresie bezpieczeństwa informacji w tym związanych z systemami informatycznymi.

3. Systematycznie prowadzona analiza ryzyka w obszarze bezpieczeństwa informacji (w tym systemów informatycznych) i ochrony danych osobowych uwzględniająca ryzyka wynikające z przypadkowego lub niezgodnego z prawem:
- zniszczenia,
- utraty,
- modyfikacji,
- nieuprawnionego ujawnienia lub dostępu do danych

4. Prowadzone są regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych.

5. Prowadzona jest ewidencja zasobów informatycznych wykorzystywanych do przetwarzania danych osobowych (sprzęt, oprogramowanie, sieć).

6. Prowadzi się regularne przeglądy i aktualizacje zasobów IT.

II. Zabezpieczenia techniczne

1. Określenie obszarów bezpiecznych (biura, pomieszczenia, serwerownie itd.) oraz odpowiednie ich zabezpieczenie przed dostępem osób nieuprawnionych (np. kraty w oknach, rolety antywłamaniowe, wzmocnione drzwi, kontrola dostępu, ochrona fizyczna, CCTV, system alarmowy).

2. Pomieszczenia, w których przetwarzane są dane zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.

3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (min. 8 znaków, wielkie i małe litery, cyfry i znaki specjalne).

4. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity oraz ich systematyczna aktualizacja.

5. Użyto systemu Firewall do ochrony dostępu do sieci komputerowej.

6. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych w systemie informatycznym (logi).

7. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w systemie informatycznym zbioru danych osobowych.

8. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu służącego do

przetwarzania danych.

9. Systemy wymuszają jakość haseł użytkowników (różne grupy znaków, długość haseł).

10. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

11. Korzystanie z systemów operacyjnych, które mają aktualne wsparcie producenta.

12. Monitorowanie w aktywny sposób bezpieczeństwa systemów informatycznych w tym m. in. działanie serwerów, ruch na serwerach, nieautoryzowane próby wejścia na serwer, próby złamania zabezpieczeń.

13. Wykonywanie kopii zapasowych danych i konfiguracji systemów teleinformatycznych oraz regularne sprawdzanie możliwość ich odtworzenia.

14. W przypadku pracy zdalnej zabronione jest wykorzystywanie prywatnego sprzętu przez pracowników oraz wykorzystuje się bezpieczne kanały komunikacji - VPN.

15. Zabronione jest wykorzystywanie nieautoryzowanych nośników USB.

16. Użytkownicy stacji roboczych nie posiadają uprawnień do instalowania nieautoryzowanego oprogramowania.

17. Komunikacja i dostęp przez internet szyfrowana jest za pomocą protokołów kryptograficznych (TLS/SSL).

18. Dane osobowe przesyłane za pomocą poczty elektronicznej przesyłane są jako zaszyfrowany załącznik (przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 9-znakowym hasłem jednorazowym, zawierającym małe i duże litery, cyfry i znaki specjalne) - hasło przekazywane jest innym bezpiecznym kanałem informacyjnym.

19. Systematycznie prowadzone są przeglądy, konserwacja i naprawy systemów informatycznych.

20. Monitoruje się pojemność i wydajność systemów informatycznych.

+ inne wskazane przez podmiot przetwarzający w liście kontrolnej

Załącznik nr 2 do Umowy powierzenia danych

Zgłoszenie naruszenia ochrony danych osobowych

1. Podmiot przetwarzający	
A. Dane podmiotu przetwarza	**ącego**
Pełna nazwa podmiotu przetwarzającego	
REGON - jeśli został podany (opcjonalnie)	
NIP	
B. Adres siedziby podmiotu przetwarzającego	
Państwo	Miejscowość

Województwo		Ulica	
Powiat		Kod pocztowy	
Gmina		Numer domu/nr lokalu	

C. Inspektor ochrony danych

Imię i nazwisko	
Numer telefonu	
Adres e-mail	

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

D. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie

2. Czas naruszenia

1) Wykrycie naruszenia

Data stwierdzenia naruszenia Wskaż kiedy dowiedziałeś/aś się o naruszeniu. Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Powody opóźnienia powiadomienia administratora o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż czas określony w umowie powierzenia

2) Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	

☐ Trwające naruszenie
Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.

Data i czas zakończenia naruszenia (opcjonalnie) Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	

3) Komentarz do czasu naruszenia (opcjonalnie)

Możesz podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia naruszenia.

3. Charakter naruszenia

6. Charakter

☐ Naruszenie poufności danych
Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

☐ Naruszenie integralności danych
Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

☐ Naruszenie dostępności danych
Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

7. Na czym polegało naruszenie?

☐ Zgubienie lub kradzież nośnika/urządzenia

☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ Nieuprawnione uzyskanie dostępu do informacji

☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ Niezamierzona publikacja

☐ Dane osobowe wysłane do niewłaściwego odbiorcy

☐ Ujawnienie danych niewłaściwej osoby

☐ Ustne ujawnienie danych osobowych

☐ Inne (wpisać jakie)

Opisz na czym polegało naruszenie.

8. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
(opcjonalnie)

9. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone

☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone

☐ Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznane)

4. Liczba osób i wpisów	
Przybliżona liczba osób, których mogło dotyczyć naruszenie	
Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)	

5. Kategorie danych osobowych UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.
Kategorie danych

Szczegółowy opis kategorii danych, których dotyczy naruszenie
Wymień jakie dane uległy naruszeniu: np. w przypadku sklepu internetowego profil użytkownika, w skład którego wchodzą: nazwa użytkownika, imię, nazwisko, hasło (zapisane otwartym tekstem lub hashowane), adres e-mail, oraz historia transakcji - kwota, data i nazwa kupionego produktu.

Dane podstawowe

☐ Dane identyfikacyjne
np. imię, nazwisko, nr dowodu osobistego, adres IP

☐ Krajowy numer identyfikacyjny
np. PESEL, SSN

☐ Dane kontaktowe
np. e-mail, numer telefonu, adres korespondencyjny

☐ Dane ekonomiczne i finansowe
np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe

☐ Oficjalne dokumenty
np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje

☐ Dane lokalizacyjne
np. GPS, dane o przemieszczaniu, miejsce zamieszkania

☐ Inne

Opisz poniżej kategorie danych:

Dane szczególnej kategorii

☐ Dane o pochodzeniu rasowym lub etnicznym

☐ Dane o poglądach politycznych

☐ Dane o przekonaniach religijnych lub światopoglądowych

☐ Dane o przynależności do związków zawodowych

☐ Dane dotyczące seksualności lub orientacji seksualnej

☐ Dane dotyczące zdrowia

☐ Dane genetyczne

☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

☐ Dane, o których mowa w art. 10 RODO

☐ Dane dotyczące wyroków skazujących

☐ Dane dotyczące czynów zabronionych

☐ Inne

Opisz poniżej kategorie danych:

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

6. Kategorie osób
UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

A. Kategorie osób, których dane dotyczą

☐ Pracownicy
☐ Użytkownicy
☐ Subskrybenci

☐ Studenci
☐ Uczniowie
☐ Służby mundurowe (np. wojsko, policja)
☐ Klienci (obecni i potencjalni)
☐ Klienci podmiotów publicznych
☐ Pacjenci
☐ Dzieci

☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie.
Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie

B. Liczba osób, których mogło dotyczyć naruszenie

Przybliżona liczba osób,
których mogło dotyczyć naruszenie

7. Środki bezpieczeństwa zastosowane przed naruszeniem

Środki zastosowane lub proponowane celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

8. Możliwe konsekwencje

A. **Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą**

☐ Utrata kontroli nad własnymi danymi osobowymi
☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
☐ Ograniczenie możliwości realizowania praw
☐ Dyskryminacja
☐ Kradzież lub sfałszowanie tożsamości
☐ Strata finansowa
☐ Naruszenie dobrego imienia
☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
☐ Nieuprawnione odwrócenie pseudonimizacji
☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

B. Ryzyko naruszenia praw i wolności osób fizycznych

☐ **Niskie**

☐ **Średnie**

☐ **wysokie**

6. Środki zaradcze

A. Środki w celu zaradzenia naruszeniu ochrony danych osobowych

Opisz dodatkowe środki (poza poinformowaniem osób) zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego wystąpienia.

Umowa nr .....

zawarta w dniu ..... w ..... pomiędzy
..... reprezentowanymi przez:
..... - .....
"Zamawiającym"

a

.....

..... reprezentowanymi przez:

..... - .....

zwaną w dalszej części umowy „Wykonawcą" łącznie zwanymi dalej „Stronami"

§ 1
Przedmiot Umowy

Zamawiający zleca, a Wykonawca przyjmuje do realizacji usługę **Usługa przeprowadzenia audytu oraz diagnozy poziomu bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) i rekomendacji dotyczących podniesienia tego poziomu jako** dwu etapowego audytu bezpieczeństwa systemu informacyjnego i ochrony danych medycznych zgodnie z dla Operatora Usługi Kluczowej zgodnie z „Wymaganiami dotyczącymi audytu bezpieczeństwa", stanowiącymi załącznik nr 2 do Umowy o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, będącej załącznikiem Nr 2 do Zarządzenia Nr 68/2022/BBIICD Prezesa NFZ z dnia 20 maja 2022 r. ,z wymaganiami ustawy z dnia 13 sierpnia 2018 roku o Krajowym Systemie Cyberbezpieczeństwa , Krajowych Ram Interoperacyjności zgodnie z wymaganiami norm PN ISO IEC 27001, PN ISO IEC 22301 poprzez badanie

a) spełniania wymogów dokumentacyjnych obowiązujących u Zamawiającego jako regulacji wewnętrznych dokumentacji normatywnej i operacyjnej dotyczących usługi kluczowej bezpieczeństwa informacji - dokumentacja SZBI/KRI/BCM , ochrony danych osobowych dokumentacja RODO i ODO ,
b) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych
c) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych

zgodnie z „Opisem przedmiotu zamówienia" stanowiącym załącznik nr 1 do niniejszej umowy.

§ 2
Terminy

1. Usługa zostanie wykonana audyt diagnostyczny do 20.09.2022 audyt końcowy do 31.11.2022
2. Szczegółowy harmonogram realizacji usługi zostanie uzgodniony pomiędzy Zamawiającym a Wykonawcą w trybie roboczym zgodnie z opisem przedmiotu zamówienia zał nr 1 do ogłoszenia Sp/AZp/382/13/poza/2022
3. Jeżeli na skutek działań lub zaniechań Wykonawcy powstaną przeszkody w terminowym wykonaniu elementu przedmiotu Umowy Wykonawca zobowiązany jest niezwłocznie powiadomić pisemnie Zamawiającego o tej okoliczności, określić pisemnie nowy termin wykonania przedmiotu Umowy oraz uzyskać pisemną zgodę Zamawiającego na nowy termin wykonania przedmiotu Umowy.

4. Zamawiający dopuszcza zmianę terminów realizacji przedmiotu Umowy, w przypadku braku możliwości jego realizacji w ustalonym przez Strony terminie, spowodowanej wprowadzeniem nowych obostrzeń w związku ze stanem epidemii wirusa SARS-CoV-2 („COVID-19"), które uniemożliwiają bądź w istotnym stopniu ograniczają możliwość wykonania Umowy. W powyższym przypadku Strony ustalą nowy termin realizacji przedmiotu Umowy, z zastrzeżeniem postanowień § 9 ust. 3.

§ 3
Sposób wykonania Umowy

1. Wykonawca zobowiązuje się do wykonania przedmiotu Umowy z należytą starannością, wymaganą przy pracach tego rodzaju, uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z obowiązującymi przepisami prawa, wymogami Zamawiającego zasadami współczesnej wiedzy technicznej i stosowanymi normami.
2. Umowa realizowana będzie przez Wykonawcę w ścisłym współdziałaniu z pracownikami odpowiednich komórek organizacyjnych Zamawiającego, przy zachowaniu zasady dzielenia się posiadaną wiedzą i doświadczeniem. Dotyczy to wszystkich kontaktów roboczych i wzajemnego informowania się przedstawicieli Zamawiającego i Wykonawcy co do treści i sposobu realizacji Umowy, zarówno pisemnie, mailowo i telefonicznie, przez cały okres trwania Umowy.
3. Wykonawca zobowiązuje się do zapewnienia na własny koszt wszystkich ewentualnych pozwoleń, zgód, koncesji, licencji, certyfikatów bezpieczeństwa wymaganych przez obowiązujące przepisy prawa w zakresie niezbędnym do prawidłowej realizacji Umowy.
4. Wykonawca nie może powierzyć, ani w całości, ani w części wykonania usługi podwykonawcom.
5. Wykonawca i wszystkie osoby realizujące zamówienie nie podejmą działań mogących spowodować naruszenie bezpieczeństwa informacji lub naruszenie danych osobowych u Zamawiającego.

§ 4
Wynagrodzenie i warunki płatności

1. Całkowite ryczałtowe wynagrodzenie Wykonawcy za należyte wykonanie całości przedmiotu Umowy, uwzględniające wszystkie koszty i opłaty wynosić będzie ..... zł netto (słownie: ..... zł netto), powiększone o należny podatek VAT 23%, co stanowi ..... zł brutto (słownie: ..... zł brutto).

2. Wynagrodzenie, o którym mowa w ust. 1 powyżej stanowi całość wynagrodzenia Wykonawcy w związku z realizacją Umowy, w tym za przeniesienie na Zamawiającego autorskich praw majątkowych i praw zależnych dla wytworzonej dokumentacji. Z tytułu przeniesienia praw autorskich Wykonawcy nie przysługują żadne inne roszczenia w stosunku do Zamawiającego.
3. Warunkiem zapłaty wynagrodzenia, o którym mowa w ust. 1, jest doręczenie Zamawiającemu prawidłowo wystawionej faktury VAT.
4. Podpisany i zatwierdzony protokół odbioru prac, bez uwag, będzie podstawą do wystawienia przez Wykonawcę faktury VAT.
5. Wynagrodzenie Wykonawcy wypłacone będzie przez Zamawiającego, poleceniem przelewu na rachunek bankowy Wykonawcy nr ..... , w terminie do 21 dni od daty doręczenia Zamawiającemu prawidłowo wystawionej faktury.

6. Termin zapłaty wynagrodzenia uważa się za zachowany, jeżeli obciążenie rachunku bankowego Zamawiającego nastąpi najpóźniej w ostatnim dniu płatności, wskazanym w ust. 4 powyżej.
7. Dla potrzeb wzajemnych rozliczeń Strony oświadczają, że są płatnikami podatku VAT.
8. Wierzytelności Wykonawcy, wynikające z Umowy nie mogą być przenoszone na osobę trzecią bez pisemnej zgody Zamawiającego.

§ 5

Odbiór przedmiotu Umowy

1. Przez wykonanie przedmiotu Umowy jej strony rozumieją wykonanie wszystkich elementów tego przedmiotu i odebranie ich przez Zamawiającego protokołem zdawczo-odbiorczym niezawierającym uwag ze strony Zamawiającego.
2. W terminie do 7 dni od daty zakończenia audytu wstępnego w siedzibie Zamawiającego Wykonawca prześle w formie elektronicznej w formacie edytowalnym i pdf raport wstępny.
W terminie do 10 dni od daty zakończenia audytu końcowego w siedzibie Zamawiającego Wykonawca prześle w formie elektronicznej w formacie edytowalnym i pdf raport końcowy.
Zamawiający ma prawo zgłoszenia uwag/zastrzeżeń do raportu , do których Wykonawca ustosunkuje się w terminie wskazanym przez Zamawiającego, w tym nanosząc ewentualne korekty.
Jeżeli Zamawiający nie będzie wnosił innych uwag/zastrzeżeń do skorygowanego raportu poinformuje o tym Wykonawcę, który przygotuje na tej podstawie raport końcowy i przekaże go Zamawiającemu, w formie elektronicznej w formacie edytowalnym i pdf, w terminie do 3 dni.
3. Ustala się, iż miejscem odbioru przedmiotu Umowy jest siedziba Zamawiającego.
4. Jeżeli przy dokonywaniu odbioru przedmiotu Umowy zostaną stwierdzone przez Zamawiającego jakiekolwiek wady, nieprawidłowości itp., odbiór przedmiotu Umowy nastąpi po ich usunięciu przez Wykonawcę. Stwierdzenie nieprawidłowości zostanie zaznaczone przez Strony w protokole odbioru.
5. Wszelkie stwierdzone w protokole odbioru wady, nieprawidłowości itp. zostaną usunięte przez Wykonawcę niezwłocznie, nie później niż w terminie 5 dni od ich stwierdzenia.
6. W razie uchylania się przez Wykonawcę od podpisania i dostarczenia do Zamawiającego podpisanego protokołu odbiory w terminie 5 dni od dnia przesłania protokołu przez Zamawiającego, Zamawiający może z upływem tego terminu uznać treść sporządzonego przez siebie protokołu za zaakceptowaną przez Wykonawcę.

§ 6
Uprawnienia wynikające z praw autorskich

1. Wraz z zadysponowaniem na rzecz Zmawiającego poszczególnych elementów przedmiotu Umowy mających charakter utworów w rozumieniu ustawy z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych*, na Zmawiającego przechodzi własność egzemplarzy tych utworów, a ponadto z tą samą chwilą Wykonawca bez składania dodatkowego oświadczenia woli przenosi na Zamawiającego, w ramach wynagrodzenia określonego w § 5 ust. 1, bez żadnych ograniczeń czasowych i terytorialnych, całość autorskich praw majątkowych do przekazanych projektów na wszystkich polach eksploatacji, znanych w dniu zawarcia Umowy, tj. w szczególności:
   a) do wyłącznego używania, wykorzystywania i udostępniania utworów do organizacji różnego rodzaju imprez masowych, zawodów sportowych, koncertów, konferencji, konwencji, zjazdów, itp.;
   b) do wyłącznego używania, wykorzystywania i udostępniania utworów w działalności promocyjnej, reklamowej, informacyjnej i usługowej;
   c) do wytwarzania, utrwalania i zwielokrotniania egzemplarzy utworu wszystkimi technikami, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz technika cyfrową, w szczególności jego zwielokrotnienia poprzez dokonywanie zapisów na wszelkiego rodzaju nośnikach danych, w tym na płytach CD lub podobnych, kasetach magnetofonowych, kasetach video, urządzeniach pamięci zewnętrznej, wprowadzenia do pamięci komputera.
2. Udostępnienie utworu powstałego w ramach realizacji Umowy może mieć miejsce w szczególności za pomocą egzemplarzy zwielokrotnionych zgodnie z ust. 1 pkt 3, a także w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym.
3. W ramach wynagrodzenia określonego Umową, od chwili nabycia autorskich praw majątkowych do utworów, o których mowa w ust. 1, Wykonawca zezwala Zamawiającemu na wykonywanie na zasadzie wyłączności zależnego prawa autorskiego w rozumieniu art. 2 ustawy z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* w stosunku do wszelkich opracowań utworów powstałych w wykonaniu Umowy tj. wyraża zgodę na korzystnie, rozporządzanie i rozpowszechnianie opracowań utworów, o których mowa w ust. 1, a także dokonywanie w nich zmian i modyfikacji, ponadto w tym samym terminie Wykonawca przenosi na Zamawiającego wyłączne prawo zezwalania na wykonywanie zależnego prawa autorskiego. Wykonywanie powyższych uprawnień będzie następowało na polach eksploatacji wskazanych w ust. 1.
4. W ramach wynagrodzenia określonego Umową Zamawiającemu przysługuje prawo do korzystania z utworów, ich elementów, fragmentów, opracowań utworów bez ograniczeń czasowych i terytorialnych, w ramach promocji i reklamy swojej działalności, działalności sponsorów, w szczególności na potrzeby reklamy internetowej, telewizyjnej, prezentacji, ofert, broszur, udziałów w konkursach, targach i innych imprezach tego typu zarówno wewnętrznych jak i z udziałem podmiotów trzecich, w tym także na polach eksploatacji określonych w Umowie.
5. Wykonawca gwarantuje, że najpóźniej na dzień przeniesienia autorskich praw majątkowych do utworów, o których mowa w ust. 1, na Zamawiającego, Wykonawca będzie wyłącznie uprawniony do dysponowania nimi, a także prawami (uprawnieniami), o których mowa w ust. 3 i 4, a prawa te pozostaną wolne od wad, w tym praw i roszczeń osób trzecich. W zakresie niniejszego oświadczenia Wykonawca ponosi względem Zamawiającego pełną odpowiedzialność odszkodowawczą obejmującą w szczególności szkodę bezpośrednią, koszty pomocy prawnej świadczonej w celu obrony interesów Zamawiającego oraz równowartość

świadczeń spełnionych przez Zamawiającego w celu zaspokojenia roszczeń osób trzecich będących autorami utworów, dotyczących naruszenia praw do tych utworów. Powyższe nie zwalnia Wykonawcy z obowiązku współdziałania z Zamawiającym w celu skutecznej obrony przed roszczeniami takich osób trzecich dotyczących naruszenia praw do ww. utworów.

6. Strony zgodnie oświadczają, iż ich intencją jest zapewnienie Zamawiającemu, w ramach wynagrodzenia określonego Umową, możliwości wyłącznego wykonywania praw autorskich majątkowych, osobistych i praw zależnych do utworów, będących przedmiotem Umowy, w szczególności nieograniczonego prawa do: korzystania z utworów, rozporządzania nimi, wprowadzania do nich zmian, sporządzania ich opracowań, tworzenia na ich podstawie nowych utworów oraz korzystania z tych opracowań, nowych utworów i rozporządzania nimi. Zamiarem stron jest zapewnienie, aby takie korzystanie z utworów, ich opracowań, nowych projektów oraz rozporządzanie nimi nie wymagało odrębnych zgód i zezwoleń Wykonawcy lub autora/ów, by nie wymagało zapłaty odrębnego wynagrodzenia i nie było przez autora/ów utworów traktowane jako naruszenie praw osobistych.

7. Zapisy ust. 1-6 dotyczą Zamawiającego oraz „Następcy Zamawiającego". Przy czym termin „Następca Zamawiającego" oznacza: następcę(ców) prawnego(ych) Zamawiającego lub podmiot(y), na który(e) Zamawiający przeniesie całość lub część praw do utworów lub podmiot(y), który(e) zostanie(ą) upoważniony(e) przez Zamawiającego do wykonywania praw autorskich do utworów lub do korzystania z nich, w szczególności na podstawie umowy licencyjnej, umowy dzierżawy, lub innej umowy.

§ 7
Odpowiedzialność za wykonanie przedmiotu Umowy

1. Wykonawca odpowiada za wszelkie szkody powstałe po stronie Zamawiającego z powodu niewykonania lub nienależytego wykonania zobowiązań wynikających z niniejszej Umowy.

2. W przypadku szkody spowodowanej umyślnym działaniem lub zaniechaniem Wykonawcy, Wykonawca ponosi odpowiedzialność za wszelkie szkody poniesione przez Zamawiającego w pełnej wysokości, w tym również za utracone korzyści.

3. Strony nie są odpowiedzialne za niewykonanie lub nienależyte wykonanie Umowy jeśli udowodnią, że niewykonanie lub nienależyte wykonanie zostało spowodowane nadzwyczajnym wydarzeniem będącym poza ich kontrolą, a w chwili zawarcia Umowy niemożliwe było przewidzenie tego zdarzenia i jego skutków, które wpłynęły na zdolność Strony do wykonania Umowy oraz że niemożliwe było uniknięcie samego zdarzenia lub jego skutków (działanie siły wyższej, np. pożar, powódź, strajk).

4. W przypadku działania siły wyższej, która uniemożliwi prawidłowe wywiązanie się z zobowiązań Strony, Strona ta niezwłocznie po wystąpieniu siły wyższej powiadomi pisemnie drugą Stronę o takiej okoliczności i przedstawi obiektywne dowody bezpośredniego wpływu działania siły wyższej na możliwość realizacji przedmiotu niniejszej Umowy. Jeżeli druga Strona Umowy nie zdecyduje inaczej w formie pisemnej, Strona powołująca się na działanie siły wyższej jest zobowiązana do kontynuowania zobowiązań wynikających z Umowy po ustąpieniu działania siły wyższej.

§ 8
Kary umowne

1. W przypadku odstąpienia od Umowy przez którąkolwiek ze Stron z przyczyn leżących po stronie Wykonawcy, Zamawiający ma prawo do naliczenia kary umownej w wysokości 20% wynagrodzenia brutto wskazanego w § 4 ust. 1 Umowy.

2. Zamawiający ma prawo do naliczenia Wykonawcy kary umownej w wysokości 1% wynagrodzenia brutto wskazanego w § 4 ust. 1 Umowy:

1) za każdy dzień opóźnienia w przypadku niedotrzymania terminów realizacji Umowy określonych w § 2,
2) za nieterminowe usunięcie wad, nieprawidłowości itp. stwierdzonych przy odbiorze przedmiotu Umowy - za każdy dzień opóźnienia.
3. W przypadku niezrealizowania lub nienależytego zrealizowania elementów przedmiotu Umowy - innych, niż wskazane w ust. 2 pkt-ach 1 i 2 Zamawiający ma prawo do naliczenia Wykonawcy kary umownej w wysokości 3% wynagrodzenia brutto określonego w § 4 ust. 1 Umowy, za każdy taki przypadek.
4. W razie rażącego naruszenia przez Wykonawcę któregokolwiek z zobowiązań opisanych w § 10, jak również w przypadku ujawnienia, przekazania lub wykorzystania informacji poufnych w sposób sprzeczny z postanowieniami Umowy, Zamawiający uprawniony będzie do naliczenia i żądania od Wykonawcy zapłaty kary umownej w wysokości 10.000 zł. za każdy przypadek naruszenia zobowiązania.

5. Naliczone kary umowne płatne są na rzecz Zamawiającego w terminie 14 dni, licząc od daty otrzymania przez Wykonawcę wezwania do ich zapłaty, zawierającego wskazanie podstawy i uzasadnienie przyczyny ich naliczenia.
6. Zamawiającemu przysługuje prawo potrącenia naliczonej kary umownej z wynagrodzenia Wykonawcy.
7. Zamawiającemu przysługuje prawo dochodzenia odszkodowania na zasadach ogólnych w przypadku gdy wysokość szkody przewyższa zastrzeżone kary umowne.

§ 9
Odstąpienie od Umowy

1. Oprócz wypadków wymienionych w przepisach Kodeksu cywilnego stronom przysługuje prawo odstąpienia od Umowy w następujących przypadkach:
1) gdy Wykonawca nie przystąpił do realizacji Umowy pomimo pisemnego wezwania do jej realizacji i wyznaczenia kolejnego terminu przez Zamawiającego;
2) gdy Wykonawca nie wywiązuje się z obowiązków określonych w niniejszej Umowie, pomimo pisemnego upomnienia i wezwania do ich realizacji we wskazanym terminie przez Zamawiającego;
3) niewykonania któregokolwiek z elementów przedmiotu Umowy;
4) istotnych zmian okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy;
5) ogłoszenia upadłości Wykonawcy;
6) wydania nakazu zajęcia majątku Wykonawcy;
2. Odstąpienie od Umowy w przypadkach, o których mowa w ust. 1 pkt. 1-3 może nastąpić w terminie 30 dni od powzięcia wiadomości o zaistnieniu zdarzeń w nich wymienionych, a w przypadkach o których mowa w ust. 1 pkt. 4-6 oraz w ust. 3 - w terminie 21 dni od powzięcia wiadomości o zaistnieniu zdarzeń w nich wymienionych.
3. Poza przypadkami wymienionymi w ust. 1 Zamawiający może, przed rozpoczęciem realizacji umowy w siedzibie Zamawiającego, w trybie natychmiastowym odstąpić od Umowy lub zmienić termin jej realizacji w razie wystąpienia siły wyższej, w szczególności wzrostu liczby zakażeń wirusa SARS-CoV-2 („COVID-19") w Polsce do wartości powyżej 10000 osób dziennie, czego nie można było przewidzieć w chwili zawarcia Umowy.
4. W przypadku odstąpienia od Umowy w trybie określonym w ust. 3 Wykonawcy nie przysługują jakiekolwiek roszczenia odszkodowawcze wobec Zamawiającego.
5. Odstąpienie od Umowy powinno nastąpić w formie pisemnej pod rygorem nieważności i powinno zawierać uzasadnienie.

§ 10
Poufność

1. Wykonawca zobowiązuje się do:

1) zachowania w tajemnicy wszelkich informacji otrzymanych i uzyskanych w związku z wykonywaniem zobowiązań wynikających z realizacji Umowy;

2) wykorzystywania informacji jedynie w celu niezbędnym dla realizacji Umowy;

3) podejmowania wszelkich kroków i działań w celu zapewnienia, że żadna z osób otrzymujących informacje w myśl postanowień pkt. 1 nie ujawni tych informacji, ani ich źródła, zarówno w całości jak i w części, stronom trzecim bez uzyskania uprzedniej, wyraźnej zgody na piśmie Zamawiającego;

4) ujawniania informacji, o której mowa w ust. 1 jedynie pracownikom, dla których będą one konieczne do wykonywania powierzonych im czynności w ramach prac określonych w zawartej Umowie i tylko w zakresie, w jakim odbiorca informacji musi mieć do nich dostęp dla celu realizacji Umowy;

5) rozstrzygania wątpliwości w przedmiocie kwalifikacji określonych informacji uzyskanych na potrzeby wykonywania niniejszej Umowy, poprzez ich określenie jako informacje chronione na mocy Umowy;

6) niesporządzania kopii ani jakiegokolwiek innego powielania, poza uzasadnionymi prawnie przypadkami, informacji otrzymanych i uzyskanych w związku z realizacją Umowy;

7) przekazywania, ujawniania oraz wykorzystywania informacji otrzymanych przez Wykonawcę od Zamawiającego, będących przedmiotem niniejszej Umowy, wyłącznie na rzecz podmiotów upoważnionych na podstawie przepisów obowiązującego prawa i w zakresie określonym Umową.

2. Zobowiązanie, o którym mowa w ust. 1 nie ma zastosowania do:

1) informacji ogólnie dostępnych i powszechnie znanych;

2) informacji, na których ujawnienie Zamawiający wyraził wyraźną zgodę na piśmie pod rygorem nieważności;

3) informacji uzyskanych przez Wykonawcę od osób trzecich, o ile takie ujawnienie przez osobę trzecią nie stanowi naruszenia powszechnie obowiązujących przepisów prawa lub zobowiązań zaciągniętych przez te osoby (w szczególności zobowiązania wobec Strony do nieujawniania danych informacji). Wykonawca zobowiązany jest do zachowania w tajemnicy informacji uzyskanych od osób trzecich, które zostały mu udostępnione z naruszeniem wymogów określonych w zdaniu poprzednim;

4) udostępnienia informacji na rzecz podmiotów uprawnionych, o ile obowiązek udostępnienia tych informacji na rzecz tych podmiotów wynika z powszechnie obowiązujących przepisów prawa. Wykonawca fakt ten zgłasza każdorazowo, niezwłocznie Zamawiającemu.

3. Wykonawca zobowiązany jest do dokonania stosownych czynności prawnych (np. zawarcia stosownych umów z pracownikami dotyczących m. in. okresu obowiązywania tajemnicy przedsiębiorstwa), niezbędnych do wykonania obowiązków, o których mowa w Umowie.

§ 11
Osoby wyznaczone przez strony do kontaktu w celu realizacji Umowy

1. Do bieżącej współpracy w sprawach związanych z wykonywaniem Umowy, w tym do prowadzenia korespondencji związanej z jej realizacją upoważnieni są:

a) ze strony Zamawiającego: ....., tel....., e-mail: .....

b) ze strony Wykonawcy: ....., tel ....., e-mail: .....

§ 12
Przetwarzanie danych osobowych

1. W celu umożliwienia realizacji Umowy niezbędne jest przetwarzanie danych osobowych, a szczegóły w tym zakresie reguluje Umowy powierzenia przetwarzania danych osobowych stanowiąca zał. 2 do niniejszej Umowy.
2. Dane osobowe osób wyznaczonych przez Wykonawcę do kontaktu z Zamawiającym będą przetwarzane przez Zamawiającego jako administratora danych osobowych wyłącznie w celu koordynowania i realizacji ustaleń wynikających z Umowy oraz w celu realizacji uprawnień i obowiązków wynikających z przepisów prawa. Wykonawca zobowiązuje się we własnym zakresie wykonać obowiązek informacyjny w powyższym zakresie zgodnie z RODO i klauzulą informacyjną stanowiącą zał. 3 do niniejszej Umowy.
3. Wykonawca zobowiązuje się do przekazania klauzuli informacyjnej, o której mowa w ust. 2 powyżej, na rzecz osób wyznaczonych do kontaktów przez Wykonawcę oraz innych osób, których dane osobowe zamierza przekazać Zamawiającemu w związku z realizacją Umowy.

§ 13
Zmiana osób uczestniczących w realizacji Umowy

1. Zmiana osoby, która będzie uczestniczyć w wykonywaniu zamówienia, możliwa jest na wniosek Wykonawcy, jak również na wniosek Zamawiającego, jeśli Zamawiający zgłosi zastrzeżenia do prac wykonywanych przez daną osobę.
2. W przypadku zmiany osoby, o której mowa w ust. 1, na wniosek Zamawiającego, Wykonawca zobowiązany jest przedstawić nową osobę posiadającą co najmniej równe kwalifikacje jak osoba zastępowana, nie później niż w ciągu 5 dni od przekazania przez Zamawiającego wniosku.
3. Zamawiający zobowiązany jest, nie później niż w ciągu 3 dni od przedstawienia przez Wykonawcę nowej osoby, o której mowa w ust. 2, zaakceptować nową osobę, lub odrzucić propozycję zmiany.
4. W przypadku odrzucenia przez Zamawiającego propozycji zmiany, o której mowa w ust. 3, odpowiednie zastosowanie mają postanowienia ust. 2-4.

§ 14
Obowiązki wykonawcy w związku z obowiązywaniem stanu epidemii SARS-CoV-2

1. Wszystkie osoby ze strony Wykonawcy realizujące przedmiot umowy w siedzibie Zamawiającego muszą być zdrowe, bez objawów infekcji lub innej choroby, w tym w szczególności zakaźnej oraz nie mogą podlegać obowiązkowej kwarantannie lub izolacji.
1. Wszystkie osoby ze strony Wykonawcy realizujące przedmiot umowy, przybywając w siedzibie Zamawiającego, zobowiązane są zakrywania ust i nosa przy użyciu maseczki.

§ 15
Postanowienia końcowe

1. Wykonawca nie jest uprawniony do zaciągania jakichkolwiek zobowiązań w imieniu Zamawiającego.
2. Wszystkie opracowania, dokumenty oraz materiały nabyte, zebrane lub przygotowane przez Wykonawcę w ramach niniejszej Umowy stanowią wyłączną własność Zamawiającego. Wykonawca może zatrzymać ich kopie, jeżeli nie będzie ich używał do celów innych niż związanych z realizacją Umowy.
2. Wykonawca zobowiązuje się powiadomić Zamawiającego o każdej zmianie danych i stanu

faktycznego, mających wpływ na realizację Umowy.

3. Wszelkie zmiany i uzupełnienia niniejszej Umowy mogą być dokonane za zgodą Stron, w formie pisemnej pod rygorem nieważności.

4. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy Kodeksu cywilnego.

5. Strony będą dążyły do polubownego rozstrzygania wszelkich sporów powstałych w związku z realizacją niniejszej Umowy, jednak gdy nie osiągną porozumienia, zaistniały spór będzie poddany rozstrzygnięciu przez Sąd właściwy miejscowo dla siedziby Zamawiającego.

6. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego i jeden dla Wykonawcy.

7. Integralną część Umowy stanowią załączniki:
   a) zał. nr 1 - Opis przedmiotu zamówienia,
   b) zał. nr 2 - Umowy powierzenia przetwarzania danych osobowych,
   c) zał. nr 3 - Klauzula informacyjna dla kontrahenta oraz osoby kontaktowej po stronie kontrahenta,
   d) zał. nr 4 - Oferta wykonawcy.

Zamawiający Wykonawca