



Ministerstwo Spraw Zagranicznych

Numer ogłoszenia:

BK 10/2026

Data ukazania się ogłoszenia: 25.02.2026 r.

Nazwa oferowanego stanowiska:

Ministerstwo Spraw Zagranicznych w Warszawie

Dyrektor Generalna Służby Zagranicznej poszukuje kandydatek/kandydatów na stanowisko audytor wewnętrzny/audytorka wewnętrzna ds. bezpieczeństwa informacji i cyberbezpieczeństwa w Referacie ds. Audytu w Biurze Kontroli, Audytu i Ewaluacji

Wskaźnik zatrudnienia osób niepełnosprawnych w urzędzie

W miesiącu poprzedzającym datę upublicznienia ogłoszenia wskaźnik zatrudnienia osób niepełnosprawnych w urzędzie, w rozumieniu przepisów o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych **jest niższy niż 6%**.

Wymiar etatu: 1

Liczba stanowisk pracy: 1

Adres urzędu i miejsce wykonywania pracy:

Ministerstwo Spraw Zagranicznych
Al. J. Ch. Szucha 23
00-580 Warszawa

Zakres zadań wykonywanych przez osobę zatrudnioną na stanowisku pracy:

1. Przeprowadza zadania audytowe w obszarach działania komórek organizacyjnych MSZ właściwych dla bezpieczeństwa informacji, cyberbezpieczeństwa i informatyki a także bezpieczeństwa fizycznego, w zakresie, w jakim ma ono wpływ na bezpieczeństwo informacji, lub w obszarach działania jednostek podległych i nadzorowanych przez kierownika jednostki, w zakresie zgodności z przepisami prawa oraz normami i standardami technicznymi a także najlepszymi praktykami dotyczącymi cyberbezpieczeństwa lub bezpieczeństwa informacji. Wyznacza zakres audytów na podstawie analizy ryzyka, programuje ich zakres i harmonogram, prowadzi dokumentację audytów oraz ustala stan faktyczny zgodnie z metodyką obowiązującą w audycie. Formułuje oceny i zalecenia dotyczące stanu kontroli zarządczej w obszarach bezpieczeństwa informacji i cyberbezpieczeństwa.
2. Przeprowadza czynności doradcze służące wspieraniu kierownika jednostki w realizacji celów i zadań oraz przedstawia propozycje w zakresie wdrożenia nowych lub usprawnienia funkcjonujących mechanizmów kontroli zarządczej.

3. Przeprowadza czynności sprawdzające, monitoruje realizację zaleceń audytowych oraz dokonuje oceny działań komórek organizacyjnych lub jednostek podległych i nadzorowanych przez kierownika jednostki w ramach ich realizacji.
4. Uczestniczy w przeprowadzaniu analizy ryzyka na potrzeby planowania rocznego i strategicznego zadań audytowych, uwzględniającej cele i zadania jednostki oraz ryzyka wpływające na ich realizację w obszarach dot. bezpieczeństwa informacji i cyberbezpieczeństwa.
5. Uczestniczy w opracowywaniu rocznych i wieloletnich planów audytu w celu wyznaczenia obszarów i zadań audytu do realizacji w danym okresie oraz sporządzaniu sprawozdań z wykonania tych planów.
6. Uczestniczy w przygotowaniu dla kierownika jednostki i Komitetu Audytu zbiorczych informacji i ocen dotyczących stanu, istotnych ryzyk i proponowanych usprawnień kontroli zarządczej.
7. Dokumentuje czynności i zdarzenia mające istotne znaczenie dla prowadzenia audytu wewnętrznego w celu spełnienia wymogów w tym zakresie określonych w obowiązujących przepisach.
8. Uczestniczy w działaniach mających na celu ciągłe podnoszenie jakości audytu wewnętrznego w celu spełnienia wymogów obowiązujących standardów audytu wewnętrznego.

Warunki pracy:

Warunki dotyczące charakteru pracy na stanowisku i sposobu wykonywania zadań:

1. krajowe lub zagraniczne wyjazdy służbowe,
2. zagrożenie korupcją,
3. częste reprezentowanie urzędu na zewnątrz.

Miejsce i otoczenie organizacyjno-techniczne stanowiska pracy:

Praca administracyjno-biurowa przy komputerze z monitorem ekranowym powyżej 4 godzin dziennie, wymagająca obsługi również innych urządzeń biurowych. Długotrwałe skupianie wzroku na tej samej płaszczyźnie. Stanowisko pracy zorganizowane w pomieszczeniu biurowym. Bariery architektoniczne: możliwość ograniczonego poruszania się po budynku – obecność wind, brak podjazdów, drzwi z samozamykaczami.

W związku z wyjazdami służbowymi otoczenie i warunki pracy mogą być różne.

Wymagania związane ze stanowiskiem pracy:

Niezbędne:

Wykształcenie:

wyższe lub równorzędne

Doświadczenie zawodowe:

co najmniej 2 lata w obszarze przeprowadzania audytów lub kontroli w obszarach bezpieczeństwa informacji lub cyberbezpieczeństwa

Pozostałe wymagania niezbędne:

1. Szkolenia zawodowe z zakresu audytu lub kontroli.
2. Posiadanie kwalifikacji zawodowych określonych w przepisach prawa dla stanowiska audytor wewnętrzny, zgodnie z ustawą o finansach publicznych: zdany egzamin potwierdzony certyfikatem: Certified Internal Auditor (CIA) lub Certified Government Auditing Professional (CGAP) lub Certified Information Systems Auditor (CISA) lub Association of Chartered Certified Accountants (ACCA) lub Certified Fraud Examiner (CFE) lub Certification in Control Self Assessment (CCSA) lub Certified Financial Services Auditor (CFSA) lub Chartered Financial Analyst (CFA) lub złożony w latach 2003-2006, z wynikiem pozytywnym, egzamin na audytora wewnętrznego przed Komisją Egzaminacyjną powołaną przez Ministra Finansów, lub uprawnienia biegłego rewidenta, lub dwuletnia

praktyka w zakresie audytu wewnętrznego i dyplom ukończenia studiów podyplomowych w zakresie audytu wewnętrznego, o których mowa w ustawie o finansach publicznych.

3. Poświadczenie bezpieczeństwa do klauzuli „tajne” lub zgoda na poddanie się postępowaniu sprawdzającemu.
4. Znajomość języka angielskiego na poziomie B2 albo łącznie: języka angielskiego na poziomie A2 i innego języka obcego na poziomie B2.
5. Znajomość aktów prawnych regulujących kwestie związane z prowadzeniem audytu wewnętrznego, w tym dotyczących obszarów bezpieczeństwa informacji i cyberbezpieczeństwa.
6. Posiadanie wiedzy merytorycznej oraz umiejętności praktycznych w zakresie realizacji zadań audytu wewnętrznego, w tym znajomość technik i metodyki audytu wewnętrznego, standardów audytu wewnętrznego oraz innych dokumentów określających zasady przeprowadzania audytów bezpieczeństwa informacji i cyberbezpieczeństwa.
7. Odpowiednia do wykonywanych zadań znajomość zagadnień informatyzacji.
8. Umiejętność tworzenia dokumentów dotyczących bezpieczeństwa.
9. Wiedza w zakresie zasad funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji.
10. Kompetencje: współpraca, komunikacja (w tym argumentowanie), organizacja pracy własnej i orientacja na osiąganie celów, samodzielność i inicjatywa, rzetelność, umiejętności analityczne, radzenie sobie ze stresem.
11. Posiadanie obywatelstwa polskiego.
12. Korzystanie z pełni praw publicznych.
13. Nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.
14. W służbie cywilnej nie może być zatrudniona osoba, która w okresie od dnia 22 lipca 1944 r. do dnia 31 lipca 1990 r. pracowała lub pełniła służbę w organach bezpieczeństwa państwa lub była współpracownikiem tych organów w rozumieniu przepisów ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów - nie dotyczy kandydatek/kandydatów urodzonych 1 sierpnia 1972 r. lub później. Osoba wybrana do zatrudnienia będzie musiała złożyć oświadczenie lustracyjne, jeśli urodziła się przed 1 sierpnia 1972 r.

Dodatkowe:

Wykształcenie:

wyższe magisterskie lub równorzędne na jednym z kierunków: prawo, informatyka, bezpieczeństwo, informacji, finanse, ekonomia, socjologia, zarządzanie, administracja

Doświadczenie zawodowe:

co najmniej 2 lata w jednostkach sektora finansów publicznych

Pozostałe wymagania dodatkowe:

1. Zdany egzamin potwierdzony certyfikatem: Certified Information Systems Auditor (CISA).
2. Znajomość języka angielskiego lub innego języka obcego na poziomie C1.

Dokumenty i oświadczenia:

niezbędne:

1. Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie wykształcenia.
2. Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie doświadczenia.
3. Kopie dokumentów potwierdzających spełnienie wymagania niezbędnego w zakresie przeszkolenia.
4. Kopia poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą „tajne” lub oświadczenie o wyrażeniu zgody na przeprowadzenie postępowania sprawdzającego zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 632, 1222).

5. CV.
6. Kwestionariusz on-line pod adresem <https://system.erecruiter.pl/FormTemplates/RecruitmentForm.aspx?WebID=32f456c84862469e90aaceb5afbedd88> (preferowany) lub kwestionariusz aplikacyjny znajdujący się na stronie MSZ (gov.pl/dyplomacja) w zakładce Praca i Kariera – Nabór do MSZ – Nabory: użyteczne informacje i pliki do pobrania: <https://www.gov.pl/web/dyplomacja/nabory-uzyteczne-informacje-i-pliki-do-pobrania>.
7. Oświadczenie o posiadaniu obywatelstwa polskiego.
8. Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych do celów naboru.
9. Oświadczenie o korzystaniu z pełni praw publicznych.
10. Oświadczenie o nieskazaniu prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.
11. Oświadczenie o przebiegu kształcenia w zagranicznych podmiotach systemu szkolnictwa wyższego i nauki.
12. Oświadczenie o niewspółpracowaniu z organami bezpieczeństwa państwa w latach 1944-1990 (nie dotyczy kandydatek/kandydatów urodzonych 1 sierpnia 1972 r. lub później).

dodatkowe:

1. Kopia dokumentu potwierdzającego niepełnosprawność – w przypadku osób, które zamierzają skorzystać z pierwszeństwa w zatrudnieniu, jeżeli znajdują się w gronie najlepszych kandydatek/kandydatów.
2. Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie wykształcenia.
3. Kopie dokumentów potwierdzających spełnienie wymagania dodatkowego w zakresie doświadczenia zawodowego.

Oferujemy:

- **wynagrodzenie zasadnicze od ok. 9600 zł do ok. 10800 zł brutto**
- dodatek stażowy w wysokości do 20% wynagrodzenia zasadniczego
- **możliwość ubiegania się o dodatek teleinformatyczny** zgodnie z wymaganiami określonymi w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa w wysokości zgodnej z załącznikiem do rozporządzenia Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa
- dodatkowe wynagrodzenie roczne
- nagroda jubileuszowa
- odprawa emerytalna/rentowa
- nagrody uznaniowe za wyniki i osiągnięcia
- elastyczny czas pracy (możliwość rozpoczęcia pracy między 7:00 a 10:00)
- bony podarunkowe
- dofinansowanie do żłobka i przedszkola*
- dofinansowanie wypoczynku*
- dofinansowanie zajęć sportowych i kulturalnych*
- karta Multisport
- dofinansowanie zakupu okularów i szkielek korekcyjnych
- wsparcie finansowe rozwoju zawodowego (szkolenia, kursy językowe)
- Pracownicza Kasa Zpomogowo-Pożyczkowa
- Przychodnia Lekarska Służby Zagranicznej (internista, stomatolog)
- biblioteka
- drużyna sportowa
- bufet pracowniczy
- doskonała lokalizacja
- pomieszczenie lub stojaki na rowery na terenie urzędu

* wysokość świadczenia uzależniona od kryterium dochodowego

Termin składania dokumentów: 17.03.2026 r.

Decyduje data wpływu oferty do urzędu

Miejsce składania dokumentów:

Kwestionariusz aplikacyjny on-line (preferowany) na stronie:

<https://system.erecruiter.pl/FormTemplates/RecruitmentForm.aspx?WebID=32f456c84862469e90aaceb5afbedd88>

lub

Ministerstwo Spraw Zagranicznych

Biuro Kapitału Ludzkiego

Al. J. Ch. Szucha 23

00-580 Warszawa

z dopiskiem na kopercie oraz w aplikacji: **BK 10/2026**

Dziennik Podawczy:

czynny w godzinach 8.30 – 16.00 (przerwa 12:00-12:30). Oferty otrzymane po terminie nie będą rozpatrywane.

Kontakt:

W ofercie należy podać adres e-mail oraz numer telefonu. Osoby zakwalifikowane będą informowane e-mailem lub telefonicznie o terminie kolejnego etapu naboru.

Kontakt: Wydział Naboru, tel. +48 (22) 523 8751 email: rekrutacja@msz.gov.pl

Inne informacje:

Informacje dotyczące kopii dokumentów potwierdzających spełnianie wymagań

Szczegółowe informacje dotyczące kopii dokumentów potwierdzających spełnianie wymagań niezbędnych oraz dodatkowych znajdują się na stronie Biuletynu Informacji Publicznej MSZ w zakładce Praca i kariera – Praca w MSZ – Zasady i użyteczne informacje:

<https://www.gov.pl/web/dyplomacja/nabory-uzyteczne-informacje-i-pliki-do-pobrania>

Kompletna aplikacja to taka, która zawiera wszystkie wymagane dokumenty. NIEKOMPLETNE APLIKACJE NIE BĘDĄ ROZPATRYWANE.

Dokumenty w języku polskim opatrzone podpisem

Nabór przeprowadzany jest w języku polskim (z wyjątkiem etapu sprawdzającego umiejętności językowe). Wszelkie dokumenty załączane do oferty wystawione w języku obcym winny być przetłumaczone na język polski lub angielski. Dokumenty winny być odwzorowane cyfrowo w przypadku skorzystania z kwestionariusza aplikacyjnego on-line. Dokumenty złożone w aplikacji nie będą zwracane. Po zakończeniu naboru oferty osób nie wskazanych do zatrudnienia będą zniszczone.

Wymogi dotyczące uznania dyplomu studiów wyższych na uczelni zagranicznej

W przypadku ukończenia studiów wyższych na uczelni zagranicznej, prosimy o przesłanie kopii potwierdzenia uznania dyplomu przez Narodową Agencję Wymiany Akademickiej lub nostryfikacji dyplomu oraz tłumaczenie przysięgłe. Informacje dotyczące uznawalności

zamieszczone są na stronie NAWA: <https://nawa.gov.pl/uznawalnosc/wydawanie-informacji-o-zagranicznych-dyplomach>

Dostępność

Osoby ze szczególnymi potrzebami mogą je zgłosić na etapie składania dokumentów (m.in. dostępność pomieszczenia dla osób poruszających się na wózkach inwalidzkich).

Dostosowujemy w miarę możliwości materiały używane podczas naboru do potrzeb osób ze szczególnymi potrzebami (np. większa czcionka w materiałach drukowanych), a także zwiększamy czas poszczególnych metod i technik naboru, jeśli to konieczne.

Proces naboru będzie składać się z następujących etapów:

- formalnej weryfikacji zgłoszeń - do kolejnego etapu zaproszone zostaną osoby, które spełnią wymagania formalne zawarte w ogłoszeniu;
- w zależności od ilości zgłoszeń spełniających wymagania formalne kolejne etapy naboru mogą składać się ze sprawdzianu wiedzy i/lub rozmowy kwalifikacyjnej - celem rozmowy będzie m.in. poznanie przygotowania i motywacji do pracy na proponowanym stanowisku oraz sprawdzenie wiedzy wymaganej w ogłoszeniu, w tym także umiejętności językowych (jeśli dotyczy).

Informacja o pracodawcy:

Ministerstwo Spraw Zagranicznych jest pracodawcą równych szans i wszystkie aplikacje są rozważane z równą uwagą bez względu na płeć, wiek, niepełnosprawność, rasę, narodowość, przekonania polityczne, przynależność związkową, pochodzenie etniczne, wyznanie, orientację seksualną czy też jakąkolwiek inną cechę prawnie chronioną.

Dane osobowe - klauzula informacyjna

Informacja dotycząca przetwarzania przez MSZ danych osobowych kandydatek/kandydatów biorących udział w procesie rekrutacji na stanowiska w służbie cywilnej, stanowiąca realizację obowiązku określonego w art. 13 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 (RODO) (Dz. Urz. UE L 119 z 4.05.2016 r., s. 1 oraz Dz. Urz. UE L 127 z 23.05.2018 r., s. 2).

1. Administratorem, w rozumieniu art. 4 pkt 7 RODO, danych osobowych osób biorących udział w naborze jest Minister Spraw Zagranicznych z siedzibą w Polsce, w Warszawie, Al. J. Ch. Szucha 23, 00-580 Warszawa.
2. Minister Spraw Zagranicznych powołał Inspektora Ochrony Danych (IOD), który realizuje swoje obowiązki w odniesieniu do danych przetwarzanych w Ministerstwie Spraw Zagranicznych i placówkach zagranicznych, Al. J. Ch. Szucha 23, 00-580 Warszawa, adres e-mail: iod@msz.gov.pl.
3. Dane osobowe są przetwarzane w celu przeprowadzenia postępowania rekrutacyjnego na wybrane stanowisko w służbie cywilnej:
 - 1) w oparciu o art. 6 ust. 1 lit. c RODO w zakresie wskazanym w art. 22¹ § 1 pkt. 1 – 3 Kodeksu Pracy,
 - 2) w oparciu o art. 6 ust. 1 lit. b RODO w zakresie wskazanym w art. 22¹ § 1 pkt. 4 – 6 Kodeksu Pracy,
 - 3) w oparciu o art. 6 ust. 1 lit. c oraz art. 10 RODO w zakresie danych niezbędnych do weryfikacji kryteriów wskazanych w art. 4 ustawy o służbie cywilnej,
 - 4) w oparciu o art. 9 ust. 2 lit. b RODO w zakresie wskazanym w art. 28 ust. 2b ustawy z dnia 21 listopada 2008 r. o służbie cywilnej,
 - 5) w oparciu o art. 6 ust. 1 lit. a oraz art. 9 ust. 2 lit. a RODO, tj. na podstawie zgody w zakresie danych nie objętych przepisami prawa, które zostały przekazane z własnej inicjatywy.
4. Podanie danych osobowych wskazanych w przepisach prawa jest niezbędne, aby uczestniczyć w postępowaniu rekrutacyjnym. Konsekwencją ich niepodania będzie brak możliwości udziału w naborze na stanowisko, którego dotyczy ogłoszenie. Podanie innych danych osobowych wykraczających poza zakres wskazany w przepisach prawa zostanie potraktowane jako zgoda na ich przetwarzanie. Wyrażenie zgody jest dobrowolne, zaś zgodę można odwołać w dowolnym czasie, poprzez przesłanie stosownej informacji na adres e-mail: rekrutacja@msz.gov.pl. W przypadku zgody na przetwarzanie danych osobowych szczególnych kategorii, musi być ona wyrażona w sposób

wyraźny. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

5. Dane osobowe zawarte w protokole naboru obejmujące do pięciu najlepszych kandydatek/kandydatów będą przetwarzane przez okres niezbędny do realizacji celu przetwarzania, a następnie przechowywane w celach archiwalnych przez okres 5 lat, zgodnie z przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164, z 2025 r. poz. 1173) oraz przepisami wewnętrznymi MSZ wynikającymi z przepisów ww. ustawy. Dane pozostałych osób biorących udział w naborze oraz dane zamieszczone w przesłanych dokumentach zostaną usunięte bezpośrednio po zakończeniu naboru lub po 3 miesiącach od jego zakończenia.
6. Dane osobowe mogą być udostępniane osobom i podmiotom trzecim uprawnionym do dostępu do nich na podstawie obowiązujących przepisów prawa. Dotyczy to w szczególności imion i nazwisk kandydatek/kandydatów, którzy spełniają wymagania formalne w zakresie określonym w ogłoszeniu o naborze oraz wyniku naboru, stanowiącym informację publiczną. Odrębną kategorię odbiorców stanowią podmioty przetwarzające dane osobowe na zlecenie Administratora, w szczególności w związku z podpisanymi umowami, np. dostawcy usług IT.
7. Uprawnienia przysługujące osobom, których dane dotyczą:
 - prawo do dostępu do treści swoich danych;
 - prawo do żądania sprostowania danych osobowych, które są nieprawidłowe;
 - prawo do cofnięcia zgody na przetwarzanie danych osobowych, jeżeli była ona podstawą przetwarzania;
 - prawo do usunięcia danych, w szczególności, jeżeli przetwarzanie danych opiera się na zgodzie, w myśl art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO lub dane osobowe są przetwarzane niezgodnie z prawem;
 - prawo do ograniczenia przetwarzania danych, w sytuacjach i na zasadach wskazanych w art. 18 RODO.
8. Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, który będzie miał wpływ na podejmowanie decyzji mogących wywołać skutki prawne lub w podobny sposób istotnie na nią wpłynąć, w tym nie będą poddawane profilowaniu.
9. Osobie, której dane dotyczą przysługuje prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Moniuszki 1A, 00-014 Warszawa.