ZAPROSZENIE DO WYRAŻENIA ZAINTERESOWANIA STANOWISKAMI PRACOWNIKÓW KONTRAKTOWYCH

W DZIEDZINIE BEZPIECZEŃSTWA ICT
Grupa funkcyjna III: Asystent ds. bezpieczeństwa ICT
Grupa funkcyjna IV: Analityk ds. bezpieczeństwa ICT

EPSO/CAST/S/7/2013

I. WPROWADZENIE

Na wniosek instytucji Unii Europejskiej Europejski Urząd Doboru Kadr (EPSO) ogłasza procedurę selekcji w celu utworzenia bazy danych osób, spośród których mogą być rekrutowani pracownicy kontraktowi **w dziedzinie ICT i bezpieczeństwa cybernetycznego**.

Instytucje Unii Europejskiej rekrutują personel kontraktowy, aby uzyskać dodatkowy potencjał w specjalistycznych dziedzinach. Personel kontraktowy jest zatrudniony zgodnie z warunkami podanymi w ppkt IX niniejszego zaproszenia do wyrażenia zainteresowania.

Stosunki pracy z instytucjami europejskimi są regulowane przez Warunki zatrudnienia innych pracowników Unii Europejskiej. Pełny tekst warunków zatrudnienia można znaleźć na następującej stronie internetowej: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20100101:PL:PDF (rozdział IV, strona 174)[1] .

Baza danych będzie wykorzystywana przez Komisję Europejską, Parlament Europejski, Sekretariat Generalny Rady, Europejską Służbę Działań Zewnętrznych i Komitet Ekonomiczno-Społeczny. **W zależności od potrzeb, miejsca zatrudnienia to głównie Bruksela i Luksemburg. Pewna niewielka liczba miejsc pracy może być zlokalizowana w niektórych delegaturach UE na świecie.**

Procedury selekcji dla personelu kontraktowego przyciągają zazwyczaj dużą liczbę wysoko wykwalifikowanych kandydatów, którzy pomyślnie przechodzą procedurę. Informuje się zatem kandydatów, że w przypadku niektórych profilów możliwe jest, że liczba nazwisk w bazie danych będzie przewyższać potrzeby instytucji.

Poniższa tabela pokazuje szacunkowe zapotrzebowanie instytucji na personel kontraktowy w omawianej dziedzinie w pewnym określonym okresie czasu, biorąc pod uwagę ograniczony charakter umów i rotację pracowników.
Przybliżona liczba laureatów potrzebnych w instytucjach w okresie trzech lat 2014-2016:

Grupa funkcji	Profil	Liczba
GFIII	Asystent ds. bezpieczeństwa ICT	50
GFIV	Analityk ds. bezpieczeństwa ICT	50

Kandydaci mogą składać kandydaturę tylko na jedno stanowisko i do jednej grupy funkcyjnej. Kandydaci składający wniosek do grupy funkcyjnej IV (GFIV) mogą jednak zostać przeklasyfikowani, za ich uprzednią zgodą, do grupy funkcyjnej III (GFIII), jeżeli nie uzyskają wymaganego minimum punktów w testach kompetencji kwalifikujących do GFIV,

[1] Ogólne przepisy wykonawcze regulujące warunki zatrudnienia personelu kontraktowego zatrudnionego przez Komisję Europejską i Parlament Europejski można znaleźć stronie internetowej Europejskiego Urzędu Doboru Kadr.

pod warunkiem, że uzyskają ocenę kwalifikującą do grupy III (zob. szczegółowe informacje w punkcie „VI. Etapy selekcji").
Kandydaci, którzy wyślą więcej niż jedno zgłoszenie, zostaną wykluczeni z procedury naboru.

II. CHARAKTER OBOWIĄZKÓW[2]

GF III – Asystent ds. bezpieczeństwa ICT

Pod nadzorem urzędników lub personelu tymczasowego, członek personelu kontraktowego będzie pomagać w obsłudze komunikatów, koordynacji alarmów i reagowaniu na incydenty, prowadzeniu dochodzeń kryminalistycznych oraz kontroli bezpieczeństwa ICT, zarządzaniu infrastrukturą bezpieczeństwa ICT, określaniu ustawień konfiguracji bezpieczeństwa ICT i opracowywaniu polityki, norm i wytycznych w zakresie bezpieczeństwa ICT.

Przykładowo do obowiązków asystenta ds. bezpieczeństwa ICT może należeć:
- asystowanie przy wdrażaniu rozwiązań w dziedzinie bezpieczeństwa (infrastruktura lub aplikacje) obejmujące projektowanie, konfigurację, programowanie, testowanie i wprowadzanie technologii związanych z bezpieczeństwem, takich jak: zapory sieciowe nowej generacji, zapory aplikacji, zarządzanie tożsamością i uprawnieniami dostępu, systemy IDS i IPS (systemy wykrywania i zapobiegania włamaniom), narzędzia DLP (ochrona przed utratą danych), DRM (zarządzanie prawami cyfrowymi) i NAC (kontrola dostępu do sieci), systemy SIEM (systemy do zarządzania informacją i zdarzeniami bezpieczeństwa) itp.;
- asystowanie przy akcjach podnoszenia świadomości i szkoleniach w dziedzinie bezpieczeństwa informacji, które mają na celu szkolenie pracowników w zakresie ryzyka informatyczne poprzez zapewnienie wskazówek i programów edukacyjnych, oraz bieżącej komunikacji;
- asystowanie przy opracowywaniu, dokumentowaniu i testowaniu kontroli procesu ICT w wielu różnych środowiskach;
- asystowanie przy kontroli i przeglądach kwestii bezpieczeństwa informacji w instytucjach UE;
- asystowanie przy zapewnieniu pomocy użytkownikom lub grupom użytkowników w odniesieniu do kwerend w zakresie bezpieczeństwa; sporządzanie wytycznych i dokumentacji w celu modernizacji linii obrony;
- asystowanie przy wdrażaniu, zarządzaniu i egzekwowaniu polityki bezpieczeństwa ICT, wytycznych i procedur w obrębie instytucji UE;
- pełnienie funkcji urzędnika dyżurującego w ramach zespołu reagowania na incydenty, który analizuje otrzymywane informacje na temat zagrożeń i zagrożonych systemów, ustala znaczenie poszczególnych informacji, opracowuje komunikaty i alarmy oraz przesyła je do właściwych odbiorców;
- asystowanie przy reagowaniu na incydenty zagrażające bezpieczeństwu informacji i przy ocenie otrzymywanych informacji na temat incydentów oraz podejmowanie odpowiednich działań;
- asystowanie przy dochodzeniach kryminalistycznych w zakresie bezpieczeństwa ICT oraz pomoc przy gromadzeniu i analizie artefaktów;
- asystowanie przy badaniu przypadków złośliwego kodu celem określenia wektora ataku, bloku danych, a także zakresu szkód i wycieku danych;
- asystowanie przy wdrażaniu rozwiązań w zakresie bezpieczeństwa dotyczących gromadzenia informacji na temat złośliwej działalności, jak również gromadzeniu informacji na temat podejrzewanej złośliwej działalności, zarządzaniu tymi informacjami oraz ich rozpowszechnianiu;
- asystowanie przy badaniu podejrzanych i faktycznych przypadków naruszenia bezpieczeństwa oraz podejmowaniu w razie konieczności działań naprawczych i sprawozdawaniu z ich wykonania; prowadzenie rejestru wszelkich incydentów oraz zaleceń i działań naprawczych;
- rozmieszczanie, konfigurowanie, zarządzanie i utrzymywanie systemów kryptograficznych;
- rozmieszczanie, konfigurowanie, zarządzanie i utrzymywanie systemów i sieci do przetwarzania informacji tajnych;
- stosowanie/egzekwowanie polityki w zakresie bezpieczeństwa ICT lub jej monitorowanie.

[2] Profile opisane w niniejszym zaproszeniu do wyrażenia zainteresowania są uproszczonymi wersjami profili ogólnych, które zostaną wykorzystane na etapie sporządzania umów. Te uproszczone wersje podaje się w celach informacyjnych i nie są one prawnie wiążące.

GF IV – Analityk ds. bezpieczeństwa ICT

Pod nadzorem urzędnika lub członka personelu zatrudnionego na czas określony personel kontraktowy wykonywać będzie pracę koncepcyjną, analizę oraz nadzór techniczny i administracyjny w dziedzinie wsparcia i infrastruktury ICT.
Członek personelu kontraktowego będzie wykonywać zadania związane z zarządzaniem komunikatami, koordynacją ostrzeżeń i reagowaniem na incydenty, dochodzeniami kryminalistycznymi, kontrolami bezpieczeństwa ICT, zarządzaniem infrastrukturą bezpieczeństwa ICT, określaniem ustawień konfiguracji bezpieczeństwa ICT i opracowywaniem polityki, norm i wytycznych z dziedziny bezpieczeństwa ICT. Wykonywanie tych zadań wymaga między innymi umiejętności redakcyjnych, zdolności analitycznych, wiedzy z zakresu nadzoru technicznego, zarządzania administracyjnego oraz biegłej znajomości oprogramowania biurowego.

Przykładowo do obowiązków analityka ds. bezpieczeństwa ICT może należeć:

- zarządzanie rozwiązaniami, koordynowanie ich i wdrażanie w dziedzinie bezpieczeństwa (infrastruktura lub aplikacje) obejmujące projektowanie, konfigurację, programowanie, testowanie i wprowadzanie technologii związanych z bezpieczeństwem, takich jak: zapory sieciowe nowej generacji, zapory aplikacji, zarządzanie tożsamością i uprawnieniami dostępu, systemy IDS i IPS (systemy wykrywania i zapobiegania włamaniom), narzędzia DLP (ochrona przed utratą danych), DRM (zarządzanie prawami cyfrowymi) i NAC (kontrola dostępu do sieci), systemy SIEM (systemy do zarządzania informacją i zdarzeniami bezpieczeństwa) itp.;
- uruchamianie akcji podnoszenia świadomości i szkoleń w dziedzinie bezpieczeństwa informacji, które mają na celu szkolenie pracowników w zakresie ryzyka informatycznego poprzez zapewnienie wskazówek i programów edukacyjnych, oraz asystowanie przy bieżącej komunikacji; opracowywanie, dokumentowanie i testowanie kontroli procesu ICT w wielu różnych środowiskach;
- zarządzanie projektami dotyczącymi bezpieczeństwa ICT polegające na planowaniu projektów, ocenie produktów, selekcji systemów i dostawców, projektowaniu infrastruktury, ocenie gotowości oraz gwarantowaniu jakości;
- zarządzanie kontrolą i przeglądem kwestii bezpieczeństwa informacji w instytucjach UE oraz koordynacja tych procesów;
- reagowanie na incydenty zagrażające bezpieczeństwu informacji i koordynowanie działań naprawczych;
- kierowanie zespołem reagowania na incydenty w celu zahamowania naruszeń bezpieczeństwa komputerowego, prowadzenie dochodzeń w przypadku ich wystąpienia i zapobieżenia przyszłym incydentom;
- opracowywanie, wdrażanie i egzekwowanie odpowiednich i użytecznych polityk w zakresie bezpieczeństwa oraz zapewnianie, by były one zgodne z dyrektywą UE o ochronie danych i innymi przepisami i uregulowaniami związanymi z bezpieczeństwem informacji; dokonywanie regularnych przeglądów polityki;
- zapewnienie uwzględnienia kwestii bezpieczeństwa informacji w strategiach i wymogach biznesowych;
- koordynowanie dochodzeń kryminalistycznych w zakresie bezpieczeństwa ICT oraz gromadzenie i analiza artefaktów;
- badanie przypadków złośliwego kodu celem określenia wektora ataku, bloku danych, a także zakresu szkód i wycieku danych;
- zarządzanie rozwiązaniami w zakresie bezpieczeństwa dotyczącymi gromadzenia informacji na temat złośliwej działalności, koordynowanie tych rozwiązań i ich wdrażanie, jak również gromadzenie informacji na temat podejrzewanej złośliwej działalności, zarządzanie tymi informacjami oraz ich rozpowszechnianie;
- prowadzenie badań w zakresie bezpieczeństwa i uwzględnianie najnowszych kwestii;
- współpraca z dostawcami, konsultantami zewnętrznymi i innymi osobami trzecimi na rzecz poprawy bezpieczeństwa informatycznego w instytucjach UE;
- zarządzanie integracją systemów bezpieczeństwa informacji w ramach otoczenia biznesowego;
- analiza, ocena i udoskonalanie narzędzi i procesów ICT, procedur i metod pracy w dziedzinie bezpieczeństwa ICT;
- projektowanie, rozmieszczanie, konfigurowanie, zarządzanie i utrzymywanie systemów kryptograficznych;
- projektowanie, rozmieszczanie, konfigurowanie, zarządzanie i utrzymywanie systemów i sieci do przetwarzania informacji tajnych;

- przedstawianie propozycji w dziedzinie polityki w zakresie bezpieczeństwa ICT, stosowanie/wdrażanie tej polityki lub jej monitorowanie.

III. ORIENTACYJNY HARMONOGRAM PROCEDURY SELEKCJI

Procedurą selekcji zarządzać będzie EPSO przy pomocy komisji selekcyjnej składającej się z przedstawicieli departamentów instytucji UE. **Orientacyjny** harmonogram jest następujący:

	Orientacyjne daty
ETAP	
Przegląd CV kandydatów	wrzesień 2013 r.
Test kompetencji	listopad 2013 r.
Wyniki testów kompetencji	grudzień 2013/styczeń 2014 r.

IV. WARUNKI UDZIAŁU W PROCEDURZE NABORU

W dniu upływu terminu składania zgłoszeń drogą elektroniczną kandydat musi spełniać następujące warunki:

A. WARUNKI OGÓLNE	
a) posiadać obywatelstwo jednego z państw członkowskich Unii Europejskiej w dniu upływu terminu składania zgłoszeń;	
b) korzystać z pełni praw publicznych;	
c) mieć uregulowany stosunek do służby wojskowej;	
d) posiadać odpowiednie cechy charakteru niezbędne do wykonywania przyszłych obowiązków.	
B. Minimalne warunki szczegółowe – edukacja i doświadczenie	
GF III – Asystent ds. bezpieczeństwa ICT • Wykształcenie na poziomie pomaturalnym, potwierdzone świadectwem ukończenia nauki, w dziedzinie technicznej związanej z zakresem obowiązków określonych w tytule II, lub • wykształcenie średnie potwierdzone świadectwem ukończenia nauki uprawniającym do podjęcia studiów wyższych oraz odpowiednie, co najmniej trzyletnie doświadczenie zawodowe odpowiadające charakterowi przyszłych obowiązków określonych w tytule II. **GF IV – Analityk ds. bezpieczeństwa ICT** Ukończone co najmniej trzyletnie studia wyższe, potwierdzone dyplomem ukończenia studiów w dziedzinie związanej z zakresem obowiązków określonych w tytule II.	
C. Znajomość języków	
a) Język 1 (L1) oraz b) Język 2 (L2)	Język podstawowy: gruntowna znajomość jednego z języków urzędowych Unii Europejskiej[3] Zadowalająca znajomość (poziom B2[4]) języka angielskiego, francuskiego lub niemieckiego; obowiązkowo innego niż język 1 powyżej. Zgodnie z wyrokiem Trybunału UE (wielka izba) w sprawie C-566/10 P, Republika Włoska przeciwko Komisji, instytucje UE mają obowiązek wskazania powodów ograniczenia w niniejszej procedurze naboru drugiego języka do mniejszej liczby języków urzędowych UE. W związku z tym niniejszym informujemy kandydatów, że możliwości wyboru drugiego języka w ramach niniejszej procedury zostały określone zgodnie z interesem służby, który wymaga, aby nowo zatrudnione osoby były niezwłocznie zdolne do wykonywania obowiązków i do skutecznej komunikacji w codziennej pracy. W przeciwnym razie wydajność pracy w instytucjach poważnie by ucierpiała. Zgodnie z długoletnią praktyką dotyczącą komunikacji wewnętrznej w instytucjach UE, a także z uwagi na potrzeby służb w zakresie komunikacji zewnętrznej i prowadzenia dokumentacji, językami najpowszechniej wykorzystywanymi są angielski, francuski i niemiecki. Ponadto angielski,

[3] Języki urzędowe Unii Europejskiej to: BG (bułgarski), HR (chorwacki), CS (czeski), DA (duński), DE (niemiecki), EL (grecki), EN (angielski), ES (hiszpański), ET (estoński), FI (fiński), FR (francuski), GA (irlandzki), HU (węgierski), IT (włoski), LT (litewski), LV (łotewski), MT (maltański), NL (niderlandzki), PL (polski), PT (portugalski), RO (rumuński), SK (słowacki), SL (słoweński), SV (szwedzki).

[4] Zob. tabela odniesienia na stronie internetowej Europass: http://europass.cedefop.europa.eu/pl/resources/european-language-levels-cefr

	francuski i niemiecki są językami zdecydowanie najczęściej wybieranymi przez kandydatów w kategorii „język 2" w procedurach selekcji, w których można dokonać w tym zakresie swobodnego wyboru. Taka sytuacja odzwierciedla obecne standardy edukacyjne i zawodowe, na podstawie których od kandydatów na stanowiska w Unii Europejskiej można oczekiwać znajomości przynajmniej jednego z tych trzech języków. W związku z tym, uwzględniając interes służby oraz potrzeby i wiedzę kandydatów, a także dziedzinę niniejszej procedury naboru, uzasadnione jest przeprowadzenie testów w trzech wspomnianych językach. Ma to zagwarantować, że wszyscy kandydaci, niezależnie od tego, jaki język jest ich językiem pierwszym, będą władać przynajmniej jednym ze wspomnianych trzech języków urzędowych na poziomie umożliwiającym wykonywanie obowiązków służbowych. Ponadto w interesie równego traktowania kandydatów, wszyscy kandydaci mają obowiązek przystąpienia do testów w swoim drugim języku, wybranym spośród trzech wskazanych. Dotyczy to również kandydatów, których pierwszym językiem jest jeden ze wskazanych trzech języków. Przeprowadzane w taki sposób testy szczególnych kompetencji kandydatów umożliwiają instytucjom dokonanie oceny zdolności kandydatów do bezzwłocznego wykonywania zadań w środowisku, które jest bardzo zbliżone do prawdziwego środowiska pracy. Powyższe pozostaje bez uszczerbku dla możliwości odbywania w późniejszym terminie szkoleń językowych w celu osiągnięcia zdolności do pracy w trzecim języku, zgodnie z art. 85 ust. 3 warunków zatrudnienia innych pracowników Unii.

Jako język podstawowy (L1) kandydaci mogą wskazać tylko jeden z 24 języków urzędowych. Po zatwierdzeniu elektronicznego formularza zgłoszeniowego nie ma możliwości zmiany wybranych języków.

Uwaga: kandydaci, którzy otrzymają zaproszenie na rozmowę kwalifikacyjną będą zobowiązani przedstawić wszystkie dokumenty potwierdzające. Jeżeli okaże się, że informacje przedstawione przez kandydata są nieprawdziwe, zostanie on wykluczony z procedury selekcji, a jego nazwisko usunięte z bazy danych.

V. SPOSÓB i TERMIN SKŁADANIA ZGŁOSZEŃ

Należy zgłosić się drogą elektroniczną zgodnie z procedurą opisaną na stronie internetowej EPSO (http://europa.eu/epso/apply/jobs/index_en.htm), a w szczególności w podręczniku na temat składania zgłoszeń. Formularz zgłoszeniowy należy wypełnić w języku angielskim, francuskim lub niemieckim.

Za dokonanie rejestracji w Internecie we wskazanym terminie odpowiadają sami kandydaci. Zaleca się, by kandydaci nie zwlekali z dokonywaniem zgłoszeń do końca przewidzianego okresu rejestracji, ponieważ duże obciążenie łączy internetowych lub błąd połączenia internetowego może wiązać się z koniecznością powtórzenia całego procesu, co stanie się niemożliwe po upływie wskazanego terminu zgłoszeń.

Po zatwierdzeniu zgłoszenia przez kandydata nie ma możliwości jego modyfikacji; dane są od razu przetwarzane przez EPSO w celu organizacji procedury selekcji.

TERMIN ZGŁASZANIA KANDYDATUR (z zatwierdzeniem włącznie)

16 lipca 2013 r. o godz. 12.00 (w południe) czasu brukselskiego

VI. ETAPY SELEKCJI

SELEKCJA W OPARCIU O ŚWIADECTWA POSIADANYCH KWALIFIKACJI

Kandydaci będą sprawdzani na podstawie ich kwalifikacji, w szczególności pod względem posiadanych dyplomów i doświadczenia zawodowego, zgodnie z kryteriami określonymi poniżej. Kandydaci, których profile najlepiej pasują do obowiązków i kryteriów selekcji, zostaną zaproszeni na test kompetencji.

Powołana zostanie komisja selekcyjna, która wspierać będzie EPSO na tym etapie procedury, w szczególności w celu przeprowadzenia wstępnej selekcji na podstawie kwalifikacji (przegląd CV kandydatów).

Kryteria selekcji opartej na świadectwach posiadanych kwalifikacji

GFIII - Asystent ds. bezpieczeństwa ICT

1. co najmniej 3-letnie doświadczenie zawodowe w dziedzinie bezpieczeństwa ICT lub bezpieczeństwa cybernetycznego, zdobyte po uzyskaniu świadectwa kształcenia pomaturalnego;
2. kandydat posiadający jedynie świadectwo wykształcenia średniego oraz trzyletnie doświadczenie związane z zakresem obowiązków, musi posiadać co najmniej 3-letnie dodatkowe doświadczenie zawodowe w dziedzinie bezpieczeństwa ICT lub bezpieczeństwa cybernetycznego;
3. niezależnie od uzyskanego świadectwa, co najmniej 6 miesięcy doświadczenia zawodowego określonego w pkt 1 lub 2 powinno być bezpośrednio związane z zakresem obowiązków określonych w pkt II „Charakter obowiązków" niniejszego zaproszenia do wyrażenia zainteresowania;
4. certyfikat bezpieczeństwa ICT lub bezpieczeństwa cybernetycznego, taki jak CISSP, GIAC itp.;
5. szkolenia (inne niż wspomniane w warunkach udziału w procedurze naboru, pkt. IV.B niniejszego zaproszenia) w dziedzinie bezpieczeństwa ICT i bezpieczeństwa cybernetycznego;
6. aktywne zaangażowanie w opracowywanie projektów dotyczących bezpieczeństwa ICT;
7. wkład w rozwój standardów w zakresie ICT (np. IETF);
8. doświadczenie w pracy jako członek zespołu reagowania na incydenty;
9. doświadczenie w pracy jako członek zespołu ds. bezpieczeństwa łączności;
10. doświadczenie w pracy z systemami bezpieczeństwa ICT do przetwarzania informacji tajnych;
11. dobra znajomość języka angielskiego (nawet jeśli jest to język 1 lub 2) (co najmniej na poziomie B2[5]).

GFIV - Analityk ds. bezpieczeństwa ICT

1. co najmniej 5-letnie doświadczenie zawodowe w dziedzinie bezpieczeństwa ICT lub bezpieczeństwa cybernetycznego, zdobyte po uzyskaniu wyższego wykształcenia;
2. co najmniej 6 miesięcy doświadczenia zawodowego określonego w pkt 1 powinno być bezpośrednio związane z zakresem obowiązków określonych w pkt II „Charakter obowiązków" niniejszego zaproszenia do wyrażenia zainteresowania;
3. certyfikat bezpieczeństwa ICT lub bezpieczeństwa cybernetycznego, taki jak CISSP, GIAC itp.;
4. szkolenia (inne niż wspomniane w warunkach udziału w procedurze naboru, pkt. IV.B niniejszego zaproszenia) w dziedzinie bezpieczeństwa ICT i bezpieczeństwa cybernetycznego;
5. aktywne zaangażowanie w opracowywanie projektów dotyczących bezpieczeństwa ICT;
6. wkład w rozwój standardów w zakresie ICT (np. IETF);
7. doświadczenie w pracy jako członek zespołu reagowania na incydenty;
8. doświadczenie w pracy jako członek zespołu ds. bezpieczeństwa łączności;
9. doświadczenie w pracy z systemami bezpieczeństwa ICT do przetwarzania informacji tajnych;

[5]Zob. tabela odniesienia na stronie internetowej Europass: http://europass.cedefop.europa.eu/pl/resources/european-language-levels-cefr

10. biegła znajomość języka angielskiego (nawet jeśli jest to język 1 lub 2) (co najmniej na poziomie C1[6]).
11. publikacje na temat bezpieczeństwa ICT i bezpieczeństwa cybernetycznego, takie jak materiały na konferencje, czasopisma naukowe lub książki.

Uwaga: kandydaci, którzy otrzymają zaproszenie na rozmowę kwalifikacyjną będą zobowiązani przedstawić wszystkie dokumenty potwierdzające. Jeżeli okaże się, że informacje przedstawione przez kandydata są nieprawdziwe, zostanie on wykluczony z procedury selekcji, a jego nazwisko usunięte z bazy danych.

Selekcja na podstawie kwalifikacji przeprowadzana jest **wyłącznie** w oparciu o informacje przedstawione przez kandydata w zakładce „ocena zdolności ” w formularzu zgłoszeniowym i odbywa się w dwóch etapach:

— etap 1: wstępna ocena kwalifikacji odbywa się w oparciu o odpowiedzi (tak/nie) zaznaczone przez kandydata i współczynnik ważności przypisywany poszczególnym pytaniom w skali od 1 do 3, w zależności od znaczenia przypisanego danemu kryterium. Kandydaci, którzy uzyskali najwyższą liczbę punktów zostaną zaproszeni do udziału w drugim etapie selekcji (w każdym profilu, liczba kandydatów zaproszonych do drugiego etapu jest około pięć razy większa niż zapotrzebowanie instytucji);

— etap 2: komisja selekcyjna przeanalizuje odpowiedzi kandydatów i przyzna każdej z nich od 0 do 4 punktów. Liczba punktów zostanie następnie pomnożona przez współczynnik ważności przypisywany danemu kryterium.

Kandydaci, którzy uzyskali najwyższą liczbę punktów zostaną zaproszeni do udziału w teście kompetencji (około dwa i pół raza więcej, według profilu, niż zapotrzebowanie instytucji). W przypadku gdy na ostatnim miejscu uplasuje się kilku kandydatów z jednakowym wynikiem, wszyscy ci kandydaci zostaną zaproszeni do testu kompetencji.

TEST KOMPETENCJI

Kandydaci przystępują do testów kompetencji sprawdzających ich wiedzę w zakresie wybranego profilu.

W przypadku grup funkcyjnych III i IV testy będą takie same, różnić się będzie natomiast wymagana minimalna liczba punktów jak przedstawiono w tabeli poniżej. Za uprzednią zgodą (udzieloną w formularzu zgłoszeniowym) kandydaci na stanowiska w GF IV, którzy nie uzyskali wymaganej minimalnej liczby punktów, zostaną przeklasyfikowani do GF III, pod warunkiem że uzyskali wymaganej minimalnej liczba punktów dla tej grupy. W przypadku wszystkich grup funkcyjnych testu nie przechodzą kandydaci, którzy nie uzyskali wymaganej minimalnej liczby punktów.

Rodzaj testu	**Czas trwania testu**	**Język testu**	**Maksymalna liczba punktów**	**Minimalna wymagana liczba punktów**	
				GF III	GF IV
Wielokrotnego wyboru	50 minut	Drugi język (L2)	25	13	16

Testy zostaną przeprowadzone na papierze i zorganizowane dla wszystkich kandydatów w Brukseli albo z wykorzystaniem komputera w ośrodkach egzaminacyjnych w państwach członkowskich Unii Europejskiej. Kandydaci zostaną powiadomieni w odpowiednim czasie o wybranym sposobie organizacji.

W przypadku gdy testy będą przeprowadzane w formie papierowej i będą odbywać się dla wszystkich kandydatów w Brukseli, EPSO przewiduje zwrot kosztów podróży zgodnie z odpowiednimi przepisami w sprawie zwrotu kosztów, które można znaleźć na stronie internetowej EPSO pod adresem http://europa.eu/epso/apply/on_going_compet/reimburse/index_en.htm.

[6]Zob. tabela odniesienia na stronie internetowej Europass: http://europass.cedefop.europa.eu/pl/resources/european-language-levels-cefr

VII. WYNIKI TESTU

Wyniki przeglądu CV kandydatów i testu kompetencji zostaną opublikowane w kontach EPSO kandydatów.

VIII. WPISANIE DO BAZY DANYCH

Nazwiska kandydatów, którzy osiągnęli wymaganą minimalną liczbę punktów w teście umiejętności, zostaną wpisane do bazy danych. Nie będą one podawane do wiadomości publicznej w żadnej innej formie. Baza danych zostanie udostępniona Komisji Europejskiej, Parlamentowi Europejskiemu, Sekretariatowi Generalnemu Rady, Europejskiej Służbie Działań Zewnętrznych i Komitetowi Ekonomiczno-Społecznemu. W razie zapotrzebowania na przedmiotowe profile inne instytucje i agencje europejskie mogą również uzyskać do niej dostęp. Baza danych będzie zachowa aktualność przez okres trzech lat od daty poinformowania kandydatów o ich wynikach.

Komisja Europejska rozpoczęła negocjacje w sprawie zmiany Regulaminu pracowniczego urzędników Unii Europejskiej i warunków zatrudnienia innych pracowników Unii Europejskiej. Zmiana może dotyczyć kariery urzędników i innych pracowników. Kandydaci, których nazwiska znajdują się w bazie danych utworzonej w ramach niniejszej procedury selekcji, mogą otrzymać propozycję pracy na podstawie nowych przepisów regulaminu pracowniczego, jeżeli zostały one przyjęte przez ustawodawcę, bez uszczerbku dla innych kwestii natury prawnej lub finansowej.

IX. SELEKCJA DOTYCZĄCA POTENCJALNEGO ZATRUDNIENIA

Umieszczenie nazwiska w bazie danych nie stanowi gwarancji otrzymania oferty pracy. W przypadku wakatów instytucje będą przeszukiwać bazę danych i zapraszać na rozmowę kwalifikacyjną kandydatów, którzy najlepiej spełniają wymagania oferowanego stanowiska. W zależności od wyniku rozmowy kandydat może otrzymać oficjalną ofertę pracy. W trakcie rozmowy oceniany będzie także poziom znajomości języka podstawowego. Jeżeli kandydat nie posiada jeszcze poświadczenia bezpieczeństwa osobowego (PBO), zobowiązuje się wystąpić o nie bezpośrednio po rekrutacji. Wybranemu kandydatowi zaoferowana zostanie umowa CA 3A[7] lub CA 3B[8] , w zależności od organu zatrudniającego składającego ofertę pracy, jak wskazano poniżej.

Umowa	Miejsce działalności
CA 3B (na czas określony)	Dyrekcje generalne Komisji (z wyjątkiem biur), Parlament Europejski, Sekretariat Generalny Rady, Europejska Służba Działań Zewnętrznych (z wyjątkiem delegatur UE) i Komitet Ekonomiczno-Społeczny, Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz Urząd Publikacji Unii Europejskiej (OP)
CA 3A (może prowadzić do umowy o pracę na czas nieokreślony)	Komisja: oba Urzędy Infrastruktury i Logistyki w Brukseli i Luksemburgu, Urząd Administracji i Wypłacania Należności Indywidualnych (PMO); Europejski Urząd Doboru Kadr (EPSO) oraz Europejska Szkoła Administracji (EUSA), agencje Unii Europejskiej oraz reprezentacje Komisji Europejskiej i delegatury Unii Europejskiej na świecie.

[7] Na mocy art. 3a warunków zatrudnienia innych pracowników Unii Europejskiej i na warunkach określonych w warunkach zatrudnienia innych pracowników Unii Europejskiej oraz ogólnych przepisów wykonawczych instytucji, urzędu lub agencji.

[8] Na mocy art. 3b warunków zatrudnienia innych pracowników Unii Europejskiej i na warunkach określonych w warunkach zatrudnienia innych pracowników Unii Europejskiej oraz ogólnych przepisów wykonawczych instytucji, urzędu lub agencji.

X. PROCEDURA PRZEGLĄDU I SKŁADANIA ODWOŁAŃ

X. 1. ODWOŁANIA

Jeżeli na jakimkolwiek etapie procedury selekcji uważają Państwo, że popełniono błąd lub że EPSO nie działało w sposób sprawiedliwy lub nie przestrzegało zasad regulujących procedurę selekcji oraz że w rezultacie naruszono Państwa interesy, można skorzystać z następujących procedur odwoławczych, w kolejności podanej w poniższej tabeli:

Procedura	**Punkt kontaktowy**	**Termin[9]**
1. Wniosek o dokonanie przeglądu	Za pośrednictwem formularza kontaktowego na stronie internetowej EPSO	10 dni kalendarzowych
2. Zażalenie na mocy art. 90 ust. 2 Regulaminu pracowniczego urzędników Unii Europejskiej[10]	Pocztą na następujący adres Europejskiego Urzędu Doboru Kadr: Office européen de sélection du personnel (EPSO) C-25, 1049 Bruxelles, Belgia lub za pośrednictwem formularza kontaktowego na stronie internetowej EPSO.	3 miesiące
Po zrealizowaniu pkt 2 (punkt pierwszy jest fakultatywny) kandydat może:		
3. Jeśli Państwa zażalenie zostanie odrzucone wyraźnie lub poprzez brak odpowiedzi, mogą Państwo złożyć skargę sądową na mocy art. 270 Traktatu o funkcjonowaniu Unii Europejskiej oraz art. 91 regulaminu pracowniczego[11]	European Union Civil Service Tribunal Boulevard Konrad Adenauer L-2925 Luksemburg	3 miesiące

Podobnie jak wszyscy obywatele Unii Europejskiej każdy kandydat może złożyć skargę do Europejskiego Rzecznika Praw Obywatelskich

European Ombudsman
1 avenue du Président Robert Schuman —
CS 30403
67001 Strasbourg Cedex
FRANCJA[12]

X.2. WNIOSKI O PODJĘCIE ŚRODKÓW NAPRAWCZYCH

Jeśli uważają Państwo, że co najmniej jedno pytanie zadane w testach zawierało błąd, który uniemożliwiał udzielenie odpowiedzi lub wpływał możliwość udzielenia prawidłowej odpowiedzi, mają

[9]Od daty publikacji decyzji na koncie EPSO kandydata.

[10]W temacie pisma należy podać następujące informacje: numer procedury selekcji; numer Państwa zgłoszenia i dopisek „skarga na podstawie art. 90 ust. 2".

[11]Szczegółowe informacje o zasadach wnoszenia odwołań i obliczania terminów można znaleźć na stronie Sądu do spraw Służby Publicznej Unii Europejskiej na stronie: http://curia.europa.eu/jcms/jcms/T5_5230.

[12] Należy zwrócić uwagę, że wniesienie skargi do rzecznika nie przerywa biegu terminu przewidzianego w art. 90 ust. 2 i art. 91 regulaminu pracowniczego na wniesienie zażalenia lub odwołania do Sądu do spraw Służby Publicznej na podstawie art. 270 Traktatu o funkcjonowaniu Unii Europejskiej. Należy również zauważyć, że zgodnie z art. 2 ust. 4 warunków ogólnych regulujących wykonywanie funkcji Rzecznika Praw Obywatelskich, każda skarga złożona do Rzecznika musi być poprzedzona odpowiednimi działaniami administracyjnymi wobec instytucji i organów, których dotyczy. Szczegółowe informacje na temat tej procedury dostępne są na stronie internetowej: Http://www.ombudsman.europa.eu/pl/home.

Państwo prawo poinformować o tym EPSO, które, po weryfikacji, podejmie ewentualne działania naprawcze.

Wniosek o podjęcie środków naprawczych musi zostać złożony w **ciągu 10 dni kalendarzowych od dnia odbycia się testu** za pośrednictwem funkcyjnej skrzynki pocztowej EPSO-CAST-S-7-2013@ec.europa.eu.

We wniosku **należy** podać swój numer kandydata oraz informacje umożliwiające zidentyfikowanie pytania(pytań), który (które) Państwa zdaniem zawierało błędy (np. wskazując, czego dotyczyło lub podając numer pytania) oraz wyjaśnić w miarę możliwości jak najdokładniej, na czym polegał rzekomy błąd.

Wnioski złożone po terminie lub niezawierające informacji, które umożliwiałyby zidentyfikowanie zakwestionowanych pytań, nie będą brane pod uwagę.

XI. PRZEKAZYWANIE INFORMACJI

EPSO skontaktuje się z kandydatami za pośrednictwem ich kont EPSO. Kandydaci powinni śledzić przebieg procedury i kontrolować informacje ich dotyczące, sprawdzając swoje konto EPSO regularnie, co najmniej 2 razy w tygodniu. Jeśli kandydat nie może tego uczynić z powodu problemów technicznych, które można przypisać EPSO, należy niezwłocznie powiadomić o tym EPSO.

Wszelka korespondencja z Epso powinna być prowadzona przy wykorzystaniu formularza kontaktowego na stronie internetowej EPSO: http://blogs.ec.europa.eu/eu-careers.info/cast/.

Aby informacje o charakterze ogólnym oraz komunikaty do kandydatów lub informacje otrzymywane od kandydatów były jasne i zrozumiałe dla obu stron, przekazywane są one wyłącznie w języku angielskim, francuskim lub niemieckim. To samo dotyczy zaproszeń na poszczególne testy i egzaminy, jak również całej korespondencji pomiędzy EPSO a kandydatami.

XII. POWODY WYKLUCZENIA Z PROCEDURY NABORU ZWIĄZANE Z PROCESEM DOKONYWANIA ZGŁOSZEŃ

EPSO czuwa nad przestrzeganiem zasady równego traktowania. W konsekwencji, jeśli na jakimkolwiek etapie procedury EPSO stwierdzi, że kandydat stworzył więcej niż jedno konto EPSO, dokonał więcej niż jednego zgłoszenia w ramach niniejszej procedury lub złożył niezgodne z prawdą oświadczenia, kandydat zostanie wykluczony.

Każde oszustwo lub próba oszustwa będą podlegały sankcjom. W związku z powyższym zwraca się uwagę na fakt, że w instytucjach zatrudniane są jedynie osoby wykazujące się najwyższą uczciwością.

XIII. SZCZEGÓLNE USTALENIA DLA KANDYDATÓW NIEPEŁNOSPRAWNYCH

a) problemy zdrowotne występujące w momencie dokonywania zgłoszenia

1.	Osoby niepełnosprawne lub z problemami zdrowotnymi, mogącymi stwarzać trudności podczas egzaminów, powinny zaznaczyć odpowiednie pole w swoim internetowym formularzu zgłoszeniowym i wskazać środki, które ich zdaniem należy podjąć, aby ułatwić im udział w poszczególnych testach i egzaminach; należy przy tym koniecznie podać numer procedury selekcji oraz numer zgłoszenia kandydata.
2.	Prosimy o przesłanie, jak najszybciej po dokonaniu zgłoszenia internetowego, zaświadczenia lekarskiego lub – w stosownym przypadku – zaświadczenia właściwego organu o niepełnosprawności. Stosowne dokumenty zostaną sprawdzone i podjęte zostaną szczególne środki, stosownie do każdego przypadku, w celu spełnienia – w miarę możliwości – wymagań

	uznanych za uzasadnione. Wnioski i stosowne dokumenty należy przesyłać: pocztą elektroniczną na adres: EPSO-accessibility@ec.europa.eu, lub faksem na nr:+ 32 22998081 z dopiskiem „EPSO accessibility”, lub zwykłą pocztą na adres: European Personnel Selection Office (EPSO) 'EPSO accessibility' (C-25) 1049 Bruxelles/Brussel BELGIA

b) problemy zdrowotne, które wystąpiły po dokonaniu zgłoszenia

1.	Jeśli opisane wyżej problemy zdrowotne wystąpiły po upływie terminu dokonywania zgłoszeń internetowych, należy jak najszybciej poinformować o tym EPSO. Kandydaci powinni wskazać na piśmie, jakie środki uznają oni za niezbędne.
2.	Należy przesłać stosowne dokumenty: pocztą elektroniczną na adres: EPSO-accessibility@ec.europa.eu lub faksem na nr:+ 32 22998081 z dopiskiem „EPSO accessibility”, lub zwykłą pocztą na adres: European Personnel Selection Office (EPSO) 'EPSO accessibility' (C-25) 1049 Bruxelles/Brussel BELGIA