UMOWA NR ……../CIS-WAZ.2720.xx.2021

W wyniku rozstrzygnięcia zapytania ofertowego CIS-WAZ.2720.xx.2021, pomiędzy:

Skarbem Państwa – Głównym Urzędem Statystycznym z siedzibą w (00-925) Warszawie, al. Niepodległości 208, NIP: 701-023-61-79 REGON nr 000331501, Zamawiającym, reprezentowanym przez Dyrektora Centrum Informatyki Statystycznej,

…… ……. - Pełnomocnika

a

…… z siedzibą w …… przy ul. ……., kod ……., wpisanym do …… posiadającym nr NIP ……. i nr REGON: ……., zwanym dalej „Wykonawcą", którego reprezentuje:

……

zwanymi dalej łącznie Stronami, została zawarta umowa następującej treści:

§ 1

PRZEDMIOT UMOWY

1. Przedmiotem umowy jest aktualizacja systemu eBiuro w zakresie dostosowania apletu kryptograficznego systemu eBiuro do nowych certyfikatów oraz do funkcji skrótu SHA-256.
2. Wykonanie przedmiotu umowy, o którym mowa w ust. 1 obejmuje wytworzenie i dostawę oprogramowania okeślonego z załączniku nr 1 do umowy.
3. Aktualizacja systemu eBiuro, o której mowa w ust. 1 i 2, wraz z instrukcją aktualizacji, zostanie dostarczona w formie elektronicznej na adres e-mail ……

§ 2

WARTOŚĆ UMOWY

1. Za prawidłowe i kompletne wykonanie przedmiotu umowy, o którym mowa w § 1, Zamawiający zapłaci Wykonawcy, wynagrodzenie w wysokości netto …… zł (słownie: …… zł i …./100), brutto …… zł (słownie: …… zł i …./100), w tym podatek VAT obliczony wg. stawki ……..% w kwocie …… zł).
2. Wynagrodzenie, określone w ust. 1 obejmuje wszelkie koszty związane z wykonaniem przedmiotu umowy, w tym koszty aktualizacji systemu eBiuro, koszty dostawy przedmiotu umowy, koszty udzielenia licencji, koszty świadczenia gwarancji, a także pozostałe koszty związane z realizacją przedmiotu umowy.

§ 3

TERMIN REALIZACJI UMOWY

1. Termin wykonania przedmiotu umowy wynosi 30 dni kalendarzowych od daty podpisania umowy.
2. Termin, o którym mowa w ust. 1 obejmuje wykonanie testów o których mowa w § 4 ust 1**.**

§ 4

POTWIERDZENIE REALIZACJI UMOWY

1. W celu zweryfikowania prawidłowego wykonania przedmiotu umowy, zostaną wykonane testy sprawdzające prawidłowość działania w zakresie wprowadzonej aktualizacji systemu eBiuro, określonej w § 1, przeprowadzone przez upoważnionych przedstawicieli Zamawiającego, o których mowa w § 5 ust 2. Wykonanie testów zostanie potwierdzone protokołem odbioru, podpisanym przez przedstawicieli Stron.
2. Protokół odbioru przedmiotu umowy, podpisany przez przedstawicieli Stron z wynikiem pozytywnym, będzie podstawą do wystawienia przez Wykonawcę faktury i wypłacenia przez Zamawiającego należnego Wykonawcy wynagrodzenia.
3. W przypadku stwierdzenia w protokole odbioru przedmiotu umowy, zastrzeżeń do wykonania przedmiotu umowy, Wykonawca niezwłocznie usunie zgłoszone zastrzeżenia bez prawa do dodatkowego wynagrodzenia.
4. Wykonawca zobowiązuje się wykonać przedmiot umowy zgodnie z obowiązującymi przepisami

i ofertą Wykonawcy stanowiącą załącznik nr 3 do umowy.

§ 5

OSOBY UPOWAŻNIONE DO WSPÓŁDZIAŁANIA PRZY REALIZACJI UMOWY

1. Upoważnionym do występowania w imieniu Wykonawcy w zakresie realizacji umowy, w tym, podpisania Protokołu odbioru umowy są:
   1) ..... - tel.: ....., e-mail: ..... ,
   2) ..... - tel.: ....., e-mail: .....
   3) ..... - tel.: ....., e-mail: .....
2. Upoważnionymi do występowania w imieniu Zamawiającego w zakresie realizacji umowy, w tym przeprowadzenia testów oraz odbioru przedmiotu umowy i podpisania protokołu odbioru, są:
   1) ..... - tel.: ....., e-mail : ..... ,
   2) ..... - tel.: ....., e-mail: .....
   3) ..... - tel.: ....., e-mail: .....
3. Zmiana danych i osób wskazanych w ust. 1-2 nie wymaga zmiany umowy, a dla swej skuteczności wymaga uprzedniego poinformowania drugiej strony, z co najmniej dwudniowym wyprzedzeniem, drogą elektroniczną, bez konieczności aneksowania umowy.

§ 6

WARUNKI PŁATNOŚCI

1. Za prawidłowe wykonanie przedmiotu umowy Zamawiający zapłaci wynagrodzenie, o którym mowa w § 2 ust. 1, określone na podstawie ceny w ofercie Wykonawcy, przelewem na rachunek bankowy Wykonawcy wskazany na fakturze, w ciągu 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury, do której dołączony zostanie oryginał protokołu odbioru, o którym mowa w § 4 ust. 2.
2. Faktury będą wystawiane na rzecz Zamawiającego z podaniem numeru umowy, określeniem przedmiotu umowy, kwoty netto, stawki i kwoty podatku VAT oraz wartości brutto, a także informacji o podzielonej płatności, jeśli dotyczy.
3. Faktura wystawiona w formie papierowej dostarczona zostanie na adres Zamawiającego: ....., al. Niepodległości 208, 00-925 Warszawa w ciągu 7 dni od daty jej wystawienia.
4. Za dotrzymanie przez Zamawiającego terminu zapłaty, o którym mowa w ust. 1, uważa się złożenie w tym terminie polecenia przelewu w banku Zamawiającego.
5. Na podstawie ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz. U. z 2020 r. poz. 1666), Zamawiający umożliwia Wykonawcy przesyłanie ustrukturyzowanych faktur elektronicznych, faktur korygujących i not księgowych za pośrednictwem platformy elektronicznego fakturowania.
6. Usługi Platformy Elektronicznego Fakturowania są świadczone pod adresami:
   1) https://efaktura.gov.pl (Portal PEF),
   2) https://brokerpefexpert.efaktura.gov.pl (Broker PEFexpert - obsługujący Zamawiającego),
   3) https://brokerinfinite.efaktura.gov.pl (Broker Infinite).
7. Zamawiający zastrzega, że nie dopuszcza przesyłania za pośrednictwem platformy elektronicznego fakturowania innych dokumentów wymienionych w rozporządzeniu Ministra Przedsiębiorczości i Technologii[1] (zlecenia dostawy/zamówienia, awizo dostawy, potwierdzenia odbioru).
8. *Wykonawca oświadcza, że numer rachunku rozliczeniowego wskazany w fakturze, która będzie wystawiona w jego imieniu, jest rachunkiem*/nie jest rachunkiem, dla którego zgodnie z Rozdziałem*

[1] Rozporządzenie Ministra Przedsiębiorczości i Technologii z dnia 25 kwietnia 2019 r. w sprawie listy innych ustrukturyzowanych dokumentów elektronicznych, które mogą być przesyłane za pośrednictwem platformy elektronicznego fakturowania służącej do przesyłania ustrukturyzowanych faktur elektronicznych oraz innych ustrukturyzowanych dokumentów elektronicznych (Dz. U. poz. 856).

3a ustawy z dnia 29 sierpnia 1997 r. - Prawo Bankowe (Dz. U. z 2020 r. poz. 1896) prowadzony jest rachunek VAT.[2]

9. *Wykonawca oświadcza, że podany numer rachunku rozliczeniowego wskazany w fakturze, jest taki sam jak w rejestrze podatników (biała lista).*

10. *Jeśli numer rachunku rozliczeniowego wskazany przez Wykonawcę, o którym mowa w ust. 6, jest rachunkiem, dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - Prawo Bankowe (Dz. U. z 2020 r. poz. 1896) prowadzony jest rachunek VAT to:*

    1) Zamawiający oświadcza, że będzie realizować płatności za fakturę z zastosowaniem mechanizmu podzielonej płatności tzw. split payment. Zapłatę w tym systemie uznaje się za dokonanie płatności w terminie określonym w § 7 ust. 1 umowy,

    2) *podzieloną płatność tzw. split payment stosuje się wyłącznie przy płatnościach bezgotówkowych, realizowanych za pośrednictwem polecenia przelewu lub polecenia zapłaty dla czynnych podatników VAT. Mechanizm podzielonej płatności nie będzie wykorzystywany do zapłaty za czynności lub zdarzenia pozostające poza zakresem VAT (np. zapłata odszkodowania), a także za świadczenia zwolnione z VAT, opodatkowane stawką 0% lub jeżeli wynika to z innych przepisów prawa.*

§ 7

GWARANCJA I RĘKOJMIA

1. Wykonawca udziela na przedmiot umowy gwarancji. Okres trwania gwarancji wynosi 30 dni od dnia podpisania protokołu odbioru z wynikiem pozytywnym. Usługi gwarancyjne obejmować będą tylko zrealizowane przez Wykonawcę w ramach umowy komponenty systemu eBiuro.

2. Zgłoszenia błędów, awarii oraz usterek (dalej określanych: „Wadą") będą zawierały, co najmniej następujące informacje:

    a) opis Wady;

    b) czas i lokalizację komputera (lub komputerów), gdzie stwierdzono wystąpienie Wady;

    c) opis czynności, których wykonywanie doprowadziło do wystąpienia Wady;

3. Usługi gwarancyjne świadczone będą w poniższych terminach:

    a) czas reakcji – 1 dzień roboczy od chwili otrzymania zgłoszenia,

    b) termin usunięcia – 5 dni roboczych od momentu otrzymania zgłoszenia.

4. Zamawiający będzie zgłaszał Wady drogą mailową, na adres wskazany przez Wykonawcę. Wykonawca będzie każdorazowo potwierdzać otrzymanie zgłoszenia (czas reakcji), tą samą drogą, którą zostało dokonane zgłoszenie. Osobami uprawnionymi do zgłaszania błędów po stronie Zamawiającego są .....

5. Obsługa zgłoszeń będzie się odbywać w dni robocze od poniedziałku do piątku, w godzinach od 9 do 16, z wyłączeniem dni ustawowo wolnych od pracy. Za moment dokonania zgłoszenia przez Zamawiającego przyjmuje się:

    a) czas otrzymania przez Wykonawcę zgłoszenia, jeśli Wykonawca otrzyma zgłoszenie w dniu roboczym, w godzinach 9 - 16;

    b) godzinę 9 następnego dnia roboczego w przypadku otrzymania przez Wykonawcę zgłoszenia w dniu roboczym po godzinie 16;

    c) godzinę 9 najbliższego dnia roboczego w przypadku otrzymania przez Wykonawcę zgłoszenia w dniu niebędącym dniem roboczym.

6. Termin usunięcia Wady ulega wydłużeniu o okres braku dostępu dla Wykonawcy do infrastruktury sprzętowo-systemowo-narzędziowej lub braku prawidłowego działania tej infrastruktury lub innych składników środowiska teleinformatycznego Zamawiającego potrzebnych dla prawidłowego funkcjonowania Systemu eBiuro (np. brak dostępu VPN).

7. Osoby wskazane przez Wykonawcę poinformują mailowo powyżej wskazane osoby o usunięciu Wady.

8. Osoby upoważnione do zgłaszania Wady potwierdzą mailowo fakt jej usunięcia.

---

[2] Zapisy kursywą stosuje się jeśli dotyczą.

9. Wykonawca odpowiada za wady przedmiotu umowy z tytułu rękojmi przez okres 12 miesięcy, którego bieg rozpoczyna się od dnia podpisania protokołu odbioru.

10. Zamawiający może dochodzić roszczeń z tytułu rękojmi także po upływie terminu jej obowiązywania, pod warunkiem, że zgłosił Wykonawcy wadę w okresie obowiązywania rękojmi.

§ 8

WARUNKI LICENCJONOWANIA

1. Wykonawca w ramach wynagrodzenia za wykonanie umowy, o którym mowa w § 2 ust. 1, udzieli Zamawiającemu licencji na wykonany przedmiot umowy (dalej „Oprogramowanie") albo zapewni jej przeniesienie od podmiotu, któremu przysługują do Oprogramowania majątkowe prawa autorskie, bez możliwości wcześniejszego wypowiedzenia.

2. Licencje, o których mowa w ust. 1 muszą pozwalać na swobodne ich przenoszenie pomiędzy urządzeniami (np. w przypadku wymiany sprzętu).

3. W ramach wykonania przedmiotu umowy, Wykonawca zobowiązany jest do przekazania Zamawiającemu, wraz z dostawą Oprogramowania, dokumentów licencyjnych w formie elektronicznej.

4. Warunki korzystania z Oprogramowania w ramach udzielonych licencji nie mogą być gorsze od standardowych warunków oferowanych innym podmiotom przez osobę lub podmiot, któremu przysługują prawa do tego Oprogramowania, w tym muszą obejmować co najmniej następujące pola eksploatacji:

   1) korzystanie z Oprogramowania w ramach wszystkich funkcjonalności w dowolny sposób w liczbie nabytych licencji i sublicencji na zasadach wskazanych w załączniku nr 1 do umowy,

   2) wprowadzanie i zapisywanie w pamięci komputerów, serwerów, odtwarzanie, utrwalanie, przekazywanie, przechowywanie, wyświetlanie, stosowanie, instalowanie i deinstalowanie Oprogramowania pod warunkiem zachowania liczby udzielonych licencji,

   3) sporządzanie kopii zapasowej (kopii bezpieczeństwa) nośników instalacyjnych i nośników z zainstalowanym Oprogramowaniem,

   4) korzystanie z produktów powstałych w wyniku eksploatacji Oprogramowania przez Zamawiającego i jednostki służb statystyki publicznej, w szczególności danych, raportów, zestawień oraz innych dokumentów kreowanych w ramach tej eksploatacji oraz modyfikowania tych produktów i dalszego z nich korzystania,

   5) utrwalanie lub zwielokrotnienie Oprogramowania w celu zastosowania procedur backupowych;

   6) prawo do kopiowania i używania dokumentacji przekazanej wraz z Oprogramowaniem na potrzeby Zamawiającego i jednostek służb statystyki publicznej.

5. Wykonawca oświadcza, że aktualizacja Oprogramowania, nie powoduje zmian pól eksploatacji określonych powyżej.

6. Wykonawca oświadcza, że odebrany przez Zamawiającego przedmiot umowy będzie wolny od wad fizycznych i prawnych.

7. Wykonawca oświadcza, że dostarczone przez niego Oprogramowanie, nie narusza jakichkolwiek praw osób trzecich, zwłaszcza w zakresie własności przemysłowej, praw autorskich i praw pokrewnych oraz nieuczciwej konkurencji i że posiada prawo do sprzedaży/udzielania licencji na Oprogramowanie, które Wykonawca dostarczył, zgodnie z postanowieniami § 1 i przejmuje w tym zakresie odpowiedzialność w przypadku roszczeń osób trzecich.

§ 9

KARY UMOWNE

1. Zamawiający może żądać od Wykonawcy zapłaty następujących kar umownych:

   1) za zwłokę w wykonaniu przedmiotu umowy w stosunku do terminu, o którym mowa w § 3 ust. 1 umowy w wysokości 1% kwoty wynagrodzenia brutto, o którym mowa w § 2 ust. 1 umowy za każdy dzień zwłoki nie więcej niż 10% kwoty wynagrodzenia brutto, o której mowa w § 2 ust. 1 umowy,

   2) za odstąpienie Zamawiającego od umowy lub rozwiązanie umowy z przyczyn leżących po stronie Wykonawcy, w wysokości 5% kwoty wynagrodzenia brutto, o którym mowa w § 2 ust. 1 Umowy,

3) za każde udokumentowane naruszenie zasad zachowania w poufności Informacji Poufnych, o których mowa w § 12 umowy, w wysokości 5% wynagrodzenia brutto określonego w § 2 ust. 1 umowy;

4) za każde udokumentowane naruszenie wymagań bezpieczeństwa informacji, o których mowa w § 13 umowy, w wysokości 10% wynagrodzenia brutto określonego w § 2 ust. 1 umowy;

2. Wykonawca wyraża zgodę na potrącanie przez Zamawiającego kar umownych z należnego mu wynagrodzenia. W innych przypadkach Wykonawca dokona zapłaty kary na podstawie noty obciążeniowej w terminie 14 dni od daty otrzymania noty obciążeniowej.

3. Postanowienia ust. 2 stosuje się z zastrzeżeniem art. 77 pkt 21) ustawy z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 (Dz.U. poz. 1086, z późn. zm.) w związku z art. 15 r[1] ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. poz. 1842).

4. Odpowiedzialność Stron z tytułu nienależytego wykonania lub niewykonania umowy wyłączają jedynie zdarzenia losowe związane z działaniem Siły Wyższej, o której mowa w § 16 umowy.

5. Łączna maksymalna wysokość kar umownych nie może przekroczyć 25% wartości brutto umowy określonej w § 2 ust. 1 umowy.

6. W przypadku, gdy szkoda przewyższy wartość kar umownych, Zamawiający może żądać odszkodowania przewyższającego wartość kar umownych na zasadach ogólnych.

§ 10

OCHRONA DANYCH OSOBOWYCH

1. Celem realizacji umowy Strony udostępniają sobie wzajemnie dane osobowe koordynatorów Umowy oraz innych osób realizujących Umowę, w zakresie :
   a) Wykonawca: imię i nazwisko, numer telefonu oraz adres mailowy pracownika, który będzie koordynować realizację Umowy ze strony Wykonawcy,
   b) Zamawiający: imiona i nazwiska, numery telefonów oraz adresy mailowe pracowników, którzy będą koordynować realizację Umowy ze strony Zamawiającego.

2. Z momentem udostępnienia danych Strona otrzymującą dane staje się ich niezależnym administratorem w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

3. Każda ze Stron oświadcza, że:
   a) jest administratorem danych będących przedmiotem udostępnienia oraz posiada podstawę prawną do ich udostępnienia;
   b) będzie przetwarzała udostępnione dane osobowe wyłącznie w celu realizacji Umowy i zgodnie z obowiązującymi przepisami prawa, w tym przepisami RODO;
   c) udostępnienie danych zostanie zrealizowane z zachowaniem najwyższych standardów bezpieczeństwa oraz z zapewnieniem przestrzegania zasad określonych w RODO.

4. Wykonawca oświadcza, iż przed zawarciem Umowy zapoznał się z Załącznikiem nr 4 do Umowy (Klauzula informacyjna RODO Zamawiającego) oraz przekazał klauzulę informacyjną Zamawiającego osobom reprezentującym go lub działającym w jego imieniu przy realizowaniu Umowy (obowiązek informacyjny przewidziany w art. 14 RODO). Wykonawca zobowiązuje się, że w przypadku wyznaczenia lub wskazania do działania przy wykonywaniu Umowy dodatkowych osób, najpóźniej wraz z przekazaniem Zamawiającemu danych osobowych tych osób, zrealizować obowiązki informacyjne w trybie art. 14 RODO zawarte w Załączniku nr 3 do Umowy.

5. Wykonawca zobowiązany jest do wypełnienia obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO, wobec Zamawiającego oraz osób, których dane zostały mu udostępnione.

§ 11
Powierzenie przetwarzania danych osobowych

W przypadku powierzenia przetwarzania danych osobowych Wykonawcy, Zamawiający wymaga podpisania przez Wykonawcę umowy powierzenia przetwarzania danych osobowych, której wzór stanowi Załącznik nr 6 do Umowy.

§ 12

POUFNOŚĆ DANYCH I INFORMACJI

1. Z zastrzeżeniem postanowień ust. 3, Wykonawca zobowiązuje się do zachowania w poufności wszelkich dotyczących Zamawiającego danych i informacji o charakterze określonym w art. 11 ust. 2 Ustawy z dnia 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji, jak też innych danych, co do których Zamawiający przekazał Wykonawcy zastrzeżenie o ich poufności, uzyskanych w jakikolwiek sposób (zamierzony lub przypadkowy) w związku z wykonywaniem umowy, bez względu na sposób i formę ich przekazania, nazywanych dalej łącznie "Informacjami Poufnymi".
2. Obowiązek, o którym mowa w ust. 1, obowiązuje Wykonawcę przez czas trwania umowy oraz przez okres 10 lat po jej rozwiązaniu, wygaśnięciu lub odstąpieniu od niej, bez względu na przyczynę.
3. Obowiązku zachowania poufności, o którym mowa w ust. 1, nie stosuje się do danych i informacji:
   1) dostępnych publicznie;
   2) otrzymanych przez Wykonawcę, zgodnie z przepisami prawa powszechnie obowiązującego, od osoby trzeciej bez obowiązku zachowania poufności;
   3) które w momencie ich przekazania przez Zamawiającego były już znane Wykonawcy bez obowiązku zachowania poufności;
   4) w stosunku do których Wykonawca uzyskał pisemną zgodę Zamawiającego na ich ujawnienie.
4. W przypadku, gdy ujawnienie Informacji Poufnych przez Wykonawcę jest wymagane na podstawie przepisów prawa powszechnie obowiązującego, Wykonawca poinformuje Zamawiającego o przyczynach i zakresie ujawnionych Informacji Poufnych. Poinformowanie takie powinno nastąpić w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej Zamawiającego, chyba że takie poinformowanie Zamawiającego byłoby sprzeczne z przepisami prawa powszechnie obowiązującego.
5. Wykonawca zobowiązuje się do:
   1) dołożenia właściwych starań w celu zabezpieczenia Informacji Poufnych przed ich utratą, zniekształceniem oraz dostępem nieupoważnionych osób trzecich;
   2) niewykorzystywania Informacji Poufnych w celach innych niż wykonanie umowy.
6. Wykonawca zobowiązuje się do poinformowania każdej z osób, przy pomocy których wykonuje umowę i które będą miały dostęp do Informacji Poufnych, o wynikających z umowy obowiązkach w zakresie zachowania poufności, a także do skutecznego zobowiązania i egzekwowania od tych osób obowiązków w zakresie zachowania poufności. Za ewentualne naruszenia tych obowiązków przez osoby trzecie Wykonawca ponosi odpowiedzialność, jak za własne działania.
7. W przypadku utraty lub zniekształcenia Informacji Poufnych lub dostępu nieupoważnionej osoby trzeciej do Informacji Poufnych, Wykonawca bezzwłocznie podejmie odpowiednie do sytuacji działania ochronne oraz poinformuje o sytuacji Zamawiającego. Poinformowanie takie, w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej Zamawiającego, powinno opisywać okoliczności zdarzenia, zakres i skutki utraty, zniekształcenia lub ujawnienia Informacji Poufnych oraz podjęte działania ochronne.
8. Po wykonaniu umowy oraz w przypadku rozwiązania umowy lub odstąpienia od umowy przez którąkolwiek ze Stron, Wykonawca bezzwłocznie zwróci Zamawiającemu lub komisyjnie usunie wszelkie Informacje Poufne w sposób uniemożliwiający ich przywrócenie. W przypadku komisyjnego usunięcia ww. Informacji, Wykonawca jest zobowiązany poinformować Zamawiającego o tym fakcie, bez zbędnej zwłoki.
9. Ustanowione umową zasady zachowania poufności Informacji Poufnych, jak również przewidziane w umowie kary umowne z tytułu naruszenia zasad zachowania poufności Informacji Poufnych, obowiązują zarówno podczas wykonania umowy, jak i po jej wygaśnięciu.
10. W przypadku udokumentowanego naruszenia zasad zachowania poufności Informacji Poufnych, Zamawiający naliczy karę umowną, o której mowa w § 9 ust. 1 pkt 3 umowy. W sytuacji, o której mowa w zdaniu pierwszym, Zamawiający będzie miał również prawo do rozwiązania umowy z przyczyn leżących po stronie Wykonawcy.

§ 13

WYMAGANIA BEZPIECZEŃSTWA INFORMACJI

1. Wykonawca oświadcza, iż przed zawarciem umowy zapoznał się z Załącznikiem nr 5 do umowy (Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych) oraz zobowiązuje się do przestrzegania zawartych w nim wymagań.
2. W przypadku udokumentowanego naruszenia wymagań bezpieczeństwa informacji, Zamawiający naliczy karę umowną, o której mowa w § 9 ust. 1 pkt 4 umowy. W sytuacji, o której mowa w zdaniu pierwszym, Zamawiający będzie miał również prawo do rozwiązania umowy z przyczyn leżących po stronie Wykonawcy.

§ 14

KONFLIKT INTERESÓW

1. Wykonawca oświadcza, że będzie realizował przedmiot umowy z zachowaniem zasad bezstronności oraz braku konfliktu interesów.
2. Strony przez konflikt interesów rozumieją:
   1) pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub są związane z tytułu przysposobienia, opieki lub kurateli z członkami organów zarządzających oraz pracownikami Zamawiającego zaangażowanymi w realizacje przedmiotu umowy;
   2) przed upływem 3 lat od dnia wszczęcia postępowania o udzielenie zamówienia pozostawały w stosunku pracy lub zlecenia z Zamawiającym;
   3) pozostają z Zamawiającym w takim stosunku prawnym lub faktycznym, że może to budzić uzasadnione wątpliwości co do bezstronności tych osób.
3. Wykonawca w przypadku zaistnienia bądź ujawnienia jakiejkolwiek okoliczności, o której mowa w ust. 2, niezwłocznie powiadomi o tej okoliczności Zamawiającego.
4. Zamawiający może żądać od Wykonawcy zamiany osoby, której dotyczy konflikt interesów, przy czym osoba zastępująca musi posiadać kwalifikacje nie niższe od osoby zastępowanej. W przypadku podwykonawcy jego kwalifikacje i doświadczenie muszą być takie same lub wyższe od kwalifikacji i doświadczenia podwykonawcy, którego dotyczy konflikt interesów.

§ 15

ROZSTRZYGANIE SYTUACJI SPORNYCH

1. W przypadku zaistnienia sporów między Stronami dotyczących realizacji przedmiotu umowy, Strony zobowiązują się do ich polubownego rozwiązywania.
2. W przypadku zaistnienia sporu dotyczącego wykonywania zobowiązań objętych umową, spór powinien zostać rozstrzygnięty przez przedstawicieli Stron. Z żądaniem rozstrzygnięcia sporu może wystąpić przedstawiciel każdej ze Stron, kierując żądanie do przedstawiciela drugiej ze stron umowy.
3. W przypadku, gdy postępowanie polubowne nie przyniesie ugody w terminie 30 dni kalendarzowych od skierowania żądania, o którym mowa w ust. 2, spór zostanie poddany pod rozstrzygnięcie Sądu właściwego dla siedziby Zamawiającego.
4. Wszelkiego rodzaju informacje przekazywane przez Strony związane z wynikłym sporem, dla zachowania swej ważności wymagają formy pisemnej.

§ 16

SIŁA WYŻSZA

1. Termin „Siła Wyższa" oznacza zewnętrzne, niemożliwe do przewidzenia i zapobieżenia zdarzenie występujące po zawarciu umowy, uniemożliwiające należyte wykonanie przez Stronę jej obowiązków, w szczególności takie jak katastrofy naturalne, wojny, ataki terrorystyczne, strajki.
2. Żadna Strona nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich zobowiązań w ramach umowy, jeżeli niewykonanie lub nienależyte wykonanie zobowiązań wynikających z umowy jest wynikiem działania Siły Wyższej.
3. Jeżeli zaistnieje Siła Wyższa, Strona, której dotyczą okoliczności Siły Wyższej bezzwłocznie zawiadomi drugą Stronę na piśmie o jej zaistnieniu i przyczynach. Strona, której dotyczą okoliczności Siły Wyższej

dołoży wszelkich starań, aby w terminie do 5 dni kalendarzowych od daty zawiadomienia przedstawić drugiej Stronie dokumentację, która wyjaśnia naturę i przyczyny zaistniałej okoliczności Siły Wyższej w takim zakresie, w jakim jest to możliwie osiągalne. Jeżeli po zawiadomieniu Strony nie uzgodnią inaczej w formie pisemnej, każda ze Stron będzie kontynuowała wysiłki w celu wywiązania się ze swoich zobowiązań.

4. W takim zakresie, w jakim niemożność wykonywania zobowiązań umownych wynika z Siły Wyższej oddziałującej na jedną ze Stron, druga Strona również nie będzie odpowiedzialna za wykonanie swoich zobowiązań.

§ 17

POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych umową mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2019 r., poz. 1145 ze zm.).
2. Wszelkie zmiany postanowień umowy wymagają formy pisemnej pod rygorem nieważności.
3. umowę sporządzono w trzech jednobrzmiących egzemplarzach, z których dwa otrzymuje Zamawiający, a jeden Wykonawca.

§ 18

ZAŁĄCZNIKI DO UMOWY

Integralną część umowy stanowią:

Zalcznikni nr 1 - Opis przedmiotu zamówienia

Załącznik nr 2 – Protokół odbioru;

Załącznik nr 3 – Oferta Wykonawcy;

Załącznik nr 4 - Informacje dotyczące przetwarzania danych osobowych w związku z realizacją umowy;

Załącznik nr 5 - Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych.

Załacznik nr 6 – Umowa powierzenia przetwarzania danych osobowych (wzór)

ZAMAWIAJĄCY **WYKONAWCA**

Data / podpis *Data / podpis*

Załącznik nr 1 do umowy nr .../CIS-WAZ.2720.....2021 z dnia 2021

Opis przedmiotu zamówienia

Załącznik nr 2 do umowy nr .../CIS-WAZ.2720.....2021 z dnia 2021

PROTOKÓŁ ODBIORU
aktualizacji systemu eBiuro

I. W przeprowadzeniu testów uczestniczyli:

Ze strony Zamawiającego - Centrum Informatyki Statystycznej,

1.....

2.....

(imię i nazwisko - stanowisko)

Ze strony Wykonawcy - .....:

1.....

2.....

(imię i nazwisko - stanowisko)

Na podstawie umowy nr **.../CIS-WAZ.2720.....2021** z dnia ..... 2021 r., której przedmiotem jest aktualizacja systemu eBiuro w zakresie dostosowania apletu kryptograficznego systemu eBiuro do nowych certyfikatów oraz do funkcji skrótu SHA-256, przedstawiciele Zamawiającego i Wykonawcy potwierdzją, że

II. Ustalenia:

1. Wykonawca zgodnie z umową w ramach przedmiotu umowy wykonał:
   .....
   .....
2. Zamawiający w wyniku przeprowadzonych testów mających na celu potwierdzenie prawidłowości działania przedmiotu mowy stwierdza, że:
   .....
   .....
3. Zamawiający wzywa do usunięcia wyżej wskazanych rozbieżności w terminie do:.....

III. Końcowy wynik odbioru:

1. Pozytywny*) - Zamawiający po wykonaniu testów dokonuje odbioru przedmiotu umowy objętego niniejszym protokołem bez zastrzeżeń i stwierdza, że usługa została wykonana w terminie, zgodnie z wymogami określonymi w umowie.
2. Pozytywny*) - Zamawiający po wykonaniu testów dokonuje odbioru przedmiotu umowy objętego niniejszym protokołem bez zastrzeżeń i stwierdza, że usługa została wykonana po terminie wymaganym w umowie. Opóźnienie liczone od dnia .....
3. Negatywny*) – *uzasadnienie*.....

Na tym protokół zakończono i podpisano:

*) - *niepotrzebne skreślić*

.....
(przedstawiciele Zamawiającego)
data / podpis

.....
(przedstawiciele Wykonawcy)
data / podpis

Załącznik nr 3 do umowy nr .../CIS-WAZ.2720.....2021 z dnia 2021

OFERTA WYKONAWCY

Załącznik nr 4

do umowy nr .../CIS-WAZ.2720.....2021 z dnia 2021

Informacje dotyczące przetwarzania danych osobowych

w związku z realizacją umowy

W związku z realizacją wymogów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[3] (RODO), administrator informuje o zasadach oraz o przysługujących Pani/Panu prawach związanych z przetwarzaniem Pani/Pana danych osobowych.

I. Administrator

Administratorem Pani/Pana danych osobowych jest Dyrektor Centrum Informatyki Statystycznej z siedzibą al. Niepodległości 208, 00-925 Warszawa.

II. Inspektor ochrony danych

Z inspektorem ochrony danych (IOD) może się Pani/Pan kontaktować:

1. pocztą tradycyjną na adres: IOD CIS, al. Niepodległości 208, 00-925 Warszawa,
2. pocztą elektroniczną na adres e-mail: IOD_CIS@stat.gov.pl.

Do IOD należy kierować wyłącznie sprawy dotyczące przetwarzania Pani/Pana danych osobowych przez administratora, w tym realizacji Pani/Pana praw wynikających z RODO.

III. Cele oraz podstawa prawna przetwarzania Pani/Pana danych osobowych

Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6. ust. 1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku ciążącego na administratorze, tj. w celu realizacji umowy zawartej w wyniku udzielenia zamówienia publicznego, zgodnie z przepisami ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2020, z późn. zm.), dalej „ustawa Pzp".

IV. Odbiorcy danych osobowych

Odbiorcą Pani/Pana danych osobowych będą podmioty współpracujące z Administratorem, w tym dostawcy usług technicznych i organizacyjnych umożliwiających wykonanie umowy oraz przechowywanie dokumentacji jej dotyczącej, osoby i podmioty upoważnione na podstawie przepisów prawa powszechnie obowiązującego.

V. Okres przechowywania danych osobowych

Pani/Pana dane osobowe będą przechowywane przez 4 lata od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata przez cały czas trwania umowy oraz do czasu przedawnienia ewentualnych roszczeń wynikających z umowy. Ponadto dane osobowe będą przechowywane zgodnie z przepisami ustawy o narodowym zasobie archiwalnym i archiwach[4] oraz rozporządzenia w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych[5] i przepisami wewnętrznymi administratora.

VI. Prawa osoby, której dane osobowe dotyczą

Przysługuje prawo do:

1. dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
2. sprostowania (poprawiania) danych osobowych;
3. usunięcia danych osobowych;
4. do sprzeciwu wobec przetwarzania danych osobowych;

[3] 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.)

[4] Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164)

[5] Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej (Dz.U. z 2019 r. poz. 246)

5. ograniczenia przetwarzania danych osobowych;
6. wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa), jeżeli Pani/Pana zdaniem przetwarzanie Pani/Pana danych osobowych narusza przepisy RODO.

VII. Dobrowolność/ Obowiązek podania danych osobowych

Obowiązek podania przez Panią/Pana danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego oraz zawarciem i realizacją umowy. Konsekwencje niepodania danych osobowych wynikają z ustawy Pzp.

VIII. Zautomatyzowane podejmowanie decyzji, w tym profilowanie

Pani/Pana dane osobowe nie będą profilowane ani też nie będą podlegały zautomatyzowanemu podejmowaniu decyzji.

Załącznik nr 5.

do umowy nr .../CIS-WAZ.2720.....2021 z dnia 2021

Wymagania bezpieczeństwa informacji

dla kontrahentów i osób zewnętrznych

I. Wstęp

1. Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych (Wymagania) stanowią element Systemu Zarządzania Bezpieczeństwem Informacji w statystyce publicznej oraz część integralną zawieranej umowy.

2. Wymagania stanowią zbiór zasad obowiązujących:

   a) kontrahentów realizujących dostawy lub świadczących usługi na rzecz Głównego Urzędu Statystycznego (GUS), Centrum Informatyki Statystycznej (CIS), Zakładu Wydawnictw Statystycznych (ZWS), Centralnej Biblioteki Statystycznej (CBS) w Warszawie;

   b) osób zewnętrznych, które uzyskują dostęp do zasobów informacyjnych na podstawie odrębnych przepisów prawa lub umowy cywilno-prawnej.

3. Zgodnie z zapisami Polityki Bezpieczeństwa Informacji Statystyki Publicznej, w przypadku, gdy kontrahent w trakcie wykonywania umowy ma lub może mieć dostęp do zasobów informacyjnych jssp, w umowach z kontrahentami wprowadzana jest klauzula dotycząca obowiązku przestrzegania bezpieczeństwa informacji. Klauzula ta zawiera zobowiązanie kontrahenta do przestrzegania Wymagań bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych, ochrony udostępnionych zasobów informacyjnych poprzez ograniczenie ich kopiowania i udostępniania oraz do ich zwrotu lub zniszczenia w momencie zakończenia umowy:

4. Do zawieranych umów z kontrahentami załączany jest wyciąg z Wymagań bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych, obejmujący rozdziały od II do X.

II. Słownik pojęć

aktywa – wszystko, co ma wartość dla jednostek służb statystyki publicznej i z tego względu wymaga ochrony [na podstawie normy PN-ISO/IEC 27000];

jednostka – rozumiane rozdzielnie GUS i pozostałe jednostki służb statystyki publicznej;

komórka organizacyjna GUS – departament, biuro, wydział, samodzielne stanowisko pracy w Głównym Urzędzie Statystycznym;

jednostka służb statystyki publicznej – jednostki służb statystyki publicznej podległe i podporządkowane Prezesowi GUS (GUS, CBS, CIS, Zakład Wydawnictw Statystycznych, urzędy statystyczne oraz CBiES);

Incydent bezpieczeństwa informacji – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji [na podstawie normy PN ISO/IEC 27000];

Pełnomocnik ds. SZBI – dyrektor komórki organizacyjnej GUS właściwej ds. bezpieczeństwa informacji powołany przez Prezesa GUS na mocy zarządzenia wewnętrznego nr 8 Prezesa GUS z dnia 20 lutego 2020 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w statystyce publicznej [definicja własna];

System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne [na podstawie art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne];

Właściciel Aktywu – dyrektor komórki organizacyjnej GUS/dyrektor jssp;

III. Zasady zachowania poufności danych i informacji

1. Kontrahenci i osoby z zewnątrz zobowiązują się do zachowania w poufności wszelkich danych i informacji, niezależnie od sposobu ich pozyskania (zamierzony lub przypadkowy) i bez względu na sposób i formę ich przekazania.

2. Obowiązek, o którym mowa w pkt 1, jeżeli przepisy prawa nie stanowią inaczej, obowiązuje przez okres 10 lat po jej rozwiązaniu, wygaśnięciu lub odstąpieniu od niej, bez względu na przyczynę.

3. Obowiązku zachowania poufności nie stosuje się do danych i informacji:

1) dostępnych publicznie;

2) otrzymanych zgodnie z przepisami prawa powszechnie obowiązującego, od osoby trzeciej bez obowiązku zachowania poufności;

3) które w momencie ich przekazania były już znane kontrahentowi/ osobie z zewnątrz bez obowiązku zachowania poufności;

4) w stosunku do których kontrahent/ osoba z zewnątrz uzyskał(a) pisemną zgodę na ich ujawnienie.

4. W przypadku, gdy ujawnienie wszelkich danych i informacji, co do których kontrahenci i osoby z zewnątrz zobowiązali się zachować w poufności jest wymagane na podstawie przepisów prawa powszechnie obowiązującego, kontrahent/ osoba z zewnątrz poinformuje osobę wskazaną do kontaktu o przyczynach i zakresie ujawnionych Informacji Poufnych. Poinformowanie takie powinno nastąpić w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej osoby wskazanej do kontaktu, chyba że takie poinformowanie byłoby sprzeczne z przepisami prawa powszechnie obowiązującego.

5. Kontrahent/ osoba z zewnątrz zobowiązuje się do niewykorzystywania Informacji Poufnych w celach innych niż cel, dla którego zostały mu ujawnione.

6. Kontrahent/ osoba z zewnątrz zobowiązuje się do dołożenia właściwych starań w celu zabezpieczenia Informacji Poufnych przed ich utratą, zniekształceniem oraz dostępem nieupoważnionych osób trzecich.

7. W przypadku utraty lub zniekształcenia Informacji Poufnych lub dostępu nieupoważnionej osoby trzeciej do Informacji Poufnych, Kontrahent/ osoba z zewnątrz bezzwłocznie podejmie odpowiednie do sytuacji działania ochronne oraz poinformuje osobę wskazaną do kontaktu o przyczynach i zakresie ujawnionych Informacji Poufnych. Poinformowanie takie powinno nastąpić w formie pisemnej lub w formie wiadomości wysłanej na adres poczty elektronicznej osoby wskazanej do kontaktu, chyba że takie poinformowanie byłoby sprzeczne z przepisami prawa powszechnie obowiązującego.

IV. Ochrona danych osobowych

1. Kontrahent/ osoba z zewnątrz zobowiązuje się przetwarzać powierzone dane osobowe zgodnie z określonym celem ich przetwarzania, rozporządzeniem RODO[1] oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą;

2. Kontrahent/ osoba z zewnątrz zobowiązuje się przed zawarciem umowy wypełnić obowiązki informacyjne przewidziane w art. 13 lub art. 14 ogólnego rozporządzenia o ochronie danych (RODO) oraz w zakresie określonym w załączniku do umowy wobec każdej osoby fizycznej, od której dane osobowe bezpośrednio lub pośrednio pozyskał w celu wpisania jej do treści umowy, jako dane osoby reprezentującej go lub działającej w jego imieniu przy realizowaniu umowy. Kontrahent/ osoba z zewnątrz zobowiązuje się w przypadku wyznaczenia lub wskazania do działania przy wykonywaniu umowy osób innych niż wymienione w jej treści, najpóźniej wraz z przekazaniem danych osobowych tych osób, zrealizować obowiązki informacyjne w trybie art. 13 lub art. 14 RODO oraz określone w załączniku do umowy.

3. W przypadku powierzenia przetwarzania danych osobowych kontrahentowi/ osobie z zewnątrz, wymaga się podpisania przez kontrahenta/ osobę z zewnątrz umowy powierzenia przetwarzania danych osobowych.

4. umowy powierzenia muszą zawierać szczegółowe uregulowania w zakresie przetwarzania powierzonych danych osobowych i ich ochrony.

[1] 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 (ogólne rozporządzenie o ochronie danych).

V. Bezpieczeństwo fizyczne i środowiskowe

1. Obowiązuje zakaz wnoszenia na teren siedziby GUS jakichkolwiek materiałów niebezpiecznych, których posiadanie i przechowywanie jest zabronione prawem. W przypadku stwierdzenia ich obecności w pomieszczeniach, dyrektor komórki organizacyjnej GUS właściwej ds. administracyjnych lub dyrektor jednostki odpowiedzialny jest za doprowadzenie do ich usunięcia.

2. Wyróżnia się następujące obszary bezpieczne:

a) strefa chroniona (strefa administracyjna),

b) strefa zabezpieczona (strefa bezpieczeństwa);

3. Wydziela się obszar dostaw i załadunku. Dostęp do pomieszczeń magazynowych jest nadzorowany. Prowadzona jest kontrola ruchu osobowego i materiałowego.

4. Pomieszczenia, w których przetwarzane są informacje wrażliwe dla statystyki publicznej, są wyposażone w zamek mechaniczny lub elektroniczny.

Strefa chroniona (strefa administracyjna):

1) na granicach strefy chronionej (strefy administracyjnej) funkcjonuje kontrola dostępu (tripody lub czytniki na drzwiach);

2) wejście do strefy chronionej (strefy administracyjnej), kontrahenta/ osoby z zewnątrz wymaga wydania identyfikatora i jego zaewidencjonowania. Ewidencjonowanie wejść do strefy chronionej (strefy administracyjnej) odbywa się poprzez dokonanie przez ochronę/recepcję lub wyznaczonego pracownika wpisu w ewidencji wejść i wyjść do strefy chronionej (strefy administracyjnej) oraz wydanie identyfikatora/karty magnetycznej typu „Gość";

3) za wszelkie naruszenia bezpieczeństwa informacji przez osoby, które uzyskały dostęp do strefy chronionej (strefy administracyjnej) odpowiada dyrektor komórki organizacyjnej GUS/ dyrektor jednostki lub pracownik wnioskujący o przyznanie identyfikatora typu „Gość";

4) osoby, bądź przedstawiciele podmiotów zewnętrznych świadczących usługi, w szczególności kurierzy, zaopatrzeniowcy, serwisanci poruszają się w granicy strefy chronionej (strefy administracyjnej) wyłącznie pod nadzorem wyznaczonego pracownika;

5) szczegóły dotyczące wejścia do strefy chronionej GUS określone zostały w zarządzeniu Dyrektora Generalnego GUS w sprawie „Zasad organizacji ruchu osób i pojazdów oraz zabezpieczenia budynku i mienia Głównego Urzędu Statystycznego".

Strefa zabezpieczona (strefa bezpieczeństwa):

1) strefa zabezpieczona (strefa bezpieczeństwa) to wydzielona część strefy chronionej (strefy administracyjnej) wyposażona w dodatkowe, niezależne systemy zabezpieczeń. Rodzaj zabezpieczeń określa Właściciel aktywów przechowywanych w danym pomieszczeniu, stosownie do ich rodzaju i wartości;

2) zasoby znajdujące się w strefie zabezpieczonej (strefie bezpieczeństwa) podlegają szczególnej ochronie i są zabezpieczone przed pożarem;

3) strefy zabezpieczone (strefy bezpieczeństwa) posiadają zabezpieczenia zapewniające ochronę nośników informacji. Serwerownie wyposażone są w system sygnalizujący wystąpienie pożaru oraz system klimatyzacji. Strefy zabezpieczone (strefy bezpieczeństwa) są chronione systemem sygnalizacji włamania i napadu oraz wyposażone w urządzenia pozwalające na alarmowe powiadomienie obsługi i ochrony. System sygnalizacji napadu i włamania zapewnia skuteczne przekazanie sygnału o realnym zagrożeniu do wskazanych osób, miejsc i urządzeń;

4) wstęp do strefy zabezpieczonej (strefy bezpieczeństwa) jest ograniczony tylko do osób, które uzyskały stosowne uprawnienia wydane przez Właściciela aktywów przechowywanych w danym pomieszczeniu. Wejście oraz wyjście ze stref bezpieczeństwa rejestrowane jest przez system kontroli dostępu lub wyznaczonego przez Właściciela aktywów przechowywanych w danym pomieszczeniu pracownika. Wyznaczony pracownik rejestruje tożsamość osób oraz czas ich wejścia i wyjścia;

5) dopuszcza się przebywanie kontrahenta i osób z zewnątrz bez uprawnień dostępu do strefy zabezpieczonej (strefy bezpieczeństwa) tylko w wyjątkowych przypadkach, w celu wykonania działań serwisowych i innych określonych w regulacjach wewnętrznych (audyt), za zezwoleniem Właściciela aktywów przechowywanych w danym pomieszczeniu. Przebywanie osób bez uprawnień dostępu do strefy zabezpieczonej (strefy bezpieczeństwa) możliwe jest wyłącznie pod nadzorem pracownika, który posiada uprawnienia dostępu do danej strefy;

6) wnoszenie i wynoszenie do i ze strefy zabezpieczonej (strefy bezpieczeństwa) elektronicznych nośników informacji jest uzasadnione (np.: wynikające z procedury dot. kaset backup) lub nadzorowane;

7) w strefie zabezpieczonej (strefie bezpieczeństwa) zabronione jest korzystanie z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach mobilnych w celu rejestracji obrazu lub dźwięku bez pisemnej zgody Właściciela aktywów przechowywanych w danym pomieszczeniu lub wyznaczonego przez niego pracownika.

VI. Dostęp do zasobów systemów teleinformatycznych

1. Dostęp do systemu teleinformatycznego uzyskuje wyłącznie uprawniony kontrahent/osoba z zewnątrz. Dostęp jest indywidualnie zdefiniowany. Kontrahent/ osoba z zewnętrz ma dostęp jedynie do zasobów, które są niezbędne.
2. Kontrola dostępu dla kontrahenta/ osoby z zewnątrz do systemu teleinformatycznego realizowana jest poprzez mechanizmy uwierzytelniania.
3. Kontrahent/osoba z zewnątrz uzyskują uprawnienia w zakresie korzystania z systemu teleinformatycznego na wniosek Właściciela aktywu. Nie dotyczy to organów umocowanych prawnie.
4. Uprawnienia dla kontrahenta/osoby z zewnątrz nie mogą być przyznane na czas nieokreślony i podlegają aktualizacji co 90 dni.
5. Warunki korzystania z połączenia wewnętrznej sieci statystyki publicznej z systemami zewnętrznymi regulują podpisane umowy, szczegółowo precyzujące warunki techniczne i funkcjonalne połączenia.

VII. Dostęp do zasobów z sieci innych instytucji

1. Kontrahent/osoba z zewnątrz otrzymują dostęp do sieci teleinformatycznej na mocy przepisów prawa.
2. Kontrahent/osoba z zewnątrz mogą uzyskać uprawnienia w zakresie korzystania z systemu teleinformatycznego na wniosek Właściciela aktywu. Nie dotyczy to organów umocowanych prawnie;
3. Wniosek o dostęp do sieci statystyki publicznej powinien zawierać informacje o celu podłączenia, przewidywanej liczbie podłączonych stanowisk i użytkowników, metodzie zabezpieczenia przed nieautoryzowanym dostępem i używanym antywirusie.
4. Przed wydaniem decyzji o zgodzie na podłączenie do sieci statystyki publicznej, Prezes GUS zasięga opinii Pełnomocnika ds. SZBI.
5. Specyfikacja techniczna połączenia jest załącznikiem do porozumienia lub zawieranej umowy.
6. Specyfikacja powinna zawierać w szczególności następujące ustalenia:
   a) szyfrowane połączenie powinno być zabezpieczone odpowiednim certyfikatem,
   b) zestawione połączenie powinno być jedynie między ściśle określonymi adresami IP podłączanej sieci oraz ściśle określonymi adresami IP sieci wewnętrznej statystyki publicznej oraz dla ściśle określonych portów przypisanych do adresów w sieci teleinformatycznej statystyki publicznej,
   c) każdorazowe zestawienie połączenia między podłączaną siecią teleinformatyczną podmiotu zewnętrznego, a siecią teleinformatyczną statystyki publicznej należy autoryzować loginem i hasłem lub certyfikatem oraz logowaniem,
   d) zasoby udostępniane użytkownikom z innych instytucji obejmują wyłącznie dostęp do aplikacji. Nie mogą być udostępniane takie zasoby jak serwery plików lub poczta elektroniczna;
7. Właściciel aktywu zatwierdza uprawnienia użytkowników z innych instytucji do danej aplikacji będącej w zasobach statystyki publicznej. Użytkownicy z innych instytucji nie mogą posiadać praw administracyjnych.

VIII. Ochrona przed szkodliwym oprogramowaniem i kodem mobilnym

1. Wszystkie elektroniczne nośniki informacji dostarczone z zewnątrz do Zamawiającego są dopuszczone do używania po wcześniejszym sprawdzeniu ich programem antywirusowym na komputerze odizolowanym od sieci Statystki publicznej.
2. Wszystkie pliki przed wysłaniem pocztą elektroniczną lub przekazaniem stronom trzecim (kontrahentowi/ osobie zewnętrznej) są testowane oprogramowaniem antywirusowym.

IX. Odbiór systemu

1. Przed przekazaniem do użytkowania oprogramowania opracowanego na rzecz statystyki publicznej, osoby je opracowujące muszą usunąć wszystkie specjalne ścieżki dostępu tak, aby dostęp był możliwy jedynie z zastosowaniem zasad bezpieczeństwa informacji. Oznacza to, że muszą być usunięte wszystkie nieudokumentowane funkcje pozwalające ominąć system zabezpieczeń. Muszą zostać również usunięte wszystkie uprawnienia systemowe ustanowione dla potrzeb prowadzenia prac nad oprogramowaniem, lecz zbędne w środowisku produkcyjnym. Powinno to być udokumentowane oświadczeniem kontrahenta, w którym potwierdza usunięcie powyższych nadmiarowych funkcjonalności.
2. W przypadku podjęcia decyzji o przechowywaniu kodu źródłowego pisanego na zamówienie statystyki publicznej poza siedzibą Zamawiającego, konieczne jest zawarcie umów depozytowych dotyczących takiego kodu źródłowego z podmiotami niezależnymi od dostawcy oprogramowania. umowy te powinny określać niezależny podmiot, któremu twórca oprogramowania dostarczy kod źródłowy i wszystkie jego aktualizacje. Powinny też określać sytuacje, w których kod źródłowy zostanie udostępniony statystyce publicznej, jak na przykład upadłość lub likwidacja dostawcy oprogramowania lub niewywiązywanie się przez niego z postanowień umowy dotyczących aktualizacji oprogramowania.

X. Naruszenia bezpieczeństwa informacji oraz wnioski dotyczące bezpieczeństwa informacji

1. Zasady bezpieczeństwa informacji obowiązują wszystkich kontrahentów i osoby z zewnątrz, które otrzymują dostęp do zasobów informacyjnych statystyki publicznej.
2. Kontrahenci i osoby z zewnątrz mający dostęp do zasobów informacyjnych na podstawie odrębnych przepisów/ upoważnień, przed przyznaniem dostępu do zasobów informacyjnych otrzymują do zapoznania się *Wymagania bezpieczeństwa informacji dla kontrahentów i osób zewnętrznych*.
3. Odpowiedzialność za bezpieczeństwo informacji statystyki publicznej obejmuje działania, które miały miejsce w siedzibie GUS oraz wszelkie sytuacje, w których informacje związane z działalnością są przetwarzane poza jej siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci teleinformatycznej statystyki publicznej.
4. Kontrahent i osoba z zewnątrz mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, procedury i instrukcje dotyczące bezpieczeństwa informacji do osoby wskazanej do kontaktu, która przekazuje te informacje do Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni w jssp, w którym aktualnie realizowane są przez nich zadania rzecz statystyki.
5. Każdy incydent związany z bezpieczeństwem informacji w GUS, CIS, ZWS i CBS powinien być zgłoszony natychmiast po jego wykryciu.
6. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji przez pracowników statystyki publicznej odbywa się przez dedykowaną stronę www (http://serwisdesk), e-mailem: serwisdesk@stat.gov.pl bądź, w godzinach pracy urzędu, telefonicznie (22 608 3689);
7. W przypadku zmian w przepisach Wymagań, kontrahent i osoba z zewnątrz zostaną o tym poinformowani na piśmie.

Załącznik nr 6

do umowy nr .../CIS-WAZ.2720.....2021 z dnia 2021
Załącznik nr 6

Umowa powierzenia przetwarzania danych osobowych
wzór

Zawarta w dniu .....2021 r. w Warszawie pomiędzy:
Centrum Informatyki Statystycznej, al. Niepodległości 208, 00-925 Warszawa, NIP: 701-023-61-79, REGON: 142396858, zwanym dalej „Zamawiającym" lub „Administratorem Danych", reprezentowanym przez:
..... – .....

a
....., zwanym dalej „Wykonawcą"

zwanych dalej łącznie „Stronami" lub osobno „Stroną".

§ 1

1. Przedmiotem Umowy jest określenie warunków, na jakich Wykonawca będzie miał dostęp do danych osobowych przekazanych w ramach realizacji umowy nr ..... /CIS-WAZ.2721.....2021 oraz wyłącznie w celu wykonywania czynności niezbędnych do realizacji postanowień umownych w ramach wykonywania przedmiotu Umowy.
2. Zakres powierzenia przetwarzania danych osobowych obejmuje: imiona i nazwiska, nr telefonów, adresy e-mail pracowników.
3. Zamawiający powierza Wykonawcy dane osobowe w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (w dalszej „RODO") do przetwarzania na zasadach i w celu określonym w Umowie.
4. Zamawiający powierza do przetwarzania dane osobowe, a Wykonawca zobowiązuje się do ich przetwarzania zgodnego z Umową, RODO, ustawą o ochronie danych osobowych i innymi przepisami prawa powszechnie obowiązującego dotyczącymi ochrony danych osobowych.
5. Wykonawca zobowiązany jest przy wykonywaniu czynności określonych w Umowie do zachowania w tajemnicy wszelkich informacji lub danych osobowych, do których będzie miał dostęp w związku z dokonywaniem czynności przy przetwarzaniu danych osobowych zarówno w trakcie Umowy jak i po jej ustaniu, a w szczególności zobowiązuje się:
   1) nie kopiować (na jakichkolwiek nośnikach), nie odtwarzać, nie rozprowadzać ani nie rozpowszechniać lub udostępniać w żaden inny sposób, na rzecz jakichkolwiek osób trzecich, jakichkolwiek informacji lub danych osobowych przetwarzanych w ramach Umowy lub zbieranych w celu włączenia do zbioru danych w związku z realizacją Umowy;
   2) nie wykorzystywać powyższych informacji lub danych osobowych na swoją własną korzyść lub korzyść osób trzecich;
   3) nie ujawniać środków ochrony fizycznej, technicznej i organizacyjnej oraz zabezpieczeń teleinformatycznych stosowanych przez Administratora Danych w odniesieniu do zbioru powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
6. Wykonawca nie może powierzyć wykonania zadań wynikających z Umowy stronie trzeciej bez uprzedniej pisemnej zgody Zamawiającego, zastrzeżeniem § 9.
7. Wykonawca odpowiada za szkody wyrządzone wskutek niewykonania lub nienależytego wykonania obowiązków wynikających z Umowy oraz z obowiązujących przepisów, w tym za szkody powstałe w wyniku udostępnienia danych osobowych osobom nieupoważnionym, ich zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących przepisów, nieuprawnioną zmianą danych, uszkodzeniem lub zniszczeniem, które nastąpiły z winy Wykonawcy. Odpowiedzialność Wykonawcy ograniczona jest do wysokości szkody rzeczywistej.
8. Zgodnie z art. 28 ust. 10 RODO jeśli Wykonawca bez wiedzy i zgody Zamawiającego samodzielnie określi nowe cele i sposoby przetwarzania danych osobowych przetwarzanych w ramach realizacji Umowy, zobowiązany jest przyjąć na siebie odpowiedzialność wobec osób, których dane są przetwarzane w związku z Usługą z

tytułu jakiejkolwiek szkody poniesionej przez te osoby, a wynikającej lub związanej z naruszeniem przez Wykonawcę przepisów prawa powszechnie obowiązującego dotyczących ochrony danych osobowych lub postanowień Umowy.

§ 2

Na podstawie Umowy Wykonawca jest uprawniony do przetwarzania danych osobowych, w ramach Umowy tylko w takim celu i w takim zakresie, w jakim jest to niezbędne do wykonania Umowy, zgodnie z § 1 ust. 1 Umowy.

§ 3

1. Wykonawca przy przetwarzaniu danych osobowych zobowiązany jest stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczy dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. W celu wykonania obowiązku, o którym mowa w zdaniu poprzedzającym, Wykonawca zobowiązany jest prowadzić dokumentację opisującą sposób przetwarzania danych osobowych oraz wyznaczy Inspektora Ochrony Danych (zwany dalej „IOD") lub będzie wykonywał obowiązki związane z ochroną danych osobowych samodzielnie.
2. Wykonawca zobowiązany jest do przestrzegania i stosowania w szczególności następujących warunków realizacji Umowy:
   1) przetwarzania danych osobowych w zakresie wskazanym w § 1 ust. 1 Umowy bez możliwości dalszego przekazywania danych, z wyłączeniem okoliczności wskazanych w § 9 Umowy;
   2) Wykonawca zobowiązuje się do przetwarzania danych osobowych tylko w obszarze Europejskiego Obszaru Geograficznego;
   3) zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, w tym tajemnicy statystycznej - jeżeli dotyczy, a także by każda osoba fizyczna działająca z upoważnienia Wykonawcy, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie;
   4) nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały dane osobowe w celu realizacji Umowy;
   5) podejmowania wszelkich środków wymaganych art. 32 RODO, a w szczególności wdrożenia odpowiednich środków fizycznych, technicznych i organizacyjnych dla zapewnienia odpowiedniego stopnia bezpieczeństwa odpowiadającemu ryzyku przetwarzania tych danych;
   6) zapewnienia pomocy Zamawiającemu w zakresie wywiązywania się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w przedmiocie jej praw określonych w RODO poprzez odpowiednie środki techniczne i organizacyjne przy uwzględnieniu charakteru dozwolonego przetwarzania oraz dostępnych Wykonawcy informacji i danych;
   7) udostępniania Zamawiającemu wszelkich informacji niezbędnych do wykazania spełnienia obowiązków Wykonawcy wynikających z Umowy i przepisów powszechnie obowiązujących oraz umożliwienia Zamawiającemu lub audytorowi upoważnionemu przez Zamawiającego przeprowadzenie audytów i inspekcji oraz współpracy w tym zakresie na zasadach określonych w § 4 Umowy;
   8) jeżeli zdaniem Wykonawcy wydane w trakcie audytu lub inspekcji polecenia stanowią naruszenie przepisów RODO lub innych przepisów o ochronie danych - niezwłocznego poinformowania Zamawiającego;
   9) w przypadku stwierdzenia jakiejkolwiek sytuacji stanowiącej naruszenie bezpieczeństwa danych osobowych przyjęcie zasad postępowania zgodnie z § 5 Umowy.
3. W zakresie przestrzegania i stosowania zabezpieczeń fizycznych i organizacyjno-technicznych Wykonawca ponosi odpowiedzialność jak administrator danych, z wyłączeniem odpowiedzialności za sposób, w jaki Zamawiający wykorzystuje swoją bazę i przetwarza w niej dane osobowe, chyba że Wykonawca będzie korzystać z systemów teleinformatycznych udostępnionych przez Zamawiającego z zachowaniem zasad funkcjonujących u Zamawiającego.
4. Wykonawca może wykonywać Usługę z wykorzystaniem systemów teleinformatycznych udostępnionych przez Zamawiającego na zasadach określonych odrębnie.
5. W przypadku korzystania z urządzeń i systemów informatycznych służących do przetwarzania danych osobowych, innych niż wskazane w ust. 4, będących własnością lub znajdujących się w posiadaniu

Wykonawcy, Wykonawca oświadcza, że używane do przetwarzania danych osobowych urządzenia i systemy zapewniają adekwatny sposób bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o którym mowa w art. 32 RODO.

§ 4

1. Zamawiający ma prawo do kontroli Wykonawcy w zakresie warunków przetwarzania powierzonych danych osobowych w celu sprawdzenia czy przetwarzanie przez Wykonawcę przekazanych danych osobowych jest zgodne z postanowieniami RODO, Umowy oraz przepisami prawa powszechnie obowiązującego dotyczącymi ochrony danych osobowych.
2. Warunkiem przeprowadzenia kontroli jest pisemne zawiadomienie Wykonawcy w terminie nie krótszym niż 7 dni przed planowanym terminem kontroli, z zastrzeżeniem ust. 3.
3. Kontrola może nastąpić z pominięciem zawiadomienia, o którym mowa w ust. 2, w przypadku uzasadnionego podejrzenia lub powzięcia informacji od osób trzecich o rażących naruszeniach Wykonawcy w zakresie ochrony danych osobowych lub zapisów Umowy.
4. Z czynności kontrolnych sporządza się protokół, którego jeden egzemplarz doręcza się Wykonawcy.
5. Wykonawca w terminie 3 dni od daty otrzymania może wnieść zastrzeżenia do protokołu.
6. Zamawiający zastrzega sobie możliwość przeprowadzenia kontroli, o której mowa w ust. 1 i 3, także u Podwykonawców Wykonawcy, a Wykonawca zobowiązany jest zapewnić możliwość przeprowadzenia czynności kontrolnych u Podwykonawców.

§ 5

1. Wykonawca każdorazowo poinformuje bez zbędnej zwłoki, nie później niż w terminie 24 godzin, Zamawiającego o wszelkich zdarzeniach mogących skutkować odpowiedzialnością Zamawiającego lub Wykonawcy na podstawie przepisów związanych z ochroną danych osobowych, także o kontrolach dotyczących przetwarzania danych osobowych lub świadczonych usług prowadzanych przez osoby trzecie / podmioty trzecie.
2. W przypadku stwierdzenia jakiejkolwiek sytuacji stanowiącej naruszenie bezpieczeństwa danych osobowych Wykonawca zobowiązany jest niezwłocznie, nie później niż w terminie 24 godzin:
   1) poinformować o tym Administratora Danych, poprzez zawiadomienie Inspektora Ochrony Danych wyznaczonego przez Administratora Danych, podając wszelkie informacje dotyczące naruszenia;
   2) ustalić przyczynę naruszenia;
   3) podjąć wszelkie czynności mające na celu usunięcie przyczyn i skutków naruszenia oraz zabezpieczenie danych osobowych w sposób należyty przed dalszymi naruszeniami;
   4) zebrać wszystkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności naruszenia i przeciwdziałaniu podobnym naruszeniom w przyszłości.

§ 6

1. Strony zobowiązują się do zachowania w poufności wszelkich danych i informacji, które powzięły w trakcie obowiązywania Umowy oraz w związku z jej realizacją, chyba że druga Strona zwolni Stronę z takiego obowiązku lub obowiązek ich ujawnienia wynika z przepisów prawa powszechnie obowiązującego.
2. Postanowienia ust. 1, pozostają w mocy również po wygaśnięciu lub rozwiązaniu Umowy.
3. Wykonawca zobowiąże pracowników zatrudnionych przy przetwarzaniu danych osobowych do zachowania w poufności, w ramach tajemnicy służbowej, wszelkich informacji lub danych osobowych, do których mogą mieć dostęp w związku z dokonywaniem czynności przy przetwarzaniu danych osobowych, jak również do nieujawniania stosowanych środków ochrony i zabezpieczeń.
4. Wykonawca wyciągnie stosowne konsekwencje wobec pracowników, którzy w jakikolwiek sposób naruszą tajemnicę służbową, o której mowa w ust. 3 lub zasady przetwarzania danych osobowych określone w Umowie, w szczególności pozbawi tych pracowników możliwości dalszego przetwarzania danych osobowych zawartych w zbiorach danych Zamawiającego, w tym zbierania danych (jeżeli ma to zastosowanie).

§ 7

Wykonawca zwolni Zamawiającego z odpowiedzialności wobec osób, których dane osobowe są przetwarzane w związku z Umową z tytułu jakiejkolwiek szkody poniesionej przez te osoby, wynikającej lub związanej z naruszeniem przez Wykonawcę jakichkolwiek przepisów dotyczących ochrony danych osobowych lub postanowień Umowy.

§ 8

Wykonawca oświadcza, że Pełnomocnikiem Zarządu ds. Ochrony Danych osobowych Wykonawcy na dzień podpisania Umowy jest: ....., tel.: ....., e-mail: .....

lub

Wykonawca oświadcza, że, jako administrator danych, osobiście wykonuje czynności związane z ochroną danych osobowych i pełni nadzór nad przetwarzaniem danych osobowych Zamawiającego.

§ 9

1. Wykonawca w celu uzyskania zgody na powierzenie stronie trzeciej (dalej „Podwykonawcy") przetwarzania danych osobowych wynikających z wykonania zadań określonych Usługą zobowiązany jest wystąpić do Zamawiającego o pisemne wyrażenie zgody na powierzenie przetwarzania danych osobowych Podwykonawcy podając jednocześnie zakres i cel powierzonych danych osobowych oraz firmę Podwykonawcy, załączając do wniosku projekt umowy z Podwykonawcą.
2. Zamawiający może nie wyrazić zgody na powierzenie Podwykonawcy przetwarzania danych osobowych w przypadku, gdy w ocenie Zamawiającego powierzenie nie będzie niezbędne dla realizacji celów związanych z procesami i projektami wynikającymi z Umowy i Usługi.
3. W przypadku, gdy Wykonawca na podstawie pisemnej zgody Zamawiającego powierzy przetwarzanie danych osobowych Podwykonawcy zobowiązany jest do wypełnienia następujących warunków:
   1) powiadomienia Zamawiającego, w formie pisemnej, drogą określoną przez Zamawiającego w treści zgody o planowanym terminie zawarcia umowy z Podwykonawcą,
   2) zawarcia umowy z Podwykonawcą na piśmie, zgodnie z obowiązującymi przepisami dotyczącymi powierzania przetwarzania danych osobowych,
   3) przekazania Zamawiającemu poświadczoną za zgodność z oryginałem kopię umowy z Podwykonawcą zawierającą w szczególności następujące warunki:
      a) wskazanie zakresu i celu umowy z Podwykonawcą, z zastrzeżeniem, że zakres i cel przetwarzania nie może być szarszy niż wynikający z Umowy i Usługi, nawet, gdy jest to niezbędne dla realizacji celów związanych z procesami i projektami wynikającymi z Umowy,
      b) zobowiązanie Podwykonawcy do nienaruszania interesów Zamawiającego.
4. Wykonawca zobowiązany jest do nałożenia na Podwykonawcę w drodze umowy tych samych obowiązków jak w Umowie zawartej pomiędzy Zamawiającym a Wykonawcą, w szczególności dotyczy to obowiązku zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO oraz obowiązującym przepisom o ochronie danych osobowych.
5. Jeżeli Podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Zamawiającego za niewypełnienie obowiązków Podwykonawcy spoczywa na Wykonawcy.

§ 10

1. Umowa zostaje zawarta na czas obowiązywania Umowy nr ...../CIS-WAZ.2720.....2021 i wygasa automatycznie z chwilą wygaśnięcia Umowy.
2. Zamawiający może wypowiedzieć Umowę bez zachowania terminu wypowiedzenia w przypadku, gdy, rażąco narusza postanowienia Umowy oraz przepisy powszechnie obowiązujące w zakresie ochrony danych osobowych stwierdzone w szczególności na podstawie protokołów z inspekcji i audytów Zamawiającego lub podmiotów trzecich albo nie podda się kontroli, o której mowa w § 4 lub utrudnia jej przeprowadzenie bez uzasadnionych przyczyn.
3. Po zakończeniu obowiązywania Umowy lub odstąpienia od Umowy Wykonawca zobowiązuje się niezwłocznie, nie później niż w terminie 7 dni przekazać Zamawiającemu kopię przetwarzanych danych osobowych i usunąć bezpowrotnie powierzone dane osobowe oraz inne informacje, których przetwarzanie na podstawie Umowy zlecił mu Zamawiający chyba, że prawo Rzeczpospolitej Polskiej i Unii Europejskiej nakazuje przechowywanie danych osobowych przez określony czas.
4. W przypadku niewykonania zobowiązania, o którym mowa w ust. 3, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20.000 złotych (słownie: dwadzieścia tysięcy złotych) za każdy przypadek naruszenia. Nie wyklucza to dochodzenia przez Zamawiającego od Wykonawcy odszkodowania na zasadach ogólnych.

§ 11

1. Strony deklarują współpracę w zakresie zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa o ochronie danych osobowych, w szczególności z RODO.
2. W miarę możliwości organizacyjnych i technicznych Wykonawca zobowiązany jest do udzielenia pomocy Zamawiającemu w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 13-19 RODO, zobowiązując Podwykonawcę do tych samych działań.
3. Strony ustalają, że w zakresie wynikającym z nowych i zmian przepisów w zakresie ochrony danych osobowych, w tym sektorowych lub wytycznych Urzędu Ochrony Danych Osobowych będą dokonywać renegocjacji warunków Umowy lub podpiszą nową umowę zapewniającą kontynuację współpracy.

§ 12

1. Strony postanawiają, że we wszelkich sprawach nieobjętych Umową stosuje się przepisy prawa polskiego.
2. Wszelkie spory związane z zawarciem i wykonaniem Umowy będą rozstrzygane przez sąd powszechny właściwy ze względu na siedzibę powoda.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Umowa sporządzona została w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron.

.....	.....
Zamawiający	Wykonawca
(podpis)	*(podpis)*