

ПОКАНА ЗА ИЗРАЗЯВАНЕ НА ИНТЕРЕС ЗА ДОГОВОРНО НАЕТ ПЕРСОНАЛ

В ОБЛАСТТА НА СИГУРНОСТТА НА ИКТ

Функционална група III: Асистент по сигурността на ИКТ
Функционална група IV: Анализатор на сигурността на ИКТ

EPSO/CAST/S/7/2013

I. ВЪВЕДЕНИЕ

По искане на институциите на Европейския съюз Европейската служба за подбор на персонал (EPSO) започва процедура за подбор на служители с цел съставяне на база данни с имената на успешно преминалите процедурата кандидати, от която да бъде набран договорно нает персонал **в областта на сигурността на ИКТ и киберсигурността.**

Институциите на Европейския съюз набират договорно нает персонал с цел осигуряване на допълнителен капацитет в специализирани области. Договорно наетият персонал се назначава в съответствие с условията, посочени в раздел IX от настоящата покана за изразяване на интерес.

Трудовите правоотношения с европейските институции са уредени в Условията за работа на другите служители на Съюза. Условията на работа са посочени подробно онлайн на следния адрес: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20100101:bg:PDF> (глава 4, стр. 179)¹.

Базата данни ще бъде използвана от Европейската комисия, Европейския парламент, Генералния секретариат на Съвета на Европейския съюз, Европейската служба за външна дейност и Икономическия и социален комитет. **В зависимост от потребностите местоработата на длъжностите ще бъде основно в Брюксел и Люксембург. Ограничен брой работни места могат да бъдат разположени в някои от делегациите на ЕС по света.**

Процедурите за подбор на договорно нает персонал обикновено привличат голям брой високо квалифицирани кандидати, които преминават успешно съответната процедура за подбор. Поради това кандидатите следва да имат предвид, че за някои профили е възможно броят на имената в базата данни да надхвърля нуждите на институциите.

Таблицата по-долу показва прогнозните нужди на институциите за договорно нает персонал в тази област за определен период от време, като се вземат предвид спрочният характер на договорите и ротацията на служителите.

В резерва, който ще е необходим на институциите за тригодишния период 2014—2016 г., ще бъде включен следният приблизителен брой кандидати, успешно преминали процедурата:

Функционална група	Профил	Брой
ФГ III	Асистент по сигурността на ИКТ	50
ФГ IV	Анализатор на сигурността на ИКТ	50

¹ Общите разпоредби за изпълнение, които уреждат условията на работа на договорно наетия персонал, назначен от Комисията и Европейския парламент, могат да бъдат намерени на уебсайта на EPSO.

Желаещите могат да кандидатстват само за един профил и една функционална група. Кандидатите за функционална група IV (ФГ IV) могат обаче да бъдат прехвърлени в класацията за функционална група III (ФГ III), при условие че са дали предварителното си съгласие за това, ако не постигнат необходимия минимален резултат за ФГ IV от тестовете за компетенции, но са постигнали минималния резултат за ФГ III (за повече подробности вж. „VI. ЕТАПИ НА ПОДБОРА“). Кандидатите с повече от една подадена кандидатура ще бъдат изключени от участие.

II. ЕСТЕСТВО НА СЛУЖЕБНИТЕ ЗАДЪЛЖЕНИЯ²

ФГ III — Асистент по сигурността на ИКТ

Под ръководството на длъжностно лице или срочно нает служител договорно наетият служител ще съдейства за изготвянето и изпращането на съобщения, координирането на предупреждения и реагиране на инциденти, извършването на криминалогични разследвания и одити на сигурността на ИКТ, управлението на инфраструктурата за сигурност на ИКТ, определянето на параметрите на конфигурацията на сигурността на ИКТ, както и изготвянето на политики, стандарти и насоки по отношение на сигурността на ИКТ.

Така например сред служебните задължения могат да бъдат следните:

- съдействие за изпълнението на решения в областта на сигурността (инфраструктура и/или приложен софтуер), включително проектирането, конфигурирането, разработването, изпитването и внедряването на технологии, свързани със сигурността, като например ново поколение защитни стени, защитни стени за приложен софтуер, управление на цифровата самоличност и достъпа, системи за откриване на проникване/системи за предотвратяване на проникване, предотвратяване на загуба на данни, управление на цифрови права, управление на достъпа до мрежата, мониторинг на информацията за сигурността и на събитията, свързани със сигурността (SIEM) и т.н.;
- съдействие за запознаване с информационната сигурност и инициативи за обучение, чрез което работната сила да се образова по отношение на рисковете, свързани с информацията, чрез осигуряване на ориентация, образователни програми и постоянна комуникация;
- съдействие при проектирането, документиранието и изпитването на контрола на процеси в ИКТ при различни условия на околната среда;
- съдействие при одит и проверки по въпроси, свързани с информационната сигурност, в институциите на ЕС;
- съдействие при оказването на подкрепа на ползвателите или службите при запитвания, свързани със сигурността; съставяне на насоки и помощна документация относно модернизирането на мерките за защита;
- съдействие за прилагането, управлението и следенето на спазването на политики, насоки и процедури по отношение на сигурността на ИКТ в рамките на институциите на ЕС;
- изпълнение на функциите на дежурен служител в екип за реагиране на инциденти, който анализира входящата информация за заплахите и системите, чиято сигурност е компрометирана, подрежда информацията по значимост, изготвя съобщения и предупреждения, както и ги изпраща до съответната целева група;
- съдействие при справянето с инциденти, свързани с информационната сигурност, оценяването на входящата информация за инциденти и предприемането на съответни действия;
- съдействие при криминалогични разследвания, свързани със сигурността на ИКТ, и/или извършването на събиране и анализ на артефакти;
- съдействие при разследването на случаи на зловредни кодове, за да се определят векторът на атаката, натоварването и размерът на щетите и извлечените данни;
- съдействие за изпълнението на решения в областта на сигурността по отношение на събирането на сведения за злонамерена дейност, както и на събирането, обработването и обмена на сведения за предполагаема злонамерена дейност;

² Описаните в настоящата покана за изразяване на интерес профили представляват опростени варианти на общите профили, които ще бъдат ползвани за съставяне на договорите. Тези опростени варианти се предоставят само за информация и нямат задължителна юридическа сила.

- съдействие при разследването на предполагаеми и действителни пробиви в сигурността и съответно при предприемането/докладването на действия за отстраняване на пропуските; водене на дневник за всички инциденти и препоръки и действия за отстраняване на пропуските;
- внедряване, конфигуриране, управление и поддръжка на криптографски системи;
- внедряване, конфигуриране, управление и поддръжка на класифицирана инфраструктура/мрежи;
- прилагане/следене на спазването или одит на политиките по отношение на сигурността на ИКТ.

ФГ IV — Анализатор на сигурността на ИКТ

Под ръководството на длъжностно лице или срочно нает служител договорно наетият служител ще се занимава с концептуална работа, анализ и технически и административен контрол в областта на поддръжката и инфраструктурата на ИКТ.

Договорно наетият служител ще изпълнява задачи, свързани с управлението на съобщения, координирането на предупреждения и реагиране на инциденти, извършването на криминологични разследвания, одити на сигурността на ИКТ, управлението на инфраструктурата за сигурност на ИКТ, определянето на параметрите на конфигурацията на сигурността на ИКТ, както и изготвянето на политики, стандарти и насоки по отношение на сигурността на ИКТ. Наред с друго за изпълнението на горните задължения се изискват способности за съставяне на документи, анализ, технически контрол и административно управление, както и задълбочени работни познания по офисен софтуер.

Така например сред служебните задължения могат да бъдат следните:

- управление, координиране и изпълнение на решения в областта на сигурността (инфраструктура и/или приложен софтуер), включително проектирането, конфигурирането, разработването, изпитването и внедряването на технологии, свързани със сигурността, като например ново поколение защитни стени, защитни стени за приложен софтуер, управление на цифровата самоличност и достъпа, системи за откриване на проникване/системи за предотвратяване на проникване, предотвратяване на загуба на данни, управление на цифрови права, управление на достъпа до мрежата, мониторинг на информацията за сигурността и на събитията, свързани със сигурността (SIEM) и т.н.;
- инициране на мерки за запознаване с информационната сигурност и инициативи за обучение, чрез което работната сила да се образова по отношение на рисковете, свързани с информацията, чрез осигуряване на ориентация, образователни програми и постоянна комуникация; проектиране, документиране и изпитване на контрола на процеси в ИКТ при различни условия на околната среда;
- управление на проекти в областта на сигурността на ИКТ, включително планиране на проекти, оценка на продукти, избор на система/доставчик, проектиране на инфраструктура, оценки на готовността и гарантиране на качеството;
- управление и координиране на одити и проверки по въпроси, свързани с информационната сигурност, в институциите на ЕС;
- организиране и координиране на мерките за реагиране на инциденти, свързани с информационната сигурност;
- ръководство на екип за реагиране на инциденти с цел ограничаване, разследване и предотвратяване на бъдещи пробиви в компютърната сигурността;
- разработване, прилагане и следене на спазването на подходящи и съответни политики по отношение на информационна сигурност, като се гарантира, че те са в съответствие с Директивата на ЕС за защита на данните и с останалото законодателство и нормативни актове, свързани с информационната сигурност; редовен преглед на политиките;
- гарантиране на включването на информационната сигурност в работните стратегии и изисквания;
- координиране на криминологични разследвания, свързани със сигурността на ИКТ, и/или извършването на събиране и анализ на артефакти;
- разследване на случаи на зловредни кодове, за да се определят векторът на атаката, натоварването и размерът на щетите и неправомерно извлечените данни;
- управление, координиране и изпълнение на решения в областта на сигурността по отношение на събирането на сведения за злонамерена дейност, както и на събирането, управлението и обмяна на сведения за предполагаема злонамерена дейност;

- провеждане на проучвания в областта на сигурността с цел осведоменост по отношение на най-новите проблеми;
- работа с доставчици, външни консултанти и други трети страни с цел подобряване на информационната сигурност в рамките на институциите на ЕС;
- управление на включването на системи за информационна сигурност в работната среда;
- анализ, оценка и подобряване на инструментите, процесите и работните процедури и методи на ИКТ във връзка със сигурността на ИКТ;
- проектиране, внедряване, конфигуриране, управление и поддръжка на криптографски системи;
- проектиране, внедряване, конфигуриране, управление и поддръжка на класифицирана инфраструктура/мрежи.
- предлагане, прилагане/следене на спазването и/или одит на политиките по отношение на сигурността на ИКТ.

III. ПРИМЕРЕН ГРАФИК НА ПРОЦЕДУРАТА ЗА ПОДБОР

Процедурата ще бъде ръководена от EPSO с помощта на комисия за подбор, състояща се от представители на отдели в институциите на ЕС. **Примерният** график е следният:

	Примерни дати
ЕТАП	
Пресяване на автобиографии	септември 2013 г.
Тест за компетенции	ноември 2013 г.
Резултати от теста за компетенции	декември 2013 г. — януари 2014 г.

IV. УСЛОВИЯ ЗА ДОПУСКАНЕ

Към датата, на която изтича крайният срок за електронна регистрация, трябва да отговаряте на следните условия:

А. Общи условия	
а) да сте гражданин на една от държавите — членки на Европейския съюз, в датата, на която изтича крайният срок за електронна регистрация;	
б) да се ползвате с пълния обем граждански права;	
в) да сте изпълнили задълженията, наложени от законите по отношение на военната служба;	
г) да притежавате необходимите нравствени качества за изпълнение на служебните задължения.	
Б. Минимални специални условия — образование/опит	
ФГ III — Асистент по сигурността на ИКТ	
<ul style="list-style-type: none"> • Образование (удостоверено с диплома), придобито след завършване на средното образование, в техническа област, свързана с описаните в раздел II служебни задължения, или • Завършено средно образование (удостоверено с диплома), даващо достъп до висше образование и последвано от 3 години професионален опит, свързан с описаните в раздел II служебни задължения. 	
ФГ IV — Анализатор на сигурността на ИКТ	
Пълен цикъл университетско обучение с продължителност най-малко 3 години, удостоверено с диплома, в област, свързана с описаните в раздел II служебни задължения.	
В. Езикови познания	
а) език 1 (L1)	Основен език: свободно владее на един от официалните езици на Европейския съюз ³ .
б) език 2 (L2)	<p>Задоволителни познания (на равнище B2⁴) по английски, немски или френски език; задължително различен от език 1 по-горе.</p> <p>Съгласно решението на Съда на Европейския съюз (голям състав) по дело C-566/10 P — Италианска република срещу Европейската комисия, институциите на ЕС трябва да посочат мотивите за ограничаване на избора на втория език в настоящата процедура за подбор до ограничен брой официални езици на ЕС.</p> <p>По тази причина кандидатите се уведомяват, че възможностите за втория език в настоящата процедура за подбор са определени в съответствие с интереса на службата, който изисква новоназначените колеги веднага да бъдат оперативни и в състояние да общуват ефикасно в ежедневната си работа. В противен случай ефективното функциониране на институциите би било сериозно нарушено.</p> <p>Въз основа на дългогодишната практика в институциите на ЕС по отношение на езиците, които се използват за вътрешна комуникация, и като се имат предвид нуждите на службите с оглед на външната комуникация и</p>

³ Официалните езици на Европейския съюз са следните: BG (български), HR (хърватски), CS (чешки), DA (датски), DE (немски), EL (гръцки), EN (английски), ES (испански), ET (естонски), FI (фински), FR (френски), GA (ирландски), HU (унгарски), IT (италиански), LT (литовски), LV (латвийски), MT (малтийски), NL (нидерландски), PL (полски), PT (португалски), RO (румънски), SK (словашки), SL (словенски) и SV (шведски).

⁴ Вж. матрицата за самооценка на уебсайта на Europass: <http://europass.cedefop.europa.eu/bg/resources/european-language-levels-cefr>

	<p>обработването на преписките, най-широко използвани езици остават английският, немският и френският. Освен това английският, немският и френският език определено са най-предпочитаните втори езици на кандидатите в процедурите за подбор, в които те имат право на свободен избор. Това потвърждава съществуващите образователни и професионални стандарти, според които се приема, че кандидатите за длъжности в службите на Европейския съюз владеят поне един от тези езици. Ето защо, като се съпостави интересът на службата с нуждите и способностите на кандидатите и като се вземе под внимание конкретната област, за която се обявява настоящата процедура за подбор, основателно е да се организират тестове на тези три езика, за да се гарантира, че независимо от първия си официален език всички кандидати владеят поне един от тези три официални езика на работно равнище. Освен това, в интерес на равното третиране на всички кандидати, всички, включително тези, чийто първи официален език е един от посочените три, са длъжни да положат теста на своя <u>втори</u> език, избран измежду въпросните три. Оценяването на специфичните компетенции по този начин позволява на институциите да преценят способността на кандидатите да работят незабавно в среда, сходна с тази, в която ще работят. Това не им пречи по-нататък да се запишат на езиково обучение, за да придобият способност за работа с трети език в съответствие с член 85, параграф 3 от Условието за работа на другите служители.</p>
--	---

Можете да регистрирате само един от 24-те официални езика като Ваш основен език (L1). След като валидирате своя електронен формуляр за кандидатстване, няма да можете да промените езиците, които сте избрали.

Бележка: Ако получите покана за явяване на интервю, ще трябва да представите всички удостоверителни документи. Ако бъде установено, че предоставените данни са неверни, ще бъдете изключен от процедурата за подбор и името Ви ще бъде заличено от базата данни.

V. НАЧИН И КРАЕН СРОК ЗА ПОДАВАНЕ НА КАНДИДАТУРАТА

Трябва да подадете кандидатурата си по електронен път, като следвате инструкциите на уебсайта на EPSO (http://europa.eu/epso/apply/jobs/index_en.htm), и по-специално в наръчника за кандидатстване. Трябва да попълните формуляра за кандидатстване на английски, френски или немски език.

Необходимо е да вземете всички мерки за приключване на електронната регистрация в обявения срок. Съветваме Ви да не чакате последните дни, за да се регистрирате, тъй като поради претоварване на линиите или проблем с интернет връзката може да се наложи да повторите електронната регистрация, което няма да бъде възможно след изтичане на срока.

След като валидирате регистрацията си, в нея повече няма да могат да бъдат правени промени, а данните от нея незабавно ще бъдат обработени от EPSO за целите на процедурата за подбор.

**КРАЕН СРОК (включително за валидиране на кандидатурата)
16/07/2013 г. в 12 ч. (на обяд), брюкселско време**

VI. ЕТАПИ НА ПОДБОРА

ПОДБОР ПО КВАЛИФИКАЦИИ

Прави се отсяване на кандидатите въз основа на техните квалификации, особено въз основа на техните дипломи и професионален опит, с помощта на посочените по-долу критерии и онези кандидати, чиито профили съответстват в най-голяма степен на служебните задължения и на критериите за подбор, получават покана да се явят на тест за компетенции.

С цел подпомагане на EPSO на този етап от процедурата за подбор ще бъде назначена комисия за подбор, която да извърши по-специално подбора по квалификации (пресяване на автобиографии).

Критерии за подбор по квалификации

ФГ III — Асистент по сигурността на ИКТ

1. Най-малко 3 години професионален опит в областта на сигурността на ИКТ или киберсигурността след получаването на диплома за образование, придобито след завършване на средното образование.
2. Ако имате само диплома за средно образование, последвано от 3 години опит, свързан със служебните задължения, необходими са още най-малко 3 години допълнителен професионален опит в областта на сигурността на ИКТ или киберсигурността.
3. Независимо от вида на придобитата диплома, като част от Вашия професионален опит съгласно точки 1 и 2 по-горе са необходими най-малко 6 месеца опит, конкретно свързан със служебните задължения, описани в раздел II „Естество на служебните задължения“ на настоящата покана.
4. Сертификат за сигурност на ИКТ или киберсигурност, като например CISSP, GIAC и др.
5. Обучение (различно от посоченото в условията за допускане в раздел IV. Б от поканата) в областта на сигурността на ИКТ и киберсигурността.
6. Активно участие в разработването на проекти за сигурност на ИКТ.
7. Принос към разработването на стандарти за ИКТ (напр. IETF).
8. Работен опит като член на екип за реагиране на инциденти.
9. Работен опит като член на екип за защитени комуникации.
10. Опит от работа с класифицирани системи за сигурност на ИКТ.
11. Добри познания по английски език (дори като език 1 или език 2) (най-малко ниво B2⁵).

ФГ IV — Анализатор на сигурността на ИКТ

1. Най-малко 5 години професионален опит в областта на сигурността на ИКТ или киберсигурността след придобиването на степен на висше образование.
2. Като част от Вашия професионален опит съгласно точка 1 са необходими най-малко 6 месеца опит, конкретно свързан със служебните задължения, описани в раздел II „Естество на служебните задължения“ на настоящата покана.
3. Сертификат за сигурност на ИКТ или киберсигурност, като например CISSP, GIAC и др.
4. Обучение (Обучение (различно от посоченото в условията за допускане в раздел IV. Б от поканата) в областта на сигурността на ИКТ и киберсигурността.
5. Активно участие в разработването на проекти за сигурност на ИКТ.
6. Принос към разработването на стандарти за ИКТ (напр. IETF).
7. Работен опит като член на екип за реагиране на инциденти.
8. Работен опит като член на екип за защитени комуникации.
9. Опит от работа с класифицирани системи за сигурност на ИКТ.
10. Задълбочени познания по английски език (дори като език 1 или език 2) (най-малко ниво C1⁶).
11. Публикации във връзка със сигурността на ИКТ или киберсигурността, т.е. материали от конференции, научни списания или книги.

⁵ Вж. матрицата за самооценка на уебсайта на Europass: <http://europass.cedefop.europa.eu/bg/resources/european-language-levels-cefr>

⁶ Вж. матрицата за самооценка на уебсайта на Europass: <http://europass.cedefop.europa.eu/bg/resources/european-language-levels-cefr>

Бележка: Ако получите покана за явяване на интервю, ще трябва да представите всички удостоверителни документи. Ако бъде установено, че предоставените данни са неверни, ще бъдете изключен от процедурата за подбор и името Ви ще бъде заличено от базата данни.

Подборът по квалификации се извършва **единствено** въз основа на информацията, предоставена от кандидата в графа „Допълнителни квалификации“ (Talent Screener) във формуляра за кандидатстване, и протича на два етапа:

- Етап 1: Началният етап на подбора по квалификации се извършва единствено въз основа на отбелязаните от кандидата отговори (да/не) и въз основа на коефициента на тежест, определен за всеки въпрос, който варира от 1 до 3 в зависимост от значимостта на съответния критерий. Получилите най-много точки кандидати се допускат до втория етап на подбора (за всеки профил около пет пъти броя на кандидатите, необходими на институциите);
- Етап 2: Комисията за подбор разглежда отговорите на кандидатите и дава за всеки отговор оценка от 0 до 4, като тази оценка се умножава по коефициента на тежест, определен за съответния критерий.

Получилите най-много точки кандидати ще бъдат поканени да се явят на тест за компетенции (за всеки профил около два и половина пъти броя на кандидатите, необходими на институциите). Ако за последното място има няколко кандидати с еднакъв резултат, всички тези кандидати ще бъдат поканени на теста за компетенции.

ТЕСТ ЗА КОМПЕТЕНЦИИ

Кандидатите ще се явят на тест за компетенции, чрез който ще бъдат оценени техните познания, свързани с избора от тях профил.

Кандидатите за функционални групи III и IV се явяват на един и същи тест, но необходимият минимален резултат е различен за двете групи, както е обяснено в таблицата по-долу. С тяхното предварително съгласие (заявено във формуляра за кандидатстване) кандидатите за ФГ IV, които не са постигнали необходимия минимален резултат, се прехвърлят в класацията за функционална група III, при условие че са постигнали необходимия минимален резултат за функционална група III. Независимо за коя функционална група кандидатстват, кандидатите, които не достигнат съответния минимален резултат, отпадат от по-нататъшно участие.

Вид тест	Продължителност на теста	Език на теста	Максимален брой точки	Необходим минимален резултат	
				ФГ III	ФГ IV
Многовариантен избор	50 минути	Език 2 (L2)	25	13	16

Тестът ще бъде или на хартиен носител и проведен за всички кандидати в Брюксел, или ще бъде тест с помощта на компютър в изпитни центрове във всички държави членки. Кандидатите ще бъдат своевременно информирани относно избраните условия.

Ако тестовете бъдат на хартиен носител и проведени за всички кандидати в Брюксел, EPSO ще плати обезщетение за пътните разходи в съответствие с приложимите правила за възстановяване на разходите, които могат да бъдат намерени на уебсайта на EPSO: http://europa.eu/epso/apply/on_going_compet/reimburse/index_en.htm.

VII. РЕЗУЛТАТИ ОТ ТЕСТОВЕТЕ

Резултатите от пресяването на автобиографии и тестовете за компетенции ще бъдат публикувани в EPSO профилите на кандидатите.

VIII. ВКЛЮЧВАНЕ В БАЗАТА ДАННИ

Имената на кандидатите, които са постигнали необходимия минимален резултат на теста за компетенции, ще бъдат вписани в база данни и няма да бъдат публично оповестени под никаква друга форма. Достъп до базата данни ще бъде предоставен на Европейската комисия, Европейския парламент, Генералния секретариат на Съвета на Европейския съюз, Европейската служба за външна дейност и Икономическия и социален комитет. Други европейски институции/агенции могат също да получат достъп, в случай че имат нужда от служители с тези профили. Срокът на валидност на базата данни е три години, считано от датата, на която кандидатите са уведомени за своите резултати.

Европейската комисия започна преговори във връзка с изменението на Правилника за длъжностните лица на Европейския съюз и Условието за работа на другите служители на Европейския съюз. Предмет на това изменение могат да бъдат кариерите на длъжностните лица и другите служители. Кандидатите, чиито имена са вписани в базата данни по настоящата процедура за подбор, могат да получат предложение за работа в съответствие с новите разпоредби на Правилника за длъжностните лица, след като тези разпоредби бъдат приети от законодателя, и без да се засягат други последици от правно или финансово естество.

IX. ПОДБОР С ОГЛЕД НА ЕВЕНТУАЛНО НАЗНАЧАВАНЕ

Включването в базата данни не гарантира, че ще Ви бъде отправено предложение за работа. При появата на свободни работни места институциите ще направят справка с базата данни и ще поканят на интервю тези кандидати, които отговарят най-пълно на изискванията, свързани с въпросната длъжност. В зависимост от това как е протекло интервюто те могат да направят официално предложение за работа. По време на интервюто ще бъде оценени и познанията Ви по основния език. Кандидатите, които не разполагат с разрешение за достъп на персонала, трябва да са съгласни да подадат официално искане за такова веднага след назначаването си. На кандидата, избран да заеме длъжността, ще бъде предложен договор за договорно нает служител по член 3а⁷ или член 3б⁸ в зависимост от направения предложеието работодател, посочен по-долу.

Договор	Месторабота
Договорно наети служители по член 3б (срочен)	Генералните дирекции на Комисията (с изключение на службите), Европейския парламент, Генералния секретариат на Съвета на Европейския съюз, Европейската служба за външна дейност (с изключение на делегациите на ЕС) и Икономическия и социален комитет; Европейската служба за борба с измамите (OLAF) и Службата за публикации на Европейския съюз (OP).
Договорно наети служители по член 3а (с възможност за последващ безсрочен трудов договор)	Комисията: Службата за инфраструктура и логистика в Брюксел, Службата за инфраструктура и логистика в Люксембург, Службата за управление и плащане по индивидуални права (PMO); Европейската служба за подбор на персонал (EPSO), Европейското училище по администрация (EUSA), европейските агенции, представителствата на Комисията и делегациите на Европейския съюз по света.

X. ПРОЦЕДУРИ ЗА ПРЕРАЗГЛЕЖДАНЕ/ОБЖАЛВАНЕ

⁷ Съгласно член 3а от Условието за работа на другите служители на Европейския съюз (УРДС) и при условията, предвидени в УРДС и общите разпоредби за изпълнение на съответната институция, агенция или служба.

⁸ Съгласно член 3б от Условието за работа на другите служители на Европейския съюз (УРДС) и при условията, предвидени в УРДС и общите разпоредби за изпълнение на съответната институция, агенция или служба.

Х.1. ОБЖАЛВАНЕ

По време на всеки един от етапите на настоящата процедура за подбор, ако считате, че е допусната грешка, че отношението на EPSO е било некоректно или че не са спазени правилата, съгласно които се провежда настоящата процедура за подбор, и поради това интересите Ви са били засегнати, можете да прибегнете до следните процедури за обжалване в реда, посочен в таблицата по-долу:

Процедура	Контакт	Срок ⁹
1. Молба за преразглеждане	Чрез страницата за контакт от уебсайта на EPSO	10 календарни дни
2. Подаване на административна жалба на основание член 90, параграф 2 от Правилника за длъжностните лица на Европейския съюз ¹⁰	По пощата на следния адрес: European Personnel Selection Office (EPSO) C-25, 1049 Brussels, Belgium; или чрез страницата за контакт от уебсайта на EPSO.	3 месеца
След приключване на етап 2 по-горе (етап 1 е по избор) Вие разполагате със следната възможност:		
3. Ако Вашата жалба е била отхвърлена изрично или мълчаливо, можете да подадете жалба до Съда на ЕС на основание член 270 от Договора за функционирането на Европейския съюз и член 91 от Правилника за длъжностните лица ¹¹ .	Tribunal de la fonction publique de l'Union européenne Boulevard Konrad Adenauer 2925 Luxembourg	3 месеца

Както всички граждани на Европейския съюз, така и Вие можете да подадете жалба до Европейския омбудсман:

European Ombudsman
1 avenue du Président Robert Schuman —
CS 30403
67001 Strasbourg Cedex
FRANCE¹²

Х.2. ИСКАНИЯ ЗА КОРИГИРАЩИ МЕРКИ

Ако смятате, че един или повече от въпросите към Вас в тестовете са съдържали грешка, направила невъзможен отговора или засегнала възможността Ви да отговорите правилно, имате право да информирате EPSO, която ще предприеме след проверка евентуални коригиращи мерки.

⁹ Считано от датата на публикуване на решението в EPSO профила на кандидата.

¹⁰ В полето „Относно“ на своето писмо посочете следното: номера на процедурата за подбор, номера на Вашата кандидатура и текста „Complaint under Article 90(2)“ (жалба на основание член 90, параграф 2).

¹¹ За реда и условията за подаване на жалба и за изчисляване на съответните срокове посетете уебсайта на Съда на публичната служба на Европейския съюз: http://curia.europa.eu/jcms/jcms/T5_5230.

¹² Обърнете внимание, че сезирането на омбудсмана не спира срока, предвиден в член 90, параграф 2 и член 91 от Правилника за длъжностните лица, за подаване на административна жалба или за обжалване пред Съда на публичната служба на основание член 270 от Договора за функционирането на Европейския съюз. Имайте предвид също така, че съгласно член 2, параграф 4 от общите условия за изпълнение на функциите на омбудсмана всяка подадена до него жалба трябва да бъде предшествана от подходящи административни постъпки пред съответните институции и органи. Пълните подробности по процедурата са представени на следния уебсайт: <http://www.ombudsman.europa.eu/en/home>.

Искането за коригиращи мерки трябва да бъде направено **в срок от 10 календарни дни от датата на Вашия тест** чрез функционалната пощенска кутия: EPSO-CAST-S-7-2013@ec.europa.eu.

Вашето искане **трябва** да включва номера на кандидатурата Ви и информацията, необходима за идентифициране на въпросите, за които смятате, че са съдържали грешки (например като опишете съдържанието на въпроса и/или посочите неговия номер), като обясните възможно най-ясно естеството на предполагаемата грешка.

Исканията, които са получени след крайния срок или не са достатъчно ясни, за да спомогнат за идентифицирането на обжалваните въпроси, няма да бъдат взети под внимание.

XI. СЪОБЩАВАНЕ НА ИНФОРМАЦИЯ И КОНТАКТИ

EPSO ще се свързва с Вас посредством Вашия EPSO профил. Ваше задължение е да следите хода на процедурата и да проверявате информацията, която Ви засяга, като редовно — поне два пъти седмично — влизате в EPSO профила си. Ако не можете да правите такива справки поради технически проблем, дължащ се на EPSO, трябва да уведомите незабавно EPSO за това.

За да се свържете с EPSO, използвайте публикувания на уебсайта на EPSO формуляр за контакт: <http://blogs.ec.europa.eu/eu-careers.info/cast/>.

За да се гарантира доброто двустранно разбиране на текстовете от общ характер и на информацията, която EPSO дава на кандидатите или получава от тях, поканите за различните тестове и цялата кореспонденция между EPSO и кандидатите се съставят единствено на английски, немски или френски език.

XII. ОСНОВАНИЯ ЗА ИЗКЛЮЧВАНЕ ОТ УЧАСТИЕ, СВЪРЗАНИ С РЕГИСТРАЦИЯТА

EPSO полага особени усилия за спазване на принципа на равно третиране. Поради това, ако по време на който и да е етап на процедурата EPSO установи, че сте създали повече от един EPSO профил, че сте подали повече от една кандидатура по настоящата процедура за подбор или че предоставените от Вас данни са неверни, Вие ще бъдете изключен от участие в процедурата.

При измама или опит за измама могат да Ви бъдат наложени санкции. В това отношение Ви обръщаме внимание на факта, че институциите наемат на работа само лица, доказали своята пълна и безусловна честност.

XIII. СПЕЦИАЛНИ МЕРКИ ПО ОТНОШЕНИЕ НА КАНДИДАТИТЕ С УВРЕЖДЕНИЯ

а) Увреждането е налице към момента на подаване на кандидатурата

1.	Ако имате увреждане или здравословен проблем, което или който може да Ви създаде трудности при провеждането на тестовете, трябва да сложите отметка в съответното квадратче в електронния формуляр за кандидатстване и да посочите мерките, които смятате за необходими, за да се улесни участието Ви в различните тестове, като задължително посочите номера на процедурата за подбор и номера на своята кандидатура.
2.	В зависимост от случая трябва да изпратите възможно най-скоро след валидиране на електронната си регистрация медицинско удостоверение или удостоверение от компетентен орган, с което се признава състоянието на лице с увреждане. След разглеждане на удостоверителните документи могат да бъдат предприети специални мерки в зависимост от всеки отделен случай, за да бъдат удовлетворени в рамките на

	<p>възможното исканията, за които се смята, че са обосновани. Исканията и удостоверителните документи следва да бъдат изпратени: или по електронна поща на следния адрес: EPSO-accessibility@ec.europa.eu; или по факс на следния номер: +32 22998081, като отбележите „EPSO accessibility“; или по пощата на следния адрес: European Personnel Selection Office (EPSO) 'EPSO accessibility' (C-25) 1049 Bruxelles/Brussel BELGIUM</p>
--	---

б) Увреждането е възникнало след подаване на кандидатурата

1.	<p>Ако описаното по-горе увреждане възникне след крайната дата, определена за електронна регистрация, трябва да уведомите за това EPSO в най-кратки срокове. Опишете писмено какви мерки са необходими според Вас.</p>
2.	<p>Изпратете съответните документи: или по електронна поща на следния адрес: EPSO-accessibility@ec.europa.eu; или по факс на следния номер: +32 22998081, като отбележите „EPSO accessibility“; или по пощата на следния адрес: European Personnel Selection Office (EPSO) 'EPSO accessibility' (C-25) 1049 Bruxelles/Brussel BELGIUM</p>