0110-KLL2.261.47.2026.1 **Załącznik nr 3 do Zaproszenia**

UMOWA NR 0110-KLL2.262….2026 (ZMIENIONY PROJEKT UMOWY)

zawarta pomiędzy:
Skarbem Państwa – Krajową Informacją Skarbową, z siedzibą w Bielsku-Białej przy ul. Warszawskiej 5, 43-300 Bielsko-Biała,
NIP: 5472169306, REGON: 366063511

reprezentowaną przez:
……. – ……..
zwaną dalej **Zamawiającym**
a
nazwa Wykonawcy ……
adres siedziby ……
NIP: …… REGON: ……
reprezentowaną przez:
……..-……
……..-…….
zwaną dalej **Wykonawcą,**
zwanymi dalej **Stronami.**

W wyniku przeprowadzonego rozpoznania rynku nr 0110-KLL2.261.47.2026.1 na świadczenie usługi odnowienia i dostawy nowych certyfikatów kwalifikowanych podpisów elektronicznych dla pracowników Krajowej Informacji Skarbowej na 2027 rok, została zawarta umowa następującej treści:

§ 1
PRZEDMIOT UMOWY

1. Przedmiotem umowy jest świadczenie usługi odnowienia i dostawy nowych certyfikatów kwalifikowanych podpisów elektronicznych dla pracowników Krajowej Informacji Skarbowej na 2027 rok poprzez świadczenie usług zaufania polegających na:
   1) odnowieniu, wytwarzaniu, wydawaniu, zawieszaniu i unieważnianiu certyfikatów,
   2) dostawie elementów urządzeń do składania i weryfikacji kwalifikowanego podpisu elektronicznego wraz z niezbędnym oprogramowaniem, zgodnie z zapisami Zaproszenia do składania ofert oraz ofertą Wykonawcy stanowiącą załącznik nr 1 do umowy.
2. Zamawiający może w ramach umowy zamawiać anonimizowane certyfikaty kwalifikowanego podpisu elektronicznego tzn. nieujawniające numeru PESEL subskrybenta w podpisie kwalifikowanym bez zmiany ceny za wykonaną usługę
3. Przedmiot umowy będzie realizowany sukcesywnie – zgodnie z zapotrzebowaniem Zamawiającego.
4. Zamawiający każdorazowo przy składaniu wniosku o wydanie certyfikatu może wskazać, czy dany certyfikat ma zawierać numer PESEL w sposób jawny czy ukryty.

W takim przypadku Wykonawca musi zapewnić, że certyfikaty z ukrytym numerem PESEL będą spełniać wszystkie wymogi wynikające z rozporządzenia eIDAS i będą zgodne z polityką certyfikacji Wykonawcy.

5. Zamawiający zastrzega możliwość skorzystania z prawa opcji polegającego na przedłużeniu okresu realizacji umowy o 12 miesięcy.
6. Skorzystanie z opcji następuje na podstawie oświadczenia woli Zamawiającego o skorzystaniu z prawa opcji złożonego Wykonawcy w terminie nie krótszym niż 10 dni przed upływem okresu zamówienia podstawowego wskazanego w § 2 ust. 1 pkt. 1).
7. Przedłużenie umowy w ramach opcji nie wymaga zawarcia nowej umowy.
8. Prawo opcji jest jednostronnym uprawnieniem Zamawiającego, z którego może skorzystać, ale nie ma obowiązku skorzystać w ramach realizacji przedmiotu zamówienia. W przypadku, gdy Zamawiający nie skorzysta z prawa opcji Wykonawcy nie przysługują żadne roszczenia z tego tytułu.

§ 2

TERMIN I MIEJSCE REALIZACJI UMOWY

1. Umowa obowiązuje w terminie od:
   1) 4 stycznia 2027 r**.** do 31 grudnia 2027 r. dla zamówienia podstawowego,
   2) dla zamówienia w ramach opcji przedłużenie umowy o kolejne 12 miesięcy tj. od dnia następującego po zakończeniu zamówienia podstawowego, pod warunkiem przekazania Wykonawcy oświadczenia o skorzystaniu z prawa opcji.
2. Procedura poświadczania tożsamości subskrybentów oraz dostawa nowych certyfikatów i odnowienia związane z wymianą karty, będą przeprowadzane **stacjonarnie i bezpośrednio przez pracownika Wykonawcy** w ustalonych przez Strony terminach w następujących lokalizacjach:
   1) Krajowa Informacja Skarbowa w Bielsku-Białej ul. Warszawska 5, 43-300 Bielsko-Biała,
   2) Krajowa Informacja Skarbowa w Bielsku-Białej ul. Teodora Sixta 17, 43-300 Bielsko-Biała,
   3) Delegatura Krajowej Informacji Skarbowej w Bielsku-Białej ul. Romualda Traugutta 2, 43-300 Bielsko-Biała.
   4) Delegatura Krajowej Informacji Skarbowej w Lesznie ul. Jana Dekana 6, 64-100 Leszno,
   5) Delegatura Krajowej Informacji Skarbowej w Lesznie ul. Jana Dekana 3b, 64-100 Leszno,
   6) Delegatura Krajowej Informacji Skarbowej w Płocku ul. 1 Maja 10, 09-402 Płock.
   7) Delegatura Krajowej Informacji Skarbowej w Piotrkowie Trybunalskim ul. Wronia 65, 97-300 Piotrków Trybunalski,
   8) Delegatura Krajowej Informacji Skarbowej w Toruniu ul. Św. Jakuba 20, 87-100 Toruń,
   9) Delegatura Krajowej Informacji Skarbowej w Toruniu ul. Szosa Chełmińska 34-36, 87-100 Toruń,
   10) Wydział Krajowej Informacji Skarbowej w Będzinie ul. Józefa Retingera 1, 42-500 Będzin.

§ 3

CENA I WARUNKI PŁATNOŚCI

1. Cena z tytułu realizacji umowy za wykonaną usługę każdorazowo ustalana będzie na podstawie wartości złożonych formularzy zgłoszeń certyfikacyjnych, zgodnie ze szczegółową wyceną poszczególnych elementów wchodzących w skład zamówienia i stanowić będzie iloczyn wykonanych usług i cen jednostkowych brutto.
2. Wszelkie czynności nieopisane w dokumentacji oraz niniejszej umowie, a niezbędne do właściwego i kompletnego wykonania przedmiotu umowy traktowane są jako oczywiste i zostały uwzględnione w cenie podanej przez Wykonawcę w Formularzu oferty.
3. Podstawą do wyliczenia ceny będą ceny usług certyfikacyjnych wskazane w formularzu cenowym stanowiącym załącznik nr 2 do umowy tj.:
   1) dla zamówienia podstawowego:
   a) …… zł brutto (słownie:…… złotych) za odnowienie 1 sztuki certyfikatu kwalifikowanego podpisu elektronicznego na okres 2 lat,
   b) …… zł brutto (słownie:…… złotych) za wystawienie 1 sztuki nowego certyfikatu kwalifikowanego podpisu elektronicznego na okres 2 lat (podpis, karta kryptograficzna, czytnik).
   2) dla zamówienia w ramach opcji:
   a) …… zł brutto (słownie:…… złotych) za odnowienie 1 sztuki certyfikatu kwalifikowanego podpisu elektronicznego na okres 2 lat,
   b) …… zł brutto (słownie:…… złotych) za wystawienie 1 sztuki nowego certyfikatu kwalifikowanego podpisu elektronicznego na okres 2 lat (podpis, karta kryptograficzna, czytnik).
4. Cena płatna będzie etapowo, po każdym miesiącu, w którym Wykonawca zrealizował usługi, na podstawie faktury wystawionej przez Wykonawcę.
5. Cena za wykonanie przedmiotu umowy płatna będzie na podstawie prawidłowo wystawionej przez Wykonawcę faktury VAT. Płatność nastąpi przelewem na rachunek bankowy Wykonawcy wskazany na fakturze, w ciągu **21 dni** kalendarzowych od dnia dostarczenia faktury. Za prawidłowo wystawioną fakturę VAT Zamawiający uważa fakturę niebędącą przedmiotem korekty. W przypadku konieczności wystawienia faktury korygującej z przyczyn leżących po stronie Wykonawcy termin płatności dla kwoty objętej korektą liczony jest od dnia otrzymania przez Zamawiającego faktury korygującej.
6. Dane do faktury: **Krajowa Informacja Skarbowa ul. Warszawska 5, 43-300 Bielsko-Biała, NIP: 547 21 69 306 i REGON: 366063511**.
   Z dniem obowiązywania przepisów ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U z 2026 r. poz. 1263), w zakresie obowiązku korzystania z Krajowego Systemu e-Faktur (KSeF) Wykonawca zobowiązany jest wystawiać i przesyłać Zamawiającemu, ustrukturyzowane faktury, poprzez Krajowy System e-Faktur (KSeF). Za datę dostarczenia faktury, od której liczony będzie termin płatności, uważa się dzień przydzielenia w tym systemie numeru identyfikującego tę fakturę.
7. W przypadku, kiedy Wykonawca nie jest podmiotem zobowiązanym na mocy powszechnie obowiązujących przepisów prawa do wystawiania i przesyłania faktur

poprzez KSeF, i nie wystawia oraz nie przesyła faktur poprzez KSeF, Zamawiający dopuszcza możliwość przesyłania (format PDF) przez Wykonawcę faktur drogą elektroniczną, które należy przesłać na adres: e-mail: kancelaria.kis@mf.gov.pl.

8. Za datę dokonania płatności Strony uznają datę obciążenia rachunku bankowego Zamawiającego.
9. Wykonawca nie może bez pisemnej zgody Zamawiającego przenieść wierzytelności wynikających z tytułu niniejszej umowy na osobę trzecią ani dokonywać kompensaty.
10. W przypadku opóźnienia w zapłacie należnej ceny w terminie określonym w ust. 5 Wykonawcy przysługuje prawo naliczenia odsetek ustawowych za opóźnienie w płatności w wysokości określonej w ustawie z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych.
11. Zamawiający na podstawie art. 4 ust. 3 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (t.j. Dz. U. z 2026 r. poz. 276 ze zm.) wyłącza stosowanie ustrukturyzowanych faktur elektronicznych.

§ 4

WARUNKI GWARANCJI I RĘKOJMI

1. Wykonawca udziela gwarancji i rękojmi na elementy wchodzące w skład przedmiotu umowy (certyfikaty kwalifikowane, karty kryptograficzne, czytniki, oprogramowanie) na okres ważności certyfikatu.
2. Reklamacje będą rozpatrywane w terminie do 5 dni roboczych od daty zgłoszenia wad, awarii i usterek, chyba że Strony zgodnie ustalą inny termin.
3. Zamawiający nie ponosi odpowiedzialności za uszkodzenia wynikłe nie z jego winy.
4. Wykonawca oświadcza, iż dostarczone wraz z certyfikatami oprogramowanie, karty kryptograficzne oraz czytniki są wolne od wad.
5. Wykonawca zobowiązany jest informować i udostępniać Zamawiającemu wszelkie powstałe aktualizacje dostarczonego wraz z certyfikatami oprogramowania, bez odrębnych opłat licencyjnych i w ramach usług serwisu gwarancyjnego.
6. Zapisy niniejszego paragrafu umowy obowiązują do upływu terminu ważności ostatniego certyfikatu wydanego lub odnowionego na podstawie niniejszej umowy.
7. Wykonawca zapewni możliwość zgłaszania wad, awarii i usterek przedmiotu umowy od poniedziałku do piątku w godzinach od 8:00 – 15:00 na adres poczty elektronicznej: adres email …….

§ 5

ZOBOWIĄZANIA ZAMAWIAJĄCEGO

1. Zamawiający zobowiązuje się do wykonywania obowiązków umownych z należytą starannością z uwzględnieniem postanowień zawartych w umowie i obowiązujących przepisach prawa.
2. Zamawiający zobowiązuje się do dostarczenia do Wykonawcy – w miarę pojawiających się potrzeb (na formularzu zgłoszenia certyfikacyjnego obejmującego wyłącznie imię

i nazwisko i numer PESEL pracownika) – zapotrzebowania dotyczącego pracowników, dla których mają być odnowione/wystawione certyfikaty.

3. Zamawiający zobowiązuje się do przekazania Wykonawcy wykazu pracowników upoważnionych do występowania z wnioskiem o unieważnienie/zawieszenie certyfikatu kwalifikowanego wraz z załączonymi (potwierdzonymi za zgodność z oryginałem) upoważnieniami udzielonymi tym pracownikom.
4. Zamawiający zobowiąże subskrybentów wskazanych w formularzu zgłoszenia certyfikacyjnego do zawarcia z Wykonawcą indywidualnych umów na świadczenie usług zaufania polegających na wystawieniu kwalifikowanego certyfikatu.
5. W przypadku każdorazowej zmiany danych zapisanych w certyfikacie dotyczących Zamawiającego lub subskrybenta, Zamawiający jest zobowiązany do niezwłocznego zgłoszenia tego faktu Wykonawcy w celu unieważnienia certyfikatu.
6. Po każdorazowym otrzymaniu certyfikatu przez subskrybenta przypisanego do umowy z Zamawiającym, Zamawiający jest zobowiązany do niezwłocznego sprawdzenia przez subskrybentów poprawności umieszczonych w nim danych przed jego użyciem (w szczególności przed wykonaniem pierwszego podpisu elektronicznego weryfikowanego przed użyciem tego certyfikatu).
7. W przypadku, gdy dane subskrybenta zawarte w certyfikacie (kraj, imię/imiona, nazwisko/nazwiska, PESEL lub NIP) nie będą zgodne z danymi zawartymi w sporządzonym przez Zamawiającego wniosku o wystawienie/odnowienie certyfikatu z danymi Subskrybenta i firmy, Wykonawca bezpłatnie wygeneruje i wyda nowy certyfikat, zawierający prawidłowe dane.
8. Strony ustanawiają do wzajemnych kontaktów na etapie realizacji umowy następujące osoby:
   a) Zamawiający ustanawia do kontaktów z Wykonawcą:
      ..... tel.: .....
   b) Wykonawca ustanawia do kontaktów z Zamawiającym
      ..... tel.: .....
9. Wykaz osób przeprowadzających procedurę poświadczenia tożsamości subskrybentów stanowi załącznik nr 6 do Projektu umowy.
10. O każdorazowej zmianie osób wyznaczonych do kontaktów lub zmianie danych teleadresowych tych osób, Strona niezwłocznie poinformuje drugą Stronę w formie dokumentowej, pisemnej lub elektronicznej, wskazując zakres zmian. Zmiana ta nie stanowi zmiany treści umowy.

§ 6

ZOBOWIĄZANIA WYKONAWCY

1. Wykonawca zobowiązuje się do wykonania usługi zaufania polegającej na odnowieniu i dostawie nowych certyfikatów kwalifikowanych podpisów elektronicznych z należytą starannością – w sposób profesjonalny i na zasadach określonych w przepisach prawa, o których mowa w ust. 4.
2. Strony wzajemnie zobowiązuję się wykonywać komunikacje w sposób bezpieczny poprzez obowiązek szyfrowania plików zawierających dane osobowe oraz przesłanie hasła do ich odszyfrowania innym kanałem komunikacji.

3. W ramach świadczenia usług, o których mowa w § 1 ust. 1, Wykonawca zobowiązuje się w szczególności do:
   1) nieodpłatnego poświadczenia tożsamości subskrybentów,
   2) wygenerowania certyfikatów kwalifikowanych o dwuletnim okresie ważności (na kartach kryptograficznych o standardowej wielkości lub w formie karty SIM) zgodnie z zamówieniami przekazanymi przez Zamawiającego, na podstawie danych określonych w formularzu zgłoszenia certyfikacyjnego,
   3) zapewnienia dla każdego z subskrybentów oprogramowania do składania i weryfikacji bezpiecznego podpisu elektronicznego, z zastrzeżeniem możliwości instalowania tego oprogramowania na dowolnej liczbie stacji roboczych Zamawiającego,
   4) nieodpłatnego udostępnienia oprogramowania do weryfikacji podpisu elektronicznego, w celu umieszczenia go na stronie Zamawiającego,
   5) wygenerowania anonimizowanych certyfikatów kwalifikowanych podpisów elektronicznych na wniosek Zamawiającego.
4. Przy realizacji niniejszej umowy znajdują zastosowanie: publikowana na stronie internetowej Wykonawcy Polityka certyfikacji dla certyfikatów kwalifikowanych oraz przepisy prawa, w tym regulujące świadczenie usług zaufania.
5. Procedura poświadczania tożsamości subskrybentów przy zakupie nowego podpisu będzie przeprowadzana wyłącznie stacjonarnie i bezpośrednio przez osobę Wykonawcy w ustalonych przez Strony terminach w lokalizacjach Zamawiającego wskazanych w § 2 ust. 2.
6. Wykonawca zobowiązuje się, po zawarciu umowy, do zawarcia z subskrybentami indywidualnych umów o świadczenie usług zaufania polegających na wystawieniu kwalifikowanego certyfikatu.
7. Wykonawca nie może przenieść praw i obowiązków wynikających z niniejszej umowy na osobę trzecią bez zgody Zamawiającego.
8. Wykonawca odpowiada za szkody zaistniałe na skutek nienależytego wywiązania się z niniejszej umowy, a poniesione przez osoby trzecie.
9. Wykonawca zobowiązany jest do zachowania w poufności wszelkich informacji prawnie chronionych uzyskanych w związku z realizacją niniejszej umowy.
10. Wykonawca zobowiązany jest do zapoznania swoich pracowników z INFORMACJĄ O ZAGROŻENIACH stanowiącą Załącznik nr 4 do umowy oraz sporządzenia WYKAZU OSÓB stanowiącego Załącznik nr 5 do umowy, które zostały poinformowane o zagrożeniach dla bezpieczeństwa i zdrowia.
11. Dokumenty określone w ust. 10, w szczególności WYKAZ OSÓB (Załącznik nr 5 do umowy), pozostają w siedzibie Wykonawcy, a ich okazanie następuje na żądanie Zamawiającego.

§ 7
PODSTAWOWE ZASADY ŚWIADCZENIA USŁUG

1. Zamawiający nie dopuszcza przekazywania Wykonawcy innych danych osobowych subskrybentów niż: imię i nazwisko oraz numer PESEL.
2. Procedura poświadczania tożsamości subskrybentów będzie przeprowadzana w sposób ściśle określony w § 6 ust. 5.

§ 8

KARY UMOWNE

1. Zamawiający zastrzega sobie prawo naliczania kar umownych od Wykonawcy za niewykonanie lub nienależyte wykonanie przedmiotu umowy, a także opóźnienie w realizacji przedmiotu umowy.
2. W przypadku niewykonania lub nienależytego wykonania umowy Zamawiającemu przysługuje prawo żądania od Wykonawcy zapłaty następujących kar umownych:
   1) w wysokości 5.000,00 zł (słownie: pięć tysięcy złotych zero groszy) za odstąpienie od umowy z przyczyn zależnych od Wykonawcy, albo z powodu niewykonania, nienależytego wykonania umowy,
   2) w wysokości 300,00 zł (słownie: trzysta złotych zero groszy) za każdy rozpoczęty dzień kalendarzowy opóźnienia w usunięciu wad, usterek i awarii objętych gwarancją i rękojmią w stosunku do terminu określonego w § 4 ust. 2, nie więcej niż 3.000,00 zł (słownie: trzy tysiące złotych zero groszy).
3. Zapłata przez Wykonawcę kary umownej nie zwalnia Wykonawcy z realizowania obowiązków określonych niniejszą umową z wyjątkiem zapłaty kary o której mowa w ust. 2 pkt 1) umowy.
4. Termin zapłaty kary umownej wynosi 7 dni kalendarzowych od dnia doręczenia zawiadomienia o obciążeniu karą umowną.
3. W przypadku opóźnienia w zapłacie kary umownej, Zamawiającemu przysługuje prawo naliczenia odsetek ustawowych za opóźnienie w transakcjach handlowych, o których mowa w art. 7 ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (Dz.U. z 2023 r. poz. 1790 ze zm.).
5. Jeżeli Wykonawca nie zapłaci kary umownej w terminie, kara ta może zostać potrącona z wynagrodzenia należnego Wykonawcy.
6. Wykonawca wyraża zgodę na potrącanie przez Zamawiającego kar umownych z wynagrodzenia należnego Wykonawcy.
7. Gdy szkoda będzie wyższa niż kara umowna, Zamawiający będzie uprawniony do dochodzenia odszkodowania przenoszącego wysokość kary umownej.
8. Kary umowne zastrzeżone na rzecz Zamawiającego mogą być dochodzone z każdego tytułu odrębnie i podlegają łączeniu.
9. W przypadku braku możliwości lub prawnej dopuszczalności potrącenia kary z wynagrodzenia Wykonawcy, będą one dochodzone na zasadach ogólnych.

§ 9

ODSTĄPIENIE OD UMOWY, JEJ ROZWIĄZANIE

1. Zamawiający może odstąpić od całości lub części umowy w przypadkach określonych w umowie lub przepisach obowiązującego prawa, w szczególności ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2026 r. poz. 795).
2. Umowne prawo odstąpienia od umowy przysługuje Zamawiającemu w sytuacji:
   1) w razie utraty przez Wykonawcę uprawnień, niezbędnych do wykonywania usługi będącej przedmiotem niniejszej umowy,

2) w przypadku nieprzystąpienia do realizacji umowy z przyczyn leżących po stronie Wykonawcy.

3. Zamawiającemu przysługuje prawo natychmiastowego wypowiedzenia umowy:
   1) w przypadku dopuszczenia się przez Wykonawcę lub osoby działające w jego imieniu lub na jego zlecenie naruszenia przepisów dotyczących ochrony tajemnic prawnie chronionych,
   2) w przypadku dopuszczenia się przez Wykonawcę lub osoby działające w jego imieniu lub na jego zlecenie naruszenia przepisów dotyczących ochrony danych osobowych,
   3) po naliczeniu kar umownych za opóźnienie o których mowa w § 8 ust. 2 pkt 2) na kwotę co najmniej 1.800,00 zł (słownie: jeden tysiąc osiemset złotych zero groszy).
4. Odstąpienie od umowy oraz jej wypowiedzenie wymagają formy pisemnej lub elektronicznej, pod rygorem nieważności oraz pisemnego uzasadnienia, które stanowi jego integralną część oraz określenia czy następuje ono ze skutkiem *ex nunc* czy *ex tunc*.
5. W uzasadnionych przypadkach umowa może być rozwiązana w każdym czasie za porozumieniem Stron.
6. W przypadku odstąpienia przez Zamawiającego od umowy w części albo jej wypowiedzenia, Strony dokonują rozliczenia prawidłowo wykonanych usług do dnia odstąpienia od umowy/wypowiedzenia w oparciu o odpowiednie stosowanie określonych w umowie podstaw wystawiania faktur, terminów płatności.

§ 10

ZASADY ZACHOWANIA POUFNOŚCI

1. Wykonawca zobowiązuje się do zachowania w poufności wszelkich informacji technicznych, technologicznych, prawnych i organizacyjnych, oraz innych informacji Zamawiającego uzyskanych w trakcie wykonywania Umowy niezależnie od formy pozyskania tych informacji i ich źródła.
2. Wykonawca zobowiązuje się do wykorzystania informacji jedynie w celach określonych postanowieniami Umowy oraz wynikającymi z obowiązujących uregulowań prawnych.
3. Wykonawca zobowiązuje się do ujawnienia informacji dotyczących Przedmiotu Umowy, w tym informacji technicznych, technologicznych, prawnych i organizacyjnych jedynie tym osobom, którym będą one niezbędne do wykonywania powierzonych im czynności i tylko w zakresie, w jakim odbiorca informacji musi mieć do nich dostęp dla celów realizacji zadania wynikającego z tytułu realizacji Umowy.
4. Wykonawca zobowiązuje się do nierozpowszechniania jakiejkolwiek części informacji związanych z realizacją Umowy, z wyjątkiem uzasadnionych przypadków takiej potrzeby, po uprzednim uzyskaniu pisemnej zgody od Zamawiającego.
5. Strony zobowiązują się do przestrzegania przy wykonywaniu Umowy wszystkich postanowień zawartych w obowiązujących przepisach prawnych związanych z ochroną tajemnic prawnie chronionych.
6. Obowiązek określony w ust. 1 nie dotyczy informacji powszechnie znanych oraz udostępniania informacji na podstawie bezwzględnie obowiązujących przepisów prawa, w szczególności na żądanie sądów, prokuratury, organów podatkowych lub organów

kontrolnych, a także informacji dostępnych publicznie, o których mowa w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej.

7. Nie będą uważane za chronione informacje, które:
   1) wcześniej stały się informacją publiczną w okolicznościach niebędących wynikiem czynu bezprawnego lub naruszającego Umowę przez którąkolwiek ze Stron;
   2) zostały przekazane Stronie otrzymującej przez osobę trzecią niebędącą Stroną Umowy zgodnie z prawem i bez ograniczeń;
   3) były zatwierdzone do rozpowszechniania na podstawie uprzedniej pisemnej zgody Strony, której dotyczą.
8. Wykonawca ponosi odpowiedzialność za zachowanie w poufności informacji przez swoich pracowników, podwykonawców i wszelkich innych osób, którymi będzie się posługiwać przy wykonywaniu Umowy.
9. Wykonawca podejmie wszelkie niezbędne kroki, w tym prawne i organizacyjne dla zapewnienia, że żaden pracownik Wykonawcy lub inna osoba, o której mowa w ust. 8, otrzymujący powyższe informacje, nie ujawni tych informacji, ani ich źródła, zarówno w całości, jak i w części podmiotom trzecim bez uzyskania uprzednio wyraźnej pisemnej zgody Zamawiającego.
10. Obowiązek zachowania w poufności informacji przez Wykonawcę i osoby, o których mowa w ust. 8, obowiązuje także po ustaniu Umowy.
11. Wykonawca odpowiada za szkodę wyrządzoną Zamawiającemu powstałą wskutek ujawnienia, przekazania, wykorzystania, zbycia lub oferowania do zbycia informacji otrzymanych od Zamawiającego, wbrew postanowieniom Umowy. Zobowiązanie to obowiązuje Wykonawcę również po wykonaniu Umowy, jej rozwiązaniu, wygaśnięciu lub odstąpieniu, bez względu na przyczynę.
12. Wykonawca oświadcza, że każda z osób uczestniczących w realizacji Przedmiotu Umowy zobowiązała się wobec niego, jako Wykonawcy, nie ujawniać żadnych informacji, z którymi zapozna się podczas wykonywania czynności zleconych do realizacji.
13. Wykonawca i osoby, o których mowa w ust. 8, zobowiązani są do zapoznania się z treścią Zasad bezpieczeństwa informacji Resortu Finansów we współpracy z podmiotami zewnętrznymi.
14. Wykonawca i osoby, o których mowa w ust. 8, zobowiązani są do złożenia oświadczenia potwierdzającego zapoznanie się z treścią Zasad, o których mowa w ust. 13, przed rozpoczęciem świadczenia Usługi. Oświadczenie może być złożone w formie elektronicznej. Wzór oświadczenia o zapoznaniu się Zasadami bezpieczeństwa informacji Resortu Finansów we współpracy z podmiotami zewnętrznymi określa Załącznik nr 3 do umowy.

§ 11

OCHRONA DANYCH OSOBOWYCH

1. W celu zawarcia i wykonania umowy, Strony wzajemnie udostępniają sobie dane osobowe (dane służbowe) reprezentantów Stron oraz osób zaangażowanych w jej realizację, w zakresie niezbędnym dla potrzeb umożliwienia utrzymywania bieżącego

kontaktu przy jej zawarciu i wykonywaniu, co stanowi prawnie uzasadniony interes Stron umowy.

2. Żadna ze Stron nie będzie wykorzystywać wzajemnie udostępnionych sobie danych osobowych w celu innym niż zawarcie i realizacja umowy
3. Wskutek udostępnienia danych osobowych osób wskazanych w ust. 1, Strony stają się odrębnymi administratorami udostępnionych im danych i zobowiązują się wzajemnie przekazać tym osobom Informację o przetwarzaniu ich danych osobowych.
   W wykonaniu tego zobowiązania każda ze Stron załączy klauzulę informacyjną RODO.

§ 12

POSTANOWIENIA KOŃCOWE

1. Wszelkie zmiany i uzupełnienia niniejszej umowy wymagają formy pisemnej lub elektronicznej pod rygorem nieważności z zastrzeżeniem ust. 2.
2. O każdorazowej zmianie osób wyznaczonych do kontaktów lub zmianie danych teleadresowych tych osób, Strona niezwłocznie poinformuje drugą Stronę w formie dokumentowej, pisemnej lub elektronicznej, wskazując zakres zmian. Zmiana ta nie stanowi zmiany treści umowy.
3. W kwestiach nieuregulowanych niniejszą umową rozstrzyga się na podstawie przepisów Kodeksu cywilnego.
4. Adresy podane na wstępie umowy są wiążące dla Stron. Doręczenia pod te adresy będzie się uważać za skuteczne o ile wysłanie korespondencji nastąpiło przed poinformowaniem drugiej Strony o zmianie adresu. Strony będą się wzajemnie informowały o ewentualnych zmianach swoich danych teleadresowych.
5. Podany w Formularzu ofertowym - Załącznik nr 1 do umowy - adres poczty elektronicznej posłuży do przekazywania informacji związanych z realizacją umowy. Dotyczy to również przekazywania informacji w zakresie naliczania kar umownych oraz składanych w formie elektronicznej oświadczeń o rozwiązaniu umowy. Dokumenty przesłane na podany adres poczty elektronicznej uważa się za doręczone Wykonawcy z dniem ich wysłania. Na żądanie Zamawiającego, Wykonawca zobowiązany jest do niezwłocznego potwierdzenia ich otrzymania. Brak potwierdzenia lub odmowa potwierdzenia, nie uchybia uznaniu oświadczenia/dokumentu za doręczony w myśl zdania trzeciego.
6. Strony postanawiają, że:
   1) we wszystkich sprawach spornych wynikających lub mogących wyniknąć z zawartej umowy wyłączna jurysdykcja przysługuje sądom polskim,
   2) wszelkie spory związane z realizacją postanowień umowy rozstrzygane będą przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
7. Zmiany osób wskazanych w § 5 ust. 8 umowy oraz ich danych teleadresowych, nie stanowią zmiany umowy i wymagają dla skuteczności poinformowania drugiej Strony co najmniej drogą mailową bądź faxem.
8. Załączniki do umowy stanowią jej integralną część.
9. Umowę uważa się za zawartą w chwilą złożenia podpisu przez ostatnią ze Stron.
10. Strony zgodnie postanawiają, że miejscem zawarcia umowy jest miejsce siedziby Zamawiającego.

11. W przypadku zawarcia umowy w formie pisemnej, sporządza się ją w trzech jednobrzmiących egzemplarzach. W przypadku zawarcia umowy w formie elektronicznej, sporządza się ją w jednym egzemplarzu.
12. Wykonawca przyjmuje do wiadomości, że Zamawiający zobowiązany jest do realizacji obowiązków wynikających z art. 34a -34d ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U z 2025 r. poz. 1483 ze zm.) oraz przepisów wykonawczych dotyczących prowadzenia Centralnego Rejestru Umów Jednostek Sektora Finansów.

.....	.....
Zamawiający	**Wykonawca**
(data, podpis)	(data, podpis)

Załączniki do umowy:

1. Załącznik nr 1 – Kopia formularza ofertowego złożonego przez Wykonawcę,
2. Załącznik nr 2 – Kopia formularza cenowego,
3. Załącznik nr 3 – Oświadczenie podmiotu zewnętrznego o zapoznaniu się z zasadami Bezpieczeństwa Informacji Resortu Finansów,
4. Załącznik nr 4 – Informacja o zagrożeniach,
5. Załącznik nr 5 – Wykaz osób,
6. Załącznik nr 6 – Wykaz osób przeprowadzających procedurę poświadczenia tożsamości subskrybentów
7. Załącznik nr 7 – Informacja dotycząca przetwarzania danych osobowych stron/reprezentantów stron (podmiotów publicznych/prywatnych) oraz osób wskazanych do kontaktu/współpracujących w ramach realizacji umowy.

KOPIA FORMULARZA OFERTOWEGO ZŁOŻONEGO PRZEZ WYKONAWCĘ

KOPIA FORMULARZA CENOWEGO

OŚWIADCZENIE PODMIOTU ZEWNĘTRZNEGO

[1].....
(miejscowość i data)[1]

.....
(Nazwisko i Imię)

.....
(Nazwa podmiotu zewnętrznego realizującego usługi na rzecz Resortu Finansów)

.....
(Stanowisko/funkcja)

OŚWIADCZENIE
o zapoznaniu się z zasadami bezpieczeństwa informacji w Resorcie Finansów we współpracy z podmiotami zewnętrznymi

W związku z realizacją zobowiązań z tytułu Umowy/Porozumienia[2] Nr 0110-KLL2.262……..2026 z dnia …….. oświadczam, że zapoznałam/em się z *Zasadami bezpieczeństwa informacji w Resorcie Finansów we współpracy z podmiotami zewnętrznymi,* stanowiącymi załącznik do niniejszego oświadczenia.

.....
(czytelny podpis)[3]

[1] wypełnić tylko w wersji papierowej
[2] niewłaściwe skreślić

Załącznik do oświadczenia

Zasady bezpieczeństwa informacji w Resorcie Finansów

we współpracy z podmiotami zewnętrznymi

1. W Resorcie Finansów w ramach współpracy z podmiotami zewnętrznymi stosuje się następujące zasady dotyczące bezpieczeństwa informacji:
   1) zasada wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań (różne zadania oznaczają różną wiedzę konieczną do ich wykonania, a tym samym inny profil dostępu);
   2) zasada potrzeby koniecznej - pracownicy mają zapewniony dostęp tylko do środków przetwarzania informacji (urządzeń teleinformatycznych, systemów, aplikacji, pomieszczeń), które są im konieczne do wykonania powierzonych im zadań;
   3) zasada uprawnionego dostępu – pracownicy są dopuszczeni do przetwarzania informacji prawnie chronionych i przeznaczonych wyłącznie do użytku wewnętrznego po uzyskaniu wiedzy z zasad postępowania, w tym ochrony, określonych grup informacji~~,~~ oraz do odbycia szkolenia z zasad ochrony informacji (w celu spełnienia kryteria dopuszczenia do przetwarzania określonych informacji i danych);
   4) zasada obecności koniecznej – prawo przebywania w obszarze przetwarzania, w tym przechowywania informacji i danych prawnie chronionych i wrażliwych, mogą mieć tylko osoby upoważnione. Przebywanie osób nieupoważnionych w tym obszarze jest możliwe wyłącznie w obecności upoważnionych pracowników;
   5) zasada świadomości zbiorowej - wszyscy pracownicy mają świadomość konieczności ochrony aktywów informacyjnych i aktywnie uczestniczą w tym procesie; świadomość pracowników w zakresie istniejących zagrożeń i zasad ochrony informacji jest podnoszona, w szczególności przez szkolenia i działania informacyjne;
   6) indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych na nich obowiązków i nadanych im uprawnień. Zasada ta dotyczy np. powierzonego sprzętu:
      - każdy pracownik odpowiada za powierzony mu do użytkowania sprzęt komputerowy, wydruków z systemu centralnego wydruku,
      - każdy pracownik odpowiada za sporządzony przez siebie wydruk;

7) rozdzielenia obowiązków - zadania krytyczne z punktu widzenia bezpieczeństwa systemu nie mogą być realizowane przez jedną osobę. Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić w celu ograniczenia okazji do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia aktywów organizacji, w szczególności należy rozdzielić realizację funkcji operacyjnych od nadzorczych i kontrolnych;
8) czystego biurka - podczas nieobecności pracownika na stanowisku pracy, także w przypadku krótkotrwałego opuszczenia pomieszczenia, dokumenty i informatyczne nośniki danych zawierające informacje prawnie chronione lub przeznaczone wyłącznie do użytku wewnętrznego należy zabezpieczyć przed dostępem osób postronnych i nieupoważnionych. Środki organizacyjno-techniczne dot. przechowywania dokumentów i informatycznych nośników danych dostosowywane są zidentyfikowanego ryzyka, z wykorzystaniem m.in. nieprzeszklonych, zamykanych na klucz mebli biurowych, szaf metalowych zamykanych na klucz lub kod, przeznaczonych do tego pomieszczeń zamykanych na klucz lub wyposażonych w system kontroli dostępu;
9) czystego ekranu - na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym – w szczególności dotyczy to serwera obsługującego systemy alarmowe, komputerów administratorów, serwerów do monitoringu. W czasie obecności pracownika monitor jest ustawiony tak, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;
10) czystego kosza – dokumenty papierowe, z wyjątkiem materiałów zawierających informacje publicznie dostępne, w tym promocyjno-informacyjne, muszą być niszczone w sposób uniemożliwiający ich odczytanie lub odtworzenie. W celu zniszczenia dokumentów papierowych zawierających informacje prawnie chronione i przeznaczone wyłącznie do użytku wewnętrznego należy korzystać z udostępnionych niszczarek o odpowiedniej klasie niszczenia, adekwatnej do informacji oraz danych utrwalonych na niszczonych dokumentach. Niszczenie informatycznych nośników danych należy przeprowadzić zgodnie z zasadami określonymi w umowie/porozumieniu;
11) czystej tablicy - po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice oraz flipchart (tablice do szkoleń);
12) czystych drukarek – w przypadku drukowania dokumentów z użyciem ogólnodostępnej drukarki drukowane informacje są zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik ma obowiązek skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru;

13) poufności informacji uwierzytelniających – każdy pracownik jest obowiązany do zachowania poufności udostępnionych mu haseł, kodów dostępu, kodów PIN, w szczególności do systemów informacyjnych;
14) prywatności kont w systemach – każdy użytkownik jest obowiązany do pracy w systemach informacyjnych wyłącznie na przypisanych lub udostępnionych mu kontach, które jednoznacznie go identyfikują. Zabronione jest udostępnianie własnych kont osobom trzecim. Zasada ta ma również zastosowanie do kart wykorzystywanych w systemach kontroli dostępu funkcjonujących w Resorcie Finansów. Stosowanie się do tej reguły pozwala zachować rozliczalność działań użytkowników;
15) dyskrecji – wszelkie informacje służbowe mogą być przekazywane innym osobom uprawnionym do pozyskania tych informacji zgodnie z obowiązującymi przepisami prawa i przyjętymi w Resorcie Finansów zasadami;
16) zamkniętego pomieszczenia – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu. Na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest obowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;
17) zgłaszania incydentów bezpieczeństwa informacji i naruszeń ochrony danych osobowych – każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu lub naruszenia mającego lub mogącego mieć wpływ na bezpieczeństwo informacji, w tym danych osobowych w Resorcie Finansów;
18) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę, w tym umowy, porozumienia, zawierają stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu aktywów informacyjnych po zakończeniu współpracy;
19) automatyzacji backupu - procesy tworzenia kopii zapasowych są odpowiednio zaplanowane z uwzględnieniem wymogów prawnych i potrzeb Resortu Finansów, jak również są zautomatyzowane oraz niemożliwe do przerwania przez pracownika;
20) legalnego oprogramowania – na serwerach i stacjach roboczych jest zainstalowane wyłącznie legalne oprogramowanie;
21) ochrony zewnętrznych (wymiennych) nośników danych – dane i informacje utrwalone na zewnętrznych nośnikach danych i wynoszone poza pomieszczenia użytkowane przez Resort Finansów są odpowiednio zabezpieczone przed nieuprawnionym dostępem, zniszczeniem oraz utratą integralności w czasie transportu i przechowywania. W szczególności dotyczy to informacji prawnie chronionych np. tajemnicy skarbowej, tajemnicy celnej, danych osobowych.

22) zasada bezpieczeństwa informacji w usługach chmurowych - wszystkie dane przetwarzane w usługach chmurowych muszą być lokalizowane w regionach Europejskiego Obszaru Gospodarczego (EOG), z preferencją regionów zlokalizowanych w Polsce. Odstępstwa od tej zasady wymagają uprzedniej zgody DBE MF, opartej na analizie ryzyka wraz z zastosowaniem mechanizmów transferowych i technicznych środków ochrony (np. szyfrowanie, kontrola kluczy). W przypadku, gdy przetwarzanie obejmuje dane osobowe, odstępstwa od lokalizacji EOG wymagają również oceny zgodności transferu danych zgodnie z RODO oraz zastosowania adekwatnych mechanizmów transferowych i środków technicznych.

2. Stosowanie zabezpieczeń lub ich grup uwzględnia następujące zasady:
   1) minimalny stosowany poziom zabezpieczeń odpowiada wymogom obowiązujących przepisów prawa;
   2) zabezpieczenia są wdrażane we wszystkich obszarach określonych w deklaracji stosowania zabezpieczeń, zgodnie z wymogami normy ISO/IEC 27001 i zasadami określonymi w normie ISO/IEC 27002;
   3) używane mechanizmy zabezpieczeń są adekwatne (odpowiednie) do zagrożeń, podatności, wartości aktywów oraz wyników szacowania ryzyka w bezpieczeństwie informacji;
   4) w doborze zabezpieczeń należy uwzględnić zalecenia i rekomendacje sformułowane w wyniku przeprowadzonych audytów bezpieczeństwa i kontroli;
   5) zabezpieczenia fizyczne, techniczne, prawne i organizacyjne uzupełniają się wzajemnie (grupy zabezpieczeń), zapewniając wymagany poziom bezpieczeństwa informacji;
   6) należy unikać niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych Resortu Finansów;
   7) niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających systemy informacyjne funkcjonujące w Resorcie Finansów bez zastosowania alternatywnych mechanizmów; systemy są sprawne i przygotowane na wystąpienie zidentyfikowanych zagrożeń;
   8) domniemanej odmowy - przyjęcia jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach („to, co nie jest dozwolone, jest zabronione”);
   9) ciągłego doskonalenia – SZBI jest stale monitorowany, stosowane zabezpieczenia są dostosowywane do zmieniających się warunków wewnętrznych i zewnętrznych, w celu zapewnienia ich przydatności, adekwatności i skuteczności.

INFORMACJA O ZAGROŻENIACH

Informacja o zagrożeniach dla bezpieczeństwa i zdrowia występujących podczas pracy na terenie Krajowej Informacji Skarbowej

Podczas przebywania i wykonywania prac na terenie budynków Krajowej Informacji Skarbowej, osoby zatrudnione u innego pracodawcy powinny zwrócić szczególną uwagę na zagrożenia, z którymi mogą się spotkać, m.in. w sytuacjach:

1) przemieszczania się na terenie obiektów (ciągi komunikacyjne wewnątrz i na zewnątrz budynków, parkingi, place manewrowe, rampy rozładunkowe itp.), możliwość poślizgnięcia, potknięcia, upadku z wysokości, potrącenia przez poruszające się środki transportu;
2) korzystania z dźwigów osobowych szczególnie podczas wsiadania lub wysiadania – m.in możliwość upadku z wysokości;
3) korzystania z maszyn, urządzeń i narzędzi – możliwość doznania urazu w wyniku używania niesprawnego lub uszkodzonego sprzętu;
4) kontaktu z uszkodzonymi przewodami, przełącznikami, gniazdkami itp. – możliwość porażenia prądem elektrycznym;
5) wykonywania pracy na wysokości – możliwość upadku, doznania urazu np. z powodu używania niesprawnego sprzętu, nieużywania lub nieprawidłowego używania przez pracowników środków ochrony indywidualnej;
6) pożaru – możliwość poparzenia, zatrucia.

Działania ochronne i zapobiegawcze, które winny być podjęte w celu wyeliminowania lub ograniczenia ww. zagrożeń:

1) przestrzeganie przepisów bezpieczeństwa i higieny pracy oraz przepisów przeciwpożarowych;
2) stosowanie środków ochrony indywidualnej oraz odzieży i obuwia roboczego;
3) korzystanie z maszyn, urządzeń i narzędzi tylko przez osoby do tego upoważnione, posiadające odpowiednie uprawnienia i kwalifikacje;
4) zakaz spożywania na terenie Krajowej Informacji Skarbowej napojów alkoholowych, narkotyków i innych środków odurzających;
5) zakaz wchodzenia i przebywania na terenie Krajowej Informacji Skarbowej, po spożyciu napojów alkoholowych, narkotyków i innych środków odurzających;
6) zakaz palenia wyrobów tytoniowych – także e-papierosów we wszystkich obiektach zakładu pracy. Palenie wyrobów tytoniowych w obrębie budynku dopuszczalne jest wyłącznie w odpowiednio zorganizowanych palarniach lub na zewnątrz budynku;
7) zakaz używania otwartego ognia;
8) poinformowanie osób zatrudnionych u innego pracodawcy o osobach wyznaczonych do udzielania pierwszej pomocy oraz lokalizacji apteczek na terenie danego obiektu;

9) zapoznanie osób zatrudnionych u innego pracodawcy z Instrukcją bezpieczeństwa pożarowego danego obiektu oraz przekazanie informacji o pracownikach wyznaczonych do wykonywania działań w zakresie zwalczania pożarów i ewakuacji pracowników;
10) każde zauważone zagrożenie, incydent lub wypadek należy zgłosić koordynatorowi sprawującemu nadzór nad bezpieczeństwem i higieną pracy.

TELEFONY ALARMOWE

Telefon alarmowy	112
Pogotowie ratunkowe	999
Straż Pożarna	998
Policja	997

Uwaga:

Uzyskanie powyższych informacji potwierdza się podpisem w „Wykazie osób", stanowiącym Załącznik nr 5 do Umowy Nr 0110-KLL2.262.…2026

WYKAZ OSÓB

Wykaz osób wykonujących pracę na terenie Krajowej Informacji Skarbowej, będących pracownikami innego pracodawcy, którzy zostali poinformowani o zagrożeniach dla bezpieczeństwa i zdrowia

Zostałem/am poinformowany/a o zagrożeniach dla bezpieczeństwa i zdrowia występujących na terenie budynków Krajowej Informacji Skarbowej co potwierdzam podpisem:

Lp.	Nazwa i adres pracodawcy	Imię i nazwisko pracownika	Data i czytelny podpis pracownika	Imię i nazwisko oraz podpis informującego o zagrożeniach	Uwagi
1.	2.	3.	4.	5.	6.

Podstawa prawna:
§ 2 ust. 2 rozporządzenia Ministra Gospodarki i Pracy z dnia 27 lipca 2004 roku w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy (Dz.U. Nr z 2024 r. poz. 1327).

WYKAZ OSÓB PRZEPROWADZAJĄCYCH PROCEDURĘ POŚWIADCZENA TOŻSAMOŚCI SUBSKRYBENTÓW

Miejsce realizacji umowy	***Imię i nazwisko osoby Wykonawcy /Podwykonawcy***
Krajowa Informacja Skarbowa w Bielsku-Białej ul. Warszawska 5, 43-300 Bielsko-Biała	
Krajowa Informacja Skarbowa w Bielsku-Białej ul. Teodora Sixta 17, 43-300 Bielsko-Biała	
Delegatura Krajowej Informacji Skarbowej w Bielsku-Białej ul. Romualda Traugutta 2, 43-300 Bielsko-Biała	
Delegatura Krajowej Informacji Skarbowej w Lesznie ul. Jana Dekana 6, 64-100 Leszno	
Delegatura Krajowej Informacji Skarbowej w Lesznie ul. Jana Dekana 3b, 64-100 Leszno	
Delegatura Krajowej Informacji Skarbowej w Płocku ul. 1 Maja 10, 09-402 Płock	
Delegatura Krajowej Informacji Skarbowej w Piotrkowie Trybunalskim ul. Wronia 65, 97-300 Piotrków Trybunalski	
Delegatura Krajowej Informacji Skarbowej w Toruniu ul. Św. Jakuba 20, 87-100 Toruń	
Delegatura Krajowej Informacji Skarbowej w Toruniu ul. Szosa Chełmińska 34/36, 87-100 Toruń	
Wydział Krajowej Informacji Skarbowej w Będzinie ul. Józefa Retingera 1, 42-500 Będzin	

0110-KLL2.261.47.2026.1 **Załącznik nr 7 do umowy nr 0110-KLL2.262.…2026**

INFORMACJA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH STRON/REPREZENTANÓW STRON (PODMIOTÓW PUBLICZNYCH / PRYWATNYCH) ORAZ OSÓB WSKAZANYCH DO KONTAKTU / WPÓŁPRACUJĄCYCH W RAMACH REALIZACJI UMOWY

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej zwane RODO, informujemy:

1. Tożsamość i dane kontaktowe administratora

Administratorem Pani/Pana danych osobowych jest Krajowa Informacja Skarbowa reprezentowana przez Dyrektora Krajowej Informacji Skarbowej. Z administratorem można kontaktować się pisemnie na adres: ul. Warszawska 5, 43-300 Bielsko-Biała; elektronicznie na adres e-mail: kis@mf.gov.pl lub na skrzynkę podawczą ePUAP: /KIS/SkrytkaESP; telefonicznie pod nr 33 472-79-00.

2. Dane kontaktowe inspektora ochrony danych

Administrator wyznaczył inspektora ochrony danych, z którym może się Pani/Pan kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z ich przetwarzaniem, elektronicznie na adres email: iod.kis@mf.gov.pl lub pisemnie na adres siedziby administratora.

3. Cele przetwarzania danych i podstawy prawne

Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b, c, f RODO w celu:

1) zawarcia i wykonania umowy – przez okres poprzedzający zawarcie umowy oraz przez okres wykonywania umowy;

2) wypełnienia obowiązku prawnego ciążącego na administratorze, w szczególności wynikającego z przepisów archiwalnych, przepisów podatkowych, przepisów o rachunkowości – przez okres wynikający z tych przepisów;

3) bieżącej komunikacji w związku z zawarciem i realizacją umowy, co stanowi prawnie uzasadniony interes administratora i odbiorcy danych (stron umowy);

4) ustalenia, dochodzenia lub obrony roszczeń z tytułu realizacji umowy.

4. Kategorie danych osobowych i źródła ich pozyskania (dotyczy przypadków pozyskiwania danych osobowych z innych źródeł niż od osoby, której dane dotyczą).

Dane osobowe pozyskaliśmy od strony umowy, w tym dane kontaktowe osób konieczne do jej realizacji, w szczególności: imię i nazwisko, służbowy adres e-mail i/lub służbowy numer telefonu, stanowisko/funkcja i miejsce pracy.

5. Odbiorcy lub kategorie odbiorców danych osobowych

Pani/Pana dane osobowe możemy przekazywać organom lub podmiotom publicznym uprawnionym do uzyskania danych na podstawie obowiązujących przepisów prawa; podmiotom, które prowadzą działalność pocztową oraz innym podmiotom świadczącym usługi na zlecenie stron w zakresie oraz celu zgodnym z umową. Podmiotem, który przetwarza dane osobowe w imieniu Administratora podczas świadczenia usługi wsparcia IT jest Centrum Informatyki Resortu Finansów z siedzibą w Radomiu.

6. Okres przechowywania danych osobowych

Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do udokumentowania czynności z Pani/Pana udziałem, w związku z realizacją umowy, przez okres wynikający z przepisów podatkowych i rachunkowych. Okresy te mogą zostać przedłużone w przypadku potrzeby ustalenia, dochodzenia lub obrony roszczeń z tytułu realizacji umowy. Dokumentacja będzie przechowywana przez okres niezbędny do realizacji ww. celów przetwarzania, a następnie w celach archiwalnych nie dłużej niż przez okres wskazany w Jednolitym Rzeczowym Wykazie Akt Krajowej Informacji Skarbowej, zgodnie z Instrukcją Kancelaryjną i przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

7. Prawa osób, których dane dotyczą

Zgodnie z RODO przysługuje Pani/Panu:

1) prawo dostępu do danych osobowych Pani/Pana dotyczących oraz uzyskania ich kopii;

2) prawo do sprostowania Pani/Pana danych osobowych, które są nieprawidłowe oraz uzupełnienia niekompletnych danych osobowych;

3) prawo żądania usunięcia Pani/Pana danych osobowych. Prawo to nie przysługuje, w szczególności, gdy przetwarzanie danych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa lub do celów archiwalnych w interesie publicznym;

4) prawo żądania ograniczenia przetwarzania Pani/Pana danych osobowych;

5) prawo wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych osobowych, ze względu na Pani/Pana szczególną sytuację, w szczególności, gdy przetwarzamy je na podstawie prawnie usprawiedliwionego interesu;

6) prawo do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych.

8. Informacja o dobrowolności lub obowiązku podania danych osobowych

Podanie danych osobowych jest dobrowolne. Brak wskazania danych osobowych koniecznych do zawarcia umowy uniemożliwi jej nawiązanie. Natomiast brak wskazania osób do kontaktu, celem jej wykonania, uniemożliwi jej realizację.

9. Informacja o zautomatyzowanym podejmowaniu decyzji i profilowaniu

Wobec Pani/Pana nie będą podejmowane decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym ich profilowaniu. Oznacza to, że decyzje nie będą podjęte za pomocą środków technicznych bez udziału człowieka, w tym nie dokonamy automatycznej oceny niektórych czynników osobowych, które Pani/Pana dotyczą.