0110-KLL2.261.64.2026.1 **Załącznik nr 3 do Zaproszenia**

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

zawarta pomiędzy:

Skarbem Państwa - Krajową Informacją Skarbową z siedzibą w Bielsku-Białej przy ul. Warszawskiej 5, 43-300 Bielsko-Biała, NIP: 547 21 69 306, REGON: 366063511,

reprezentowaną przez:

……

zwaną dalej **Zamawiającym**

a

……

NIP: ……, REGON: ……..

reprezentowaną przez:

……..

zwaną dalej **Wykonawcą,**

zwanymi dalej **Stronami.**

W wyniku przeprowadzonego postępowania 0110-KLL2.261.64.2026.1 na wykonanie audytu instalacji elektrycznej oraz weryfikacja mocy przyłączeniowej w budynku Delegatury Krajowej Informacji Skarbowej w Lesznie przy ul. Dekana 6, została zawarta umowa następującej treści:

§ 1

PRZEDMIOT UMOWY

1. Przedmiotem umowy jest wykonanie audytu instalacji elektrycznej oraz weryfikacja mocy przyłączeniowej w budynku Delegatury Krajowej Informacji Skarbowej w Lesznie przy ul. Dekana 6 (zwanego dalej jako: „ekspertyza”) zgodnie z warunkami określonymi w niniejszej umowie, opisie przedmiotu zamówienia stanowiącym załącznik nr 2 do umowy i na podstawie oferty Wykonawcy stanowiącej załącznik nr 1 do umowy.

§ 2

TERMIN I WARUNKI REALIZACJI UMOWY

1. Przedmiot umowy zostanie zrealizowany w terminie do **22 grudnia 2026 r.** Przez termin realizacji umowy Strony rozumieją termin protokolarnego odbioru ekspertyzy.
2. Miejsce realizacji umowy: Delegatura Krajowej Informacji Skarbowej w Lesznie, ul. Dekana 6, 64-100 Leszno.
3. Miejsce dostarczenia ekspertyzy: Delegatura Krajowej Informacji Skarbowej w Lesznie, ul. Dekana 6, 64-100 Leszno.

§ 3

ZASADY WSPÓŁPRACY STRON UMOWY

1. Na Wykonawcy spoczywają w całości obowiązki w zakresie wykonania ekspertyzy zgodnie z powszechnie obowiązującymi przepisami prawa.
2. Wykonawca oświadcza, że ekspertyza będzie opracowana przez pracowników dysponujących odpowiednimi kwalifikacjami i uprawnieniami.
3. Wykonawca zobowiązany jest do zapoznania swoich pracowników oraz osoby współpracujące z nim na innej niż stosunek pracy podstawie 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.
4. Dokumenty określone w ust. 3, w szczególności WYKAZ OSÓB (Załącznik nr 5 do umowy), pozostają w siedzibie Wykonawcy, a ich okazanie następuje na żądanie Zamawiającego.
5. Osobami wyznaczonymi do kontaktów w ramach realizacji umowy, w tym do podpisania protokołu odbioru ekspertyzy są:
   a) ze strony Wykonawcy, tel.: ....., adres e-mail: …… ……. lub inna osoba wskazana przez Wykonawcę,
   b) ze strony Zamawiającego, tel.: ....., adres e-mail: …… ……. lub inna osoba wskazana przez Zamawiającego.

6. Osoby wyznaczone do kontaktów w ramach realizacji umowy wskazane w ust. 5 nie są uprawnione do zaciągania zobowiązań w ramach niniejszej umowy oraz do dokonywania zmian w zakresie jej postanowień.
7. Strony umowy mogą dokonać zmian osób wskazanych w ust. 5 na inne. Zmiana nie stanowi zmiany umowy i dla swej skuteczności wymaga powiadomienia drugiej strony w formie pisemnej lub elektronicznej.

§ 4

WYNAGRODZENIE I WARUNKI PŁATNOŚCI

1. Z tytułu wykonania przedmiotu umowy Wykonawcy przysługuje wynagrodzenie, które wynosi łącznie ……zł brutto (słownie: ……. zł), netto ……zł (słownie: …… zł), zgodnie z formularzem oferty złożonym przez Wykonawcę (załącznik nr 1 do umowy).
2. Wynagrodzenie określone w ust. 1 zawiera wszystkie koszty bezpośrednie, pośrednie związane z prawidłową realizacją umowy i stanowi zapłatę za całość prac składających się na przedmiot umowy i uwzględnia koszty niezbędne do jej realizacji.
3. Podstawą wystawienia faktury przez Wykonawcę będzie podpisany bez zastrzeżeń przez obie strony protokół odbioru ekspertyzy – Załącznik nr 3 do umowy.
4. Wynagrodzenie za wykonanie przedmiotu umowy płatne będzie na podstawie prawidłowo wystawionej przez Wykonawcę faktury VAT i podpisanego przez obie Strony protokołu odbioru ekspertyzy – załącznik nr 3 do umowy. Płatność nastąpi przelewem na rachunek bankowy Wykonawcy wskazany na fakturze, w ciągu **7 dni kalendarzowych** od dnia dostarczenia faktury. Dane do faktury: **Krajowa Informacja Skarbowa ul. Warszawska 5, 43-300 Bielsko-Biała, NIP: 547 21 69 306 i REGON: 366063511.**
5. W związku z obowiązywaniem 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.

6. 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: kancelaria.kis@mf.gov.pl.
7. Za datę dokonania zapłaty Strony uznają datę obciążenia rachunku bankowego Zamawiającego.
8. Wykonawca nie może bez pisemnej zgody Zamawiającego przenieść wierzytelności wynikających z tytułu niniejszej umowy na osoby trzecie, ani dokonywać kompensaty.
9. W przypadku opóźnienia w zapłacie wynagrodzenia w terminie uzgodnionym w ust. 11 umowy 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.
10. 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.

§ 5

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 przypadku niewykonania umowy lub odstąpienia od umowy lub jej wypowiedzenia z przyczyn, za które Wykonawca ponosi odpowiedzialność – karę umowną w wysokości 20% wynagrodzenia brutto określonego w § 4 ust. 1 umowy,
   2) w przypadku nieuzasadnionego przekroczenia terminu wykonania ekspertyzy o którym mowa w § 2 ust. 1 umowy karę umowną za każdy rozpoczęty dzień

opóźnienia w wysokości 100,00 zł (słownie: sto złotych 0/100) nie więcej niż 2.000,00 zł (słownie: dwa tysiące złotych 0/100).

3. Kary umowne zastrzeżone na rzecz Zamawiającego mogą być dochodzone z każdego tytułu odrębnie i podlegają łączeniu.
4. Zapłata przez Wykonawcę kary umownej nie zwalnia Wykonawcy z obowiązku realizowania zapisów określonych niniejszą umową, za wyjątkiem ust. 2 pkt 1.
5. Gdy szkoda będzie wyższa niż kara umowna, Zamawiający będzie uprawniony do dochodzenia odszkodowania przenoszącego wysokość kary umownej.
6. Termin zapłaty kary umownej wynosi 7 dni od daty doręczenia Wykonawcy zawiadomienia o obciążeniu karą umowną.
7. 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.).
8. W przypadku niezapłacenia kary umownej przez Wykonawcę w terminie wskazanym w zawiadomieniu o obciążeniu karą umowną Wykonawca wyraża zgodę na potrącanie przez Zamawiającego kar umownych z należnego Wykonawcy wynagrodzenia.
9. W przypadku braku możliwości lub prawnej dopuszczalności potrącenia kary z wynagrodzenia należnego Wykonawcy, będą one dochodzone na zasadach ogólnych.

§ 6

ODSTĄPIENIE OD UMOWY I JEJ ROZWIĄZANIE

1. Zamawiający może odstąpić od całości lub części umowy w przypadkach określonych w umowie lub przepisach obowiązującego prawa, w szczególności ustawy Kodeks cywilny.
2. Zamawiający może odstąpić od części lub całości umowy ze skutkiem ex-nunc z przyczyn leżących po stronie Wykonawcy, w szczególności:
    1) nieuzasadnionego niedotrzymania terminu wykonania umowy, o którym mowa w § 2 ust. 1 umowy o więcej niż 5 dni roboczych, z przyczyn nieleżących po stronie Wykonawcy,

2) w razie utraty przez Wykonawcę uprawnień, niezbędnych do wykonywania usługi będącej przedmiotem niniejszej umowy,
3) w przypadku dopuszczenia się przez Wykonawcę lub osoby działające w jego imieniu lub na jego zlecenie naruszenia przepisów dotyczących ochrony tajemnic prawnie chronionych,

3. Odstąpienie od umowy następuje w formie pisemnej pod rygorem nieważności i wymaga uzasadnienia.
4. Umowne prawo odstąpienia od umowy, o którym mowa w ust. 2 Zamawiający może zrealizować w terminie 14 (czternastu) dni od powzięcia wiadomości o okolicznościach, będących podstawą odstąpienia.

§ 7

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 ustaleniami umowy oraz wynikającymi z obowiązujących uregulowań prawnych.
3. Wykonawca zobowiązuje się do ujawnienia informacji dotyczących przedmiotu umowy, w tym informacji technicznych, technologicznych 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. Wykonawcę zobowiązuje się do niekopiowania, niepowielania, a także do nierozpowszechniania jakiejkolwiek części informacji związanych z realizacją umowy z wyjątkiem uzasadnionej potrzeby do celów związanych z realizacją umowy po uprzednim uzyskaniu pisemnej zgody od Zamawiającego, którego informacja lub źródło informacji dotyczy.

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, a 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 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, którego informacja lub źródło informacji dotyczy.
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 przez ujawnienie, przekazanie, wykorzystanie, zbycie lub oferowanie do zbycia informacji otrzymanych od Zamawiającego, wbrew postanowieniom umowy. Zobowiązanie to wiąże Wykonawcę

również po wykonaniu przedmiotu umowy, jej rozwiązaniu, wygaśnięciu lub odstąpieniu, bez względu na przyczynę.

12. Wykonawca oświadcza, że:

    1) znana jest mu treść przepisów w zakresie ochrony informacji i tajemnic prawnie chronionych tj.

        a) ustawa z dnia 6 czerwca 1997 r. Kodeks Karny,

        b) 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 („RODO"),

        c) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,

        a także, że będzie ich przestrzegał zarówno w czasie realizacji Umowy jak i po jej zakończeniu;

    2) 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 oraz zapoznała się z treścią ww. przepisów i zobowiązała się do ich przestrzegania, zarówno w czasie realizacji umowy, jak i po jej zakończeniu.

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 6 do umowy.

§ 8

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.

§ 9

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 , składanych w formie elektronicznej oświadczeń o odstąpieniu od umowy, jej wypowiedzeniu oraz do przesyłania korespondencji dotyczącej nałożenia kar umownych po odstąpieniu od umowy lub jej wypowiedzeniu, jednakże w terminie nie dłuższym jak 60 dni od daty odstąpienia lub wypowiedzenia, chyba że doręczenie nastąpi za pośrednictwem poczty, kuriera lub posłańca na adresy wskazane na wstępie 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. Załączniki do umowy stanowią jej integralną część.
8. Umowę uważa się za zawartą w chwilą złożenia podpisu przez ostatnią ze Stron.
9. Strony zgodnie postanawiają, że miejscem zawarcia umowy jest miejsce siedziby Zamawiającego.
10. 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.
11. 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 (t.j. Dz. U z 2025 r. poz. 1483 ze zm.) oraz przepisów wykonawczych dotyczących prowadzenia Centralnego Rejestru Umów Jednostek Sektora Finansów Publicznych (CRU). Dane dotyczące niniejszej Umowy podlegają publikacji w CRU w zakresie wynikającym z obowiązujących przepisów prawa.

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

<u>Załączniki do umowy:</u>

1. Załącznik nr 1 – Kopia formularza oferty złożonego przez Wykonawcę,
2. Załącznik nr 2 – Kopia opisu przedmiotu zamówienia,
3. Załącznik nr 3 – Protokół odbioru ekspertyzy,
4. Załącznik nr 4 – Informacja o zagrożeniach,
5. Załącznik nr 5 – Wykaz osób,
6. Załącznik nr 6 – Oświadczenie podmiotu zewnętrznego o zapoznaniu się z zasadami bezpieczeństwa informacji Resortu Finansów,
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.

0110-KLL2.261.64.2026.1 **Załącznik nr 1 do umowy**

KOPIA FORMULARZA OFERTY ZŁOŻONEGO PRZEZ WYKONAWCĘ

0110-KLL2.261.64.2026.1 **Załącznik nr 2 do umowy**

KOPIA OPISU PRZEDMIOTU ZAMÓWIENIA

0110-KLL2.261.64.2026.1 **Załącznik nr 3 do umowy**

PROTOKÓŁ ODBIORU EKSPERTYZY

1. Zamawiający: Krajowa Informacja Skarbowa, ul. Warszawska 5, 43-300 Bielsko-Biała.
2. W wyniku realizacji umowy nr 0110-KLL2.262…..2026, w dniu ……. dokonano odbioru następujących dokumentów, składających się na ekspertyzę:

Lp.	Nazwa	Ilość sztuk
1		
2		
3		
4		
5		

UWAGI ZAMAWIAJĄCEGO:

……
……..

Za Zamawiającego: Za Wykonawcę:

(imię, nazwisko i podpis) *(imię, nazwisko i podpis)*

0110-KLL2.261.64.2026.1 **Załącznik nr 4 do umowy**

INFORMACJA O ZAGROŻENIACH

Informacja o zagrożeniach dla bezpieczeństwa i zdrowia występujących podczas pracy na terenie budynku Delegatury Krajowej Informacji Skarbowej w Lesznie przy ul. Dekana 6, 64-100 Leszno

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

0110-KLL2.261.64.2026.1 **Załącznik nr 5 do umowy**

WYKAZ OSÓB

wykonujących pracę na terenie budynku Delegatury Krajowej Informacji Skarbowej w Lesznie przy ul. Dekana 6, 64-100 Leszno, 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 budynku Delegatury Krajowej Informacji Skarbowej w Lesznie przy ul. Dekana 6, 64-100 Leszno, 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.

<u>Podstawa prawna</u>:

§ 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. z 2024 r. poz. 1327)

0110-KLL2.261.64.2026.1 *Załącznik nr 6 do umowy*

OŚWIADCZENIE PODMIOTU ZEWNĘTRZNEGO

.....
(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
[3] wypełnić tylko w wersji papierowej

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 DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH STRON/REPREZENTANÓW STRON (PODMIOTÓW PUBLICZNYCH / PRYWATNYCH) ORAZ OSÓB WSKAZANYCH DO KONTAKTU / WSPÓŁPRACUJĄCYCH W RAMACH REALIZACJI UMOWY NR 0110-KLL2.262……..2026

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 KIS. 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:

- zawarcia i wykonania umowy – przez okres poprzedzający zawarcie umowy oraz przez okres wykonywania umowy;
- wypełnienia obowiązku prawnego ciążącego na administratorze, w szczególności wynikającego z przepisów archiwalnych, przepisów podatkowych, przepisów o rachunkowości – przez okres wynikający z tych przepisów;
- bieżącej komunikacji w związku z zawarciem i realizacją umowy, co stanowi prawnie uzasadniony interes administratora i odbiorcy danych (stron umowy);
- 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.