РЕШЕНИЕ (ЕС, Евратом) 2019/1963 НА КОМИСИЯТА

от 17 октомври 2019 година

за определяне на правилата за прилагане по отношение на индустриалната сигурност във връзка с класифицирани договори за обществени поръчки

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 249 от него,

като взе предвид Договора за създаване на Европейската общност за атомна енергия, и по-специално член 106 от него,

като взе предвид Решение (ЕС, Евратом) 2015/443 на Комисията от 13 март 2015 г. относно сигурността в Комисията ([1]),

като взе предвид Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 г. относно правилата за сигурност за защита на класифицираната информация на ЕС ([2]),

като взе предвид Решение (ЕС, Евратом) 2017/46 на Комисията от 10 януари 2017 г. относно сигурността на комуникационните и информационните системи в Европейската комисия ([3]),

след консултация с Експертната група по сигурността на Комисията в съответствие с член 41, параграф 5 от Решение (ЕС, Евратом) 2015/444 на Комисията,

като има предвид, че:

(1) В членове 41, 42, 47 и 48 от Решение (ЕС, Евратом) 2015/444 се предвижда, че в допълнение и подкрепа на глава 6 от посоченото решение следва да се определят по-подробни разпоредби в правила за прилагане по отношение на индустриалната сигурност, уреждащи въпроси, като например участието в процедури за възлагане на поръчка, сключването на класифицирани договори, удостоверенията за сигурност на структура, разрешенията за достъп на служител, посещенията, предаването и пренасянето на класифицирана информация на Европейския съюз (КИЕС).

(2) В Решение (ЕС, Евратом) 2015/444 се посочва, че класифицираните договори следва да се изпълняват в тясно сътрудничество с националния орган по сигурността, определения орган по сигурността или друг компетентен орган на съответните държави членки; държавите членки са се споразумели да гарантират, че всеки субект под тяхна юрисдикция, който може да получава или да генерира класифицирана информация, създадена от Комисията, е преминал подходяща проверка за надеждност и е в състояние да осигури адекватна защита, равностойна на тази, предоставяна от правилата за сигурност на Съвета на Европейския съюз за защита на класифицирана информация на ЕС, носеща съответните грифове за сигурност, предвидени в Споразумението между държавите — членки на Европейския съюз, заседаващи в рамките на Съвета, относно защитата на класифицирана информация, която се обменя в интерес на Европейския съюз (2011/C 202/05) ([4]).

(3) Съветът, Комисията и върховният представител на Съюза по въпросите на външните работи и политиката на сигурност се споразумяха да гарантират максимална съгласуваност в прилагането на правилата за сигурност по отношение на осигуряваната от тях защита на КИЕС, като същевременно се отчитат специфичните им институционални и организационни потребности, в съответствие с декларациите, приложени към протокола от заседанието на Съвета, на което бе прието Решение 2013/488/ЕС на Съвета ([5]) относно правилата за сигурност за защита на класифицирана информация на ЕС.

(4) Ето защо правилата за прилагане на Комисията по отношение на индустриалната сигурност във връзка с класифицирани договори следва също да гарантират максимална съгласуваност и да вземат предвид насоките в областта на индустриалната сигурност, одобрени от Комитета по сигурността на Съвета на 13 декември 2016 г., и членове 7 и 22 от Директива № 2009/81/ЕО на Европейския парламент и на Съвета ([6]).

(5) На 4 май 2016 г. Комисията прие решение ([7]) за оправомощаване на члена на Комисията, който отговаря за въпросите на сигурността, да приеме от името на Комисията и на нейна отговорност правилата за прилагане, предвидени в член 60 от Решение (ЕС, Евратом) 2015/444,

([1]) ОВ, L 72, 17.3.2015 г., стр. 41.
([2]) ОВ L 72, 17.3.2015 г., стр. 53.
([3]) ОВ L 6, 11.1.2017 г., стр. 40.
([4]) ОВ C 202, 8.7.2011 г., стр. 13.
([5]) Решение 2013/488/ЕС на Съвета от 23 септември 2013 година относно правилата за сигурност за защита на класифицирана информация на ЕС (ОВ L 274, 15.10.2013 г., стр. 1).
([6]) Директива 2009/81/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно координирането на процедурите за възлагане на някои поръчки за строителство, доставки и услуги от възлагащи органи или възложители в областта на отбраната и сигурността (ОВ L 216, 20.8.2009 г., стр. 76).
([7]) Решение на Комисията от 4 май 2016 г. относно оправомощаване, свързано със сигурността [C(2016) 2797 final].

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

ГЛАВА 1

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и приложно поле

1. С настоящото решение се определят правилата за прилагане по отношение на индустриалната сигурност във връзка с класифицирани договори за обществени поръчки с цел подкрепа на прилагането на Решение (ЕС, Евратом) 2015/444, и по-специално глава 6 от посоченото решение.

2. В настоящото решение се определят специфичните изисквания за гарантиране на защитата на класифицираната информация на Европейския съюз (КИЕС) от икономически оператори в преддоговорната фаза, по време на целия жизнен цикъл на класифицираните договори, сключени от Европейската комисия, и в договорите за подизпълнение, сключени от избраните от Комисията изпълнители.

3. Настоящото решение се отнася до информация, класифицирана на следните нива:

а) RESTREINT UE/EU RESTRICTED;

б) CONFIDENTIEL UE/EU CONFIDENTIAL;

в) SECRET UE/EU SECRET.

Член 2

Отговорност в рамките на Комисията

(1) Като част от отговорностите, описани във Финансовия регламент ([8]), всеки оправомощен разпоредител с бюджетни кредити на възлагащия орган на Комисията гарантира, че класифицираният договор се позовава на минималните стандарти за индустриална сигурност, установени в глава 6 от Решение (ЕС, Евратом) 2015/444 на Комисията и в настоящите правила за тяхното прилагане, и, когато е уместно, в обявлението за обществена поръчка или поканата за представяне на оферти, както и че тези стандарти се спазват в хода на изпълнението.

2. За тази цел съответният разпоредител с бюджетни кредити се консултира на всички етапи с органа по сигурността на Комисията по въпросите, свързани с елементите на сигурността на класифицирания договор, програма или проект, и уведомява местния служител по сигурността относно сключените договори. Решението относно нивото на класификация за сигурност на определени теми се взема от възложителя и трябва да бъде взето, като се взема надлежно предвид ръководството за класифициране за целите на сигурността.

3. При спазването на изискванията на настоящите правила за прилагане органът по сигурността на Комисията си сътрудничи тясно с националните органи за сигурност (НОС) и определените органи за сигурност (ООС) на съответните държави членки, по-специално по отношение на удостоверенията за сигурност на структура (УСС), разрешенията за достъп на служител (РДС), процедурите при посещение и плановете за пренос.

ГЛАВА 2

РАБОТА С ПОКАНИ ЗА ПРЕДСТАВЯНЕ НА ОФЕРТИ ЗА КЛАСИФИЦИРАНИ ДОГОВОРИ

Член 3

Основни принципи

1. Класифицираните договори се възлагат единствено на икономически оператори, регистрирани в държава членка, или на икономически оператори, регистрирани в трета държава или учредени от международна организация, когато съответната трета държава или международна организация е сключила споразумение за сигурност на информацията с Европейския съюз или има административна договореност с Комисията ([9]).

2. Преди да обяви покана за представяне на оферти за класифициран договор, възложителят определя класификацията за сигурност на информацията, която би могла да се предостави на оферентите. Възложителят определя също така максималната класификация за сигурност на информацията, генерирана при изпълнението на договора, програмата или проекта, или поне очаквания обем и вид на информацията, която ще бъде изготвена или обработена, както и необходимостта от класифицирана комуникационна и информационна система (КИС).

([8]) Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета от 18 юли 2018 г. за финансовите правила, приложими за общия бюджет на Съюза, за изменение на регламенти (ЕС) № 1296/2013, (ЕС) № 1301/2013, (ЕС) № 1303/2013, (ЕС) № 1304/2013, (ЕС) № 1309/2013, (ЕС) № 1316/2013, (ЕС) № 223/2014 и (ЕС) № 283/2014 и на Решение № 541/2014/ЕС и за отмяна на Регламент (ЕС, Евратом) № 966/2012 (ОВ L 193, 30.7.2018 г., стр. 1).

([9]) Списъкът на споразуменията, сключени от ЕС, и на административните договорености, сключени от Европейската комисия, по силата на които класифицирана информация на ЕС може да се обменя с трети държави и международни организации, може да бъде намерен на уебсайта на Комисията.

3. Възложителят гарантира, че в обявленията за поръчки за класифицирани договори се предоставя информация за специалните задължения по отношение на сигурността, свързани с класифицирана информация. В приложение I е даден примерен образец за информацията в обявление за поръчка.

4. Възложителят гарантира, че информацията с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се разкрива на оферентите само след като са подписали споразумение за неразкриване на информация, задължаващо оферентите да работят с КИЕС и да я защитават в съответствие с Решение (ЕС, Евратом) 2015/444 и правилата за неговото прилагане.

5. Всички изпълнители, от които се изисква да работят с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET или да я съхраняват в рамките на своите съоръжения, било то по време на изпълнението на самия класифициран договора, или по време на преддоговорния етап, трябва да притежават УСС на изискваното ниво. По-долу се посочват трите сценария, които могат да възникнат по време на етапа на представяне на оферти за класифициран договор, включващ КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET:

а) липса на достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET по време на етапа на представяне на оферти:

когато обявлението за поръчка или поканата за представяне на оферти се отнася до договор, който ще включва КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, но не изисква оферентът да работи с такава информация на етапа на представяне на офертата, оферент, който не притежава УСС на изискваното равнище, не се изключва от процедурата на оферирane на основание, че не притежава УСС;

б) достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET в помещенията на възложителя по време на етапа на представяне на оферти:

достъп се предоставя на служителите на оферента, които притежават РДС на изискваното ниво и имат „необходимост да се знае“. Преди да се предостави този достъп, възложителят уточнява, посредством органа по сигурността на Комисията, със съответния НОС/ООС дали УСС се изисква на този етап също и съгласно националните законови и подзаконови актове;

в) работа с КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET или нейно съхраняване в помещенията на възложителя по време на етапа на представяне на оферти:

когато в обявлението за поръчка или поканата за представяне на оферти се изисква от оферентите да работят с КИЕС или да я съхраняват в помещенията си, оферентът трябва да притежават УСС на изискваното ниво. При тези обстоятелства възложителят трябва да получи посредством органа по сигурността на Комисията уверение от съответния НОС/ООС, че на оферента е предоставено съответното УСС. Достъп се предоставя на служителите на оферента, които притежават РДС на изискваното ниво и имат „необходимост да се знае“.

6. По принцип УСС не се изисква за достъп до информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED нито на етапа на представяне на оферти, нито за изпълнението на договора. Когато, съгласно посоченото в приложение IV, по силата на своите национални законови и подзаконови актове държавите членки изискват УСС за договори за изпълнение или подизпълнение с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, тези национални изисквания нито налагат допълнителни задължения на другите държави членки, нито изключват оференти, изпълнители или подизпълнители от държавите членки, които нямат такива изисквания относно УСС за достъп до информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, от съответните договори за изпълнение/подизпълнение или процедурата по тяхното възлагане. Тези договори се изпълняват в държавите членки в съответствие с техните национални законови и подзаконови актове.

7. Когато за изпълнението на класифициран договор се изисква УСС, възложителят подава посредством органа по сигурността на Комисията искане до НОС/ООС на изпълнителя, като използва информационен формуляр за удостоверение за сигурност на структура (ИФУСС). В приложение III, допълнение Г е даден образец на ИФУСС ([10]). Класифицираният договор не се възлага, докато НОС/ООС на изпълнителя не потвърди УСС на оферента. Отговор на ИФУСС се предоставя, доколкото е възможно, в срок от десет работни дни от датата на искането.

([10]) Други формуляри, които се използват, могат да се различават по отношение на оформлението си от образеца, предоставен в настоящите правила за прилагане.

Член 4

Възлагане на подизпълнение на класифицирани договори

1. Условията, при които изпълнител, на когото е възложен класифициран договор на Комисията, може да възлага подизпълнение, се определят в поканата за представяне на оферти и в документацията за поръчката. Когато класифицираният договор допуска възлагането на подизпълнение на някои от неговите части, това възлагане на подизпълнение подлежи на предварително писмено съгласие от възложителя. Преди да даде съгласието си, възложителят се консултира с органа по сигурността на Комисията.

2. Класифицираните договори се възлагат за подизпълнение единствено на икономически оператори, регистрирани в държава членка, или на икономически оператори, регистрирани в трета държава или учредени от международна организация, когато тази трета държава или международна организация е сключила споразумение за сигурност на информацията с ЕС или има административна договореност с Комисията ([11]).

ГЛАВА 3

ВЪЗЛАГАНЕ НА КЛАСИФИЦИРАНИ ДОГОВОРИ ОТ СТРАНА НА КОМИСИЯТА

Член 5

Основни принципи

1. При възлагането на класифициран договор възложителят, заедно с органа по сигурността на Комисията, гарантира, че задълженията на изпълнителя по отношение на защитата на КИЕС, предоставена на посочения изпълнител или генерирана при изпълнението на договора, са неразделна част от договора. Специфичните за договора изисквания относно сигурността се оформят като приложение относно аспектите на сигурността (ПАС). Образец на ПАС е даден в приложение III.

2. Преди подписването на класифициран договор възложителят изготвя, след консултация с органа по сигурността на Комисията, ръководство за класифициране за целите на сигурността (РКЦС) във връзка със задачите, които следва да бъдат изпълнени, и информацията, генерирана при изпълнението на договора или на равнището на програмата или проекта, когато това е приложимо. РКЦС трябва да бъде част от ПАС.

3. Специфичните за програмата или проекта изисквания относно сигурността се оформят като инструкции за сигурност на програмата (или проекта) (ИСП). ИСП могат да бъдат изготвени, като се използват разпоредбите на образеца на ПАС, даден в приложение III. ИСП се разработват от службата на Комисията, управляваща програмата или проекта, в тясно сътрудничество с органа по сигурността на Комисията, като се предоставят за становище на Експертната група по сигурността на Комисията. Когато договорът е част от програма или проект със собствени ИСП, ПАС на договора трябва да бъде в опростена форма и да включва препратка към разпоредбите за сигурност, съдържащи се в ИСП на програмата или проекта.

4. Възложителят се счита за създател на класифицираната информация, която е създадена и с която се работи за изпълнението на договора.

5. Посредством органа по сигурността на Комисията възложителят уведомява НОС/ООС на всички изпълнители и подизпълнители относно сключването на класифицирани договори за изпълнение или подизпълнение, както и за всяко удължаване или предсрочно прекратяване на тези договори за изпълнение или подизпълнение. В приложение IV е предоставен списък на изискванията по държави.

6. Договорите, включващи информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, трябва да съдържат клауза относно сигурността на договора, която прави разпоредбите, съдържащи се в приложение III, допълнение Д, задължителни за изпълнителя. Посочените договори включват ПАС, в което се определят като минимум изискванията за работа с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, включително аспектите на гарантираност на сигурността на информацията и специфичните изисквания, които трябва да бъдат изпълнени от изпълнителя по силата на делегираните от възложителя правомощия за акредитирането на работата на КИС на изпълнителя с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

([11]) Списъкът на споразуменията, сключени от ЕС, и на административните договорености, сключени от Европейската комисия, по силата на които класифицирана информация на ЕС може да се обменя с трети държави и международни организации, може да бъде намерен на уебсайта на Комисията.

7. Когато на оферентите или на потенциалните изпълнители се предоставя информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, минималните изисквания, посочени в параграф 6, се включват в офертите или в съответните договорености за неразкриване на информация, сключени на етапа на представянето на оферти.

8. Когато това се изисква от националните законови и подзаконови актове на държавите членки, НОС/ООС гарантират, че изпълнителите или подизпълнителите, които са под тяхна юрисдикция, спазват приложимите разпоредби за сигурност относно защитата на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, и извършват посещения за проверка в съоръженията на изпълнителите, които се намират на тяхна територия. Когато НОС/ООС не е обвързан с такова задължение, възложителят гарантира, че изпълнителят прилага необходимите разпоредби за сигурност, съдържащи се в приложение III.

Член 6

Достъп на служители на изпълнители и подизпълнители до КИЕС

1. В качеството си на възложител службата на Комисията гарантира, че класифицираните договори включват разпоредби, указващи, че на служителите на изпълнител или подизпълнител, които за изпълнението на класифицирания договор или поддоговор се нуждаят от достъп до КИЕС, може да бъде предоставен достъп само ако:

а) е установено, че имат „необходимост да се знае“;

б) са получили от съответния НОС/ООС или друг компетентен орган РДС на необходимото ниво за информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

в) са информирани за приложимите правила по сигурността за защита на КИЕС и са потвърдили, че осъзнават своята отговорност за защитата на такава информация;

2. Ако изпълнител или подизпълнител желае да наеме гражданин на държава извън ЕС на длъжност, изискваща достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, отговорност на изпълнителя или подизпълнителя е да задейства процедурата за проучване за надеждност на това лице в съответствие с националните законови и подзаконови актове, приложими на мястото, където ще бъде предоставен достъп до КИЕС.

ГЛАВА 4

ПОСЕЩЕНИЯ ВЪВ ВРЪЗКА С КЛАСИФИЦИРАНИ ДОГОВОРИ

Член 7

Основни принципи

1. Когато за изпълнението на класифициран договор на Комисията е необходимо изпълнителите и подизпълнителите да получат на взаимна основа достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET в помещенията си, се уреждат посещения, като се поддържа връзка с НОС/ООС или друг съответен компетентен орган по сигурността.

2. Посещенията, посочени в параграф 1, подлежат на следните изисквания:

а) посещението трябва да има официална цел, свързана с класифициран договор, възложен от Комисията;

б) за да има достъп до КИЕС, предоставена или генерирана при изпълнението на класифициран договор, възложен от Комисията, всеки посетител трябва да притежава РДС на необходимото ниво, както и „необходимост да се знае“.

Член 8

Искания за посещения

1. Посещенията на изпълнители в структури на други изпълнители или в помещения на Комисията, които са свързани с достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, се организират съгласно следната процедура:

а) служителят по сигурността на структурата, която изпраща посетителя, попълва всички релевантни части от формуляра за искане за посещение (ИП) и подава искането до НСО/ООС на структурата; образец на формуляра за ИП е даден в приложение III, допълнение B;

б) преди да представи искането за посещение на НСО/ООС на приемащата структура (или на органа по сигурността на Комисията, ако посещението е в помещения на Комисията), е необходимо НСО/ООС на изпращащата структура да потвърди ИП на посетителя;

в) след това служителят по сигурността на изпращащата структура получава от своя НОС/ООС отговора на НОС/ООС на приемащата структура (или органа по сигурността на Комисията), с който се одобрява или отхвърля ИП;

г) ИП се счита за одобрено, ако до пет работни дни преди датата на посещението не бъдат повдигнати възражения.

2. Посещенията на служители на Комисията в структури на изпълнител, които са свързани с достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, се организират съгласно следната процедура:

а) посетителят попълва всички релевантни части от формуляра за ИП и го подава до органа по сигурността на Комисията;

б) преди да представи искането за посещение на НСО/ООС на приемащата структура, органът по сигурността на Комисията потвърждава РДП на посетителя;

в) органът по сигурността на Комисията получава отговор от НСО/ООС на приемащата структура, с който се одобрява или отхвърля ИП;

г) ИП се счита за одобрено, ако до пет работни дни преди датата на посещението не бъдат повдигнати възражения.

3. ИП може да обхваща еднократно посещение или многократни посещения. В случай на многократни посещения ИП може да бъде валидно за срок до една година от поисканата начална дата.

4. Валидността на ИП не може надвишава срока на валидност на РДП на посетителя.

(5) Като общо правило ИП следва да бъде подадено до компетентния орган по сигурността на приемащата структура най-малко 15 работни дни преди датата на посещението.

Член 9

Процедури при посещение

1. Преди да позволи на посетител да има достъп до КИЕС, служителят по сигурността на приемащата структура трябва да спази всички свързани с посещенията процедури и правила за сигурност, определени от НОС/ООС на структурата.

2. При пристигането си в приемащата структура посетителите трябва да докажат своята самоличност, като представят валидна лична карта или паспорт. Тази информация за идентификация трябва да съответства на информацията, предоставена в ИП.

3. Приемащата структура гарантира, че се регистрират всички посетители, включително техните имена, представляваната от тях организация, датата на изтичане на РДП, датата на посещението и имената на посетените лица. Тези регистри се съхраняват за срок от най-малко пет години или за по-дълъг срок, ако това се изисква от националните правила и разпоредби на държавата, в която се намира приемащата структура.

Член 10

Пряко организирани посещения

1. В контекста на конкретни проекти съответните НОС/ООС и органът по сигурността на Комисията могат да се споразумеят за процедура, при която посещенията за конкретен класифициран договор могат да бъдат организирани пряко между служителя по сигурността на посетителя и служителя по сигурността на структурата, които трябва да бъде посетена. Образец на формуляра, който се използва за тази цел, е даден в приложение III, допълнение B. Тази извънредна процедура се урежда в ИСП или други специфични договорености. В тези случаи процедурите, установени в член 8 и в член 9, параграф 1, не се прилагат.

2. Посещенията, свързани с достъп до информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, се организират пряко между изпращащия и приемащия субект, без да е необходимо да се следват процедурите, определени в член 8 и в член 9, параграф 1.

ГЛАВА 5

ПРЕДАВАНЕ И ПРЕНАСЯНЕ НА КИЕС ПРИ ИЗПЪЛНЕНИЕТО НА КЛАСИФИЦИРАНИ ДОГОВОРИ

Член 11

Основни принципи

Възложителят гарантира, че всички решения, свързани с предаването и пренасянето на КИЕС, са в съответствие с Решение (ЕС, Евратом) 2015/444 и правилата за неговото прилагане, както и с условията на класифицирания договор, включително съгласието на създателя на информацията.

Член 12

Работа в електронна форма

1. Работата с КИЕС и нейното предаване в електронна форма се извършват в съответствие с глави 5 и 6 от Решение (ЕС, Евратом) 2015/444 и правилата за неговото прилагане.

Комуникационните и информационните системи, собственост на изпълнителя и използвани за работа с КИЕС при изпълнението на договора („КИС на изпълнителя“), подлежат на акредитиране от отговорния орган по акредитиране на сигурността (ОАС). Всяко електронно предаване на КИЕС се защитава чрез криптографски продукти, одобрени в съответствие с член 36, параграф 4 от Решение (ЕС, Евратом) 2015/444. Мерките по TEMPEST се прилагат в съответствие с член 36, параграф 6 от посоченото решение.

2. Акредитацията за сигурност на КИС на изпълнителя, които работят с КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, както и всяка връзка помежду им могат да бъдат делегирани на служителя по сигурността на изпълнителя, ако националните законови и подзаконови актове позволяват това. Когато посочената задача е делегирана, изпълнителят носи отговорност за изпълнението на минималните изисквания за сигурност, посочени в ПАС, при работа в неговите КИС с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED. Съответните НОС/ООС и ОАС запазват обаче отговорността за защитата на информацията с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, с която работи изпълнителят, както и правото да подлагат на проверка мерките за сигурност, предприети от изпълнителя. Освен това изпълнителят предоставя на възложителя и, когато това се изисква от националните законови и подзаконови актове, на компетентния национален ОАС декларация за съответствие, удостоверяваща, че КИС на изпълнителя и съответните връзки между тях са акредитирани за работа с КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED ([12]).

Член 13

Транспортиране с платени куриерски услуги

При транспортирането на КИЕС с платени куриерски услуги трябва да се спазват съответните разпоредби на решенията на Комисията относно правилата за прилагане при работа с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED и CONFIDENTIEL UE/EU CONFIDENTIAL.

Член 14

Пренасяне на ръка

1. Пренасянето на класифицирана информация на ръка подлежи на строги изисквания за сигурност.

2. Информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED може да бъде пренасяна на ръка от служители на изпълнителя в рамките на ЕС, при условие че са изпълнени следните изисквания:

а) използваният плик или опаковка не прозира и не носи обозначение за класификацията на своето съдържание;

([12]) Минималните изисквания за комуникационни и информационни системи, работещи с КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, са определени в приложение III, допълнение Д.

б) класифицираната информация не напуска приносителя;

в) пликът или опаковката не се отваря по пътя.

3. Пренасянето на ръка на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET от служители на изпълнителя в рамките на държава — членка на ЕС, се организира предварително между изпращащата и приемащата организация. Изпращащият орган или структура информира получаващия орган или структура за подробностите на пратката, включително референтен номер, класификация, очаквано време на пристигане и името на куриера. Такова пренасяне на ръка се разрешава, при условие че са спазени следните изисквания:

а) класифицираната информация се пренася в двоен плик или опаковка;

б) външният плик или опаковка има защита и не носи никакво обозначение за класификацията на своето съдържание, а вътрешният плик носи нивото на класификация за сигурност;

в) КИЕС не напуска приносителя;

г) пликът или опаковката не се отваря по пътя;

д) пликът или опаковката се пренася в куфарче, което се заключва, или подобен одобрен сейф с такива размери и тегло, че да може да остане през цялото време при приносителя, без да се предава в багажното отделение;

е) куриерът носи удостоверение за куриер, издадено от неговия компетентен орган по сигурността, с което на куриера се разрешава пренасянето на класифицираната пратка, както е посочена.

4. За пренасянето на ръка от служители на изпълнителя на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET от една държава — членка на ЕС, в друга, се прилагат следните допълнителни правила:

а) куриерът отговаря за безопасното съхраняване на пренасяния класифициран материал до предаването му на получателя;

б) в случай на нарушение на сигурността НОС/ООС на изпращача могат да поиска от органите в държавата, в която е било извършено нарушението, да проведат разследване, да докладват своите констатации и да предприемат съответните правни или други действия;

в) куриерът трябва да е информиран за всички задължения по отношение на сигурността, които трябва да се спазват по време на пренасянето, и да е подписал съответна декларация за това;

г) инструкциите за куриера се прикрепват към удостоверението за куриер;

д) на куриера се предоставят описание на пратката и маршрут;

е) след приключване на пътуването(пътуванията) документите се връщат на издаващия НОС/ООС или се съхраняват в наличност от получателя за целите на мониторинга;

ж) ако митническите, имиграционните органи или граничната полиция поискат да проучат и проверят пратката, им се разрешава да отворят и разгледат достатъчно части на пратката, за да се установи, че тя не съдържа материал, различен от декларирания;

з) митническите органи следва да бъдат приканени да зачитат официалния характер на транспортните документи и на разрешението, носени от куриера.

Ако пратката бъде отворена от митническите органи, това следва да се извърши без видимост за неупълномощени лица, както и в присъствието на куриера, когато това е възможно. Куриерът трябва да поиска пратката бъде опакована отново, както и това органите, извършващи проверката, да поставят нова пломба на пратката и да потвърдят писмено, че е отваряна от тях.

5. Пренасянето на ръка от служители на изпълнителя на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET за трета държава или международна организация е предмет на разпоредбите на споразумението за сигурност на информацията или на административната договореност, сключени между съответно Европейския съюз или Комисията и въпросната трета държава или международна организация.

ГЛАВА 6

ПЛАН ЗА НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА

Член 15

Планове за действие при извънредни ситуации и мерки за възстановяване

В качеството си на възложител службата на Комисията гарантира, че класифицираният договор изисква от изпълнителя да състави планове за действие при извънредни ситуации с цел защита на КИЕС, с която се работи във връзка с изпълнението на класифицирания договор в извънредни ситуации, както и да въведе мерки за предотвратяване и възстановяване в контекста на планирането на непрекъснатостта на дейността с цел свеждане до минимум въздействието на инциденти, свързани с работата с КИЕС и нейното съхранение. Изпълнителят трябва да сведе до знанието на възлагащия орган своите планове за действие при извънредни ситуации.

Член 16

Влизане в сила

Настоящото решение влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 17 октомври 2019 година.

За Комисията

от името на Председателя,

Günther OETTINGER

Член на Комисията

ПРИЛОЖЕНИЕ I

СТАНДАРТНА ИНФОРМАЦИЯ В ОБЯВЛЕНИЯТА ЗА ОБЩЕСТВЕНИ ПОРЪЧКИ

(да се адаптира към използваните обявления за поръчки)

За договори, свързани с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET

Други специални условия (*ако е приложимо*)

Изпълнението на договора е предмет на специални условия ● да ○ не

(*ако да*) Описание на специалните условия:

Договорът ще включва достъп до, обработка и/или съхранение на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, спрямо която се прилагат правилата за сигурност за защита на класифицираната информация на ЕС, установени с Решение (ЕС, Евратом) 2015/444, и правилата за прилагане на Решението ([1]).

Ще се изисква удостоверение за сигурност на структурата, както и разрешение за достъп до класифицирана информация на служителите на изпълнителя, които работят с класифицирана информация.

Специалните задължения по отношение на сигурността ще бъдат част от договора (приложение относно аспектите на сигурността). Възлагането на подизпълнители ще подлежи на предварителното писмено съгласие на възложителя, както и на спазването на всички правила за сигурност от подизпълнителя и неговия персонал.

За договори, свързани с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED

Други специални условия (*ако е приложимо*)

Изпълнението на договора е предмет на специални условия ● да ○ не

(*ако да*) Описание на специалните условия:

Договорът ще предполага достъп до, обработка и/или съхранение на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, спрямо която се прилагат правилата за сигурност за защита на класифицираната информация на ЕС, установени с Решение (ЕС, Евратом) 2015/444, и правилата за прилагане на Решението ([2]).

Специалните задължения по отношение на сигурността ще бъдат част от договора (приложение относно аспектите на сигурността). Възлагането на подизпълнители ще подлежи на предварителното писмено съгласие на възложителя, както и на спазването на всички правила за сигурност от подизпълнителя и неговия персонал.

([1]) Възложителят следва да вмъкне позоваванията веднага след приемането на правилата за прилагане.
([2]) Възложителят следва да вмъкне позоваванията веднага след приемането на правилата за прилагане.

ПРИЛОЖЕНИЕ II

СТАНДАРТНИ КЛАУЗИ В ДОГОВОРИТЕ ЗА ОБЩЕСТВЕНИ ПОРЪЧКИ

(да се адаптира към използваните договори)

ЧЛЕН XX

ЗАДЪЛЖЕНИЯ ПО ОТНОШЕНИЕ НА СИГУРНОСТТА

XX.1 Класифицирана информация на ЕС

Ако изпълнението на договора включва използване или генериране на класифицирана информация на ЕС, тази информация трябва да се третира в съответствие с приложението относно аспектите на сигурността (ПАС) и неговото ръководството за класифициране за целите на сигурността (РКЦС), както е посочено в приложение 1 и в Решение (ЕС, Евратом) 2015/444 и правилата за неговото прилагане ([1]), до момента на нейната декласификация.

Всички планирани резултати, съдържащи класифицирана информация, трябва да бъдат представени в съответствие със специални процедури, договорени с възложителя.

Задачите за действия, свързани с класифицирана информация, не трябва да се възлагат на подизпълнители без предварителното изрично писмено одобрение на възложителя.

Класифицираната информация на ЕС не трябва да се предоставя на трети страни (включително подизпълнители) без предварителното изрично писмено одобрение на възложителя.

([1]) Възложителят следва да вмъкне позоваванията веднага след приемането на правилата за прилагане.

ПРИЛОЖЕНИЕ III

[приложение IV (към рамковия договор)]

ПРИЛОЖЕНИЕ ОТНОСНО АСПЕКТИТЕ НА СИГУРНОСТТА (ПАС)

[Образец]

Допълнение А

ИЗИСКВАНИЯ ЗА СИГУРНОСТ

Възложителят трябва да включи следните изисквания за сигурност в приложението относно аспектите на сигурността (ПАС). Някои клаузи може да не са приложими към договора. Те са представени в квадратни скоби.

Списъкът на клаузите не е изчерпателен. Могат да се добавят допълнителни клаузи в зависимост от естеството на класифицирания договор.

ОБЩИ УСЛОВИЯ

[*Забележка: прилагат се за всички класифицирани договори*]

1. Настоящото приложение относно аспектите на сигурността (ПАС) е неразделна част от класифицирания договор [или договор за подизпълнение] и описва свързаните с договора изисквания за сигурност. Неспазването на тези изисквания може да представлява достатъчно основание за прекратяване на договора.

2. Изпълнителите имат всички задължения, посочени в Решение (ЕС, Евратом) 2015/444 и правилата за неговото прилагане ([1]).

3. Класифицираната информация, генерирана при изпълнението на договора, трябва да бъде обозначена като класифицирана информация на ЕС (КИЕС) на ниво на класификация за сигурност, както е определено в ръководството за класифициране за целите на сигурността (РКЦС) в допълнение Б към настоящото приложение. Отклонение от нивото на класификация, определено в РКЦС, се допуска само с писменото разрешение на възложителя.

4. Правата, с които разполага създателят на КИЕС, създадена и третирана при изпълнението на класифицирания договор, се упражняват от Комисията в качеството ѝ на възложител.

5. Без писменото съгласие на възложителя изпълнителят или подизпълнителят няма право да използва никаква информация или материал, предоставен от възложителя или изготвени от негово име, за каквато и да било цел, различна от тази на договора.

6. Изпълнителят трябва да разследва всички нарушения на сигурността, свързани с КИЕС, и да докладва за тях на възложителя възможно най-бързо. Изпълнителят или подизпълнителят трябва незабавно да докладва на компетентния национален орган по сигурността (НОС) или на определения орган по сигурността (ООС) и, когато националните законови и подзаконови актове го позволяват, на органа по сигурността на Комисията, всички случаи, в които е известно или има основание да се подозира, че КИЕС, предоставена или генерирана съгласно договора, е била изгубена или разкрита на неупълномощени лица.

7. След изтичането на договора изпълнителят или подизпълнителят трябва да върне всяка КИЕС, с която разполага, на възложителя във възможно най-кратък срок. Когато е възможно, изпълнителят или подизпълнителят може да унищожи КИЕС, вместо да я върне. Това трябва да се прави в съответствие с националните законови и подзаконови актове на държавата, в която е установен изпълнителят, с предварителното съгласие на органа по сигурността на Комисията и съгласно неговите указания. КИЕС трябва да бъде унищожена по начин, който прави невъзможно нейното цялостно или частично възстановяване.

8. Когато на изпълнителя или подизпълнителя е разрешено да задържи КИЕС след прекратяването или сключването на договора, КИЕС трябва да продължи да бъде защитена в съответствие с Решение (ЕС, Евратом) 2015/444 (наричано по-нататък „Решение 2015/444 на Комисията“) и правилата за неговото прилагане ([2]).

9. При всяка електронна работа, обработване и предаване на КИЕС трябва да се спазват разпоредбите на глави 5 и 6 от Решение 2015/444 на Комисията. Това включва, наред с другото, изискването комуникационните и информационните системи, притежавани от изпълнителя и използвани за обработването на КИЕС за целите на договора (наричани по-долу „КИС на изпълнителя“), да са преминали акредитация ([3]); изискването предаването на КИЕС по електронен път да бъде защитено чрез криптографски продукти, одобрени в съответствие с член 36, параграф 4 от Решение 2015/444 на Комисията, както и изискването мерките за сигурност по TEMPEST да се прилагат в съответствие с член 36, параграф 6 от Решение 2015/444 на Комисията.

([1]) Възложителят следва да вмъкне позоваванията веднага след приемането на правилата за прилагане.
([2]) Възложителят следва да вмъкне позоваванията веднага след приемането на правилата за прилагане.
([3]) Преминаващата през акредитацията страна трябва да предостави на възложителя декларация за съответствие чрез органа по сигурността на Комисията и в координация със съответния национален орган по акредитиране на сигурността (ОАС).

10. Изпълнителят или подизпълнителят трябва да разполага с вътрешнофирмени планове за действие при извънредни ситуации с цел защита на КИЕС, с която се работи при изпълнението на класифицирания договор, в извънредни ситуации и трябва да въведе превантивни мерки и мерки за възстановяване с цел свеждане до минимум на въздействието на инцидентите, свързани с работата с КИЕС и нейното съхранение. Изпълнителят или подизпълнителят трябва да сведе до знанието на възложителя своите вътрешнофирмени планове за действие при извънредни ситуации.

ДОГОВОРИ, НАЛАГАЩИ ДОСТЪП ДО ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ RESTREINT UE/EU RESTRICTED

11. За спазването на договора не се изисква разрешение за достъп на служител (РДС). Въпреки това информацията или материалите с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED трябва да са достъпни само за служителите на изпълнителя, които се нуждаят от такава информация за изпълнението на договора (на принципа „необходимост да се знае“), които са били информирани от служителя по сигурността на изпълнителя относно своите отговорности и относно последиците от всеки случай на компрометиране или нарушение на сигурността на такава информация и които са потвърдили писмено, че са запознати с последиците при неосигуряване на защита на КИЕС.

12. С изключение на случаите, когато възложителят е дал писменото си съгласие, изпълнителят или подизпълнителят не трябва да предоставя достъп до информация или материали с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED на субекти или лица, различни от неговите служители, които имат „необходимост да се знае“.

13. Изпълнителят или подизпълнителят не може да премахва грифовете за сигурност на класифицираната информация, генерирана или предоставена по време на изпълнението на договора, и не може да декласифицира информация без писменото съгласие на възложителя.

14. Информацията или материалите с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED трябва да се съхраняват в заключени офис мебели, когато не се използват. Когато се пренасят, документите трябва да се съхраняват в непрозрачен плик. Документите не трябва да напускат приносителя и не трябва да бъдат отваряни при преноса.

15. Изпълнителят или подизпълнителят може да предава на Комисията документи с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, като използва платени куриерски услуги, пощенски услуги, предаване на ръка или електронни средства. За тази цел изпълнителят или подизпълнителят трябва да спазва инструкциите за сигурност на програмата (или проекта) (ИСП), издадени от Комисията, и/или правилата за прилагане по отношение на индустриалната сигурност на Комисията във връзка с класифицирани договори за обществени поръчки ([4]).

16. Когато вече не са необходими, документите с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED трябва да бъдат унищожени по начин, който прави невъзможно тяхното цялостно или частично възстановяване.

17. Акредитацията за сигурност на КИС на изпълнителя, които работят с КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, както и на всяка връзка помежду им може да бъде делегирана на служителя по сигурността на изпълнителя, ако националните законови и подзаконови актове позволяват това. Когато акредитацията е делегирана по този начин, НОС/ООС/ОАС запазват отговорността за защитата на информацията с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, с която работи изпълнителят, и имат правото да подлагат на проверка мерките за сигурност, предприети от изпълнителя. Освен това изпълнителят предоставя на възложителя и, когато това се изисква от националните законови и подзаконови актове, на компетентния национален ОАС декларация за съответствие, удостоверяваща, че КИС на изпълнителя и съответните връзки между тях са акредитирани за работа с КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

РАБОТА С ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ RESTREINT UE/EU RESTRICTED В КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ СИСТЕМИ (КИС)

18. Минималните изисквания за КИС, работещи с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, са посочени в допълнение Д към настоящото приложение относно аспектите на сигурността (ПАС).

УСЛОВИЯ, ПРИ КОИТО ИЗПЪЛНИТЕЛЯТ МОЖЕ ДА СКЛЮЧВА ДОГОВОРИ ЗА ПОДИЗПЪЛНЕНИЕ

19. Изпълнителят трябва да получи разрешение от съответния отдел на Комисията в качеството му на възложител, преди да възложи на подизпълнител която и да е част от класифициран договор.

([4]) Възложителят следва да вмъкне позоваванията веднага след приемането на правилата за прилагане.

20. Договор за подизпълнение не може да бъде възлаган на дружество, регистрирано в държава извън ЕС, или на субект, принадлежащ на международна организация, ако тази държава извън ЕС или международна организация не е сключила споразумение за сигурност на информацията с ЕС или административна договореност с Комисията.

21. Когато изпълнителят възлага договор за подизпълнение, разпоредбите за сигурност на договора се прилагат *mutatis mutandis* по отношение на подизпълнителя(ите) и неговия(техния) персонал. В такъв случай изпълнителят е отговорен да гарантира, че всички подизпълнители прилагат тези принципи спрямо собствените си договорености за подизпълнение. За да се осигури подходящ надзор над сигурността, НОС/ООС на изпълнителя и подизпълнителя трябва да бъдат уведомени за възлагането на всички свързани класифицирани договори за подизпълнение с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET. Когато е целесъобразно, на НОС/ООС на изпълнителя и подизпълнителя се предоставя копие от конкретните разпоредби за сигурност на договора за подизпълнение. НОС/ООС, които е необходимо да бъдат уведомявани относно разпоредбите за сигурност на класифицирани договори с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, са изброени в приложението към правилата за прилагане на Комисията по отношение на индустриалната сигурност във връзка с класифицирани договори за възлагане на обществени поръчки ([1]).

22. Изпълнителят няма право да предоставя КИЕС на подизпълнител без предварителното писмено одобрение на възложителя. Ако изпращането на КИЕС на подизпълнители ще се извършва често или рутинно, възложителят може да даде своето одобрение за определен период (например 12 месеца) или за срока на договора за подизпълнение.

ПОСЕЩЕНИЯ

Ако спрямо посещенията, свързани с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, ще се прилага стандартната процедура за исканията за посещения, възложителят трябва да включи параграфи 23, 24 и 25 и да заличи параграф 26. Ако посещенията, свързани с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, се организират директно между изпращащите и приемащите субекти, възложителят трябва да заличи параграфи 24 и 25 и да включи само параграф 26.

23. Посещенията, свързани с достъп или потенциален достъп до информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, се организират директно между изпращащите и приемащите субекти, без да е необходимо да се следва процедурата, описана в параграфи 24—26 по-долу.

[24. За посещенията, свързани с достъп или потенциален достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, се прилага следната процедура:

а) служителят по сигурността на структурата, която изпраща посетителя, попълва всички релевантни части от формуляра за искане за посещение (допълнение B) и подава искането до НСО/ООС на структурата;

б) НСО/ООС на изпращащата структура трябва да потвърди РДС на посетителя, преди да представи искането за посещение на НСО/ООС на приемащата структура (или на органа по сигурността на Комисията, ако посещението е в помещения на Комисията);

в) след това служителят по сигурността на изпращащата структура получава от своя НОС/ООС отговора, получен от НОС/ООС на приемащата структура (или от органа по сигурността на Комисията), с който се разрешава или отхвърля искането за посещение;

г) искането за посещение се счита за одобрено, ако до пет работни дни преди датата на посещението не бъдат повдигнати възражения.]

[25. Преди да предостави на посетителя(ите) достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, приемащата структура трябва да е получила разрешение за това от своя НОС/ООС.]

[26. Посещенията, свързани с достъп или потенциален достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, се организират директно между изпращащите и приемащите субекти (образец на формуляра, който може да се използва за тази цел, се съдържа в допълнение B).]

([1]) Възложителят следва да вмъкне позоваванията веднага след приемането на правилата за прилагане.

27. При пристигането си в приемащата структура посетителите трябва да докажат своята самоличност, като представят валидна лична карта или паспорт.

28. Структурата, която е домакин на посещението, трябва да гарантира, че всички посетители се регистрират. Регистрите трябва да включват имената на посетителите, организацията, която те представляват, датата на изтичане на срока на валидност на РДС (ако е приложимо), датата на посещението и името (имената) на посетеното(ите) лице(а). Без да се засягат европейските правила за защита на данните, тези регистри трябва да се съхраняват за срок от не по-малко от пет години или в съответствие с националните правила и разпоредби, според случая.

ПОСЕЩЕНИЯ ЗА ОЦЕНКА

29. Органът по сигурността на Комисията може, в сътрудничество със съответния НОС/ООС, да извършва посещения на структурите на изпълнителите или подизпълнителите, за да се увери, че изискванията за сигурност при работа с КИЕС се спазват.

РЪКОВОДСТВО ЗА КЛАСИФИЦИРАНЕ ЗА ЦЕЛИТЕ НА СИГУРНОСТТА

30. В ръководството за класифициране за целите на сигурността (РКЦС) се съдържа списък на всички елементи в договора, които са класифицирани или трябва да бъдат класифицирани в хода на изпълнението на договора, правилата за това, както и описание на приложимите нива на класификация. РКЦС е неразделна част от този договор и се съдържа в допълнение Б към настоящото приложение.

Допълнение Б

РЪКОВОДСТВО ЗА КЛАСИФИЦИРАНЕ ЗА ЦЕЛИТЕ НА СИГУРНОСТТА

[специфичен текст, който трябва да се адаптира в зависимост от предмета на договора]

Допълнение B

ИСКАНЕ ЗА ПОСЕЩЕНИЕ

(ОБРАЗЕЦ)

Подробни указания за попълване на искането за посещение

(Заявлението трябва да бъде подадено само на английски език)

HEADING	Слага се отметка в полетата за вида на посещението и вида на информацията и се посочва колко обекта ще бъдат посетени и броят на посетителите.
4. **ADMINISTRATIVE DATA**	Попълва се от отправящия искането НОС/ООС.
5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY**	Посочват се пълното название и пощенският адрес. Посочват се град, държава и пощенски код, както е приложимо.
6. **ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED**	Посочват се пълното название и пощенският адрес. Посочват се град, държава, пощенски код, номер на телекс или факс (ако е приложимо), телефонен номер и адрес на електронна поща. Посочват се името и номерът на телефон/факс и адресът на електронна поща на основното звено за контакт или на лицето, с което е уредена срещата за посещението. Забележки: 1) Посочването на правилния пощенски код е важно, тъй като едно дружество може да има различни структури. 2) Когато искането се подава на ръка, приложение 1 може да се използва, когато трябва да бъдат посетени две или повече структури по един и същ повод. Когато се използва приложение, в точка 3 се посочва: „SEE ANNEX 1, NUMBER OF FAC: …“ (посочва се броят на структурите).
7. **DATES OF VISIT**	Посочва се фактическата дата или период (от — до) на посещението във формат „ден — месец — година“. Когато е приложимо, в скоби се посочва алтернативна дата или период.
8. **TYPE OF INITIATIVE**	Посочва се дали посещението е по инициатива на отправящата искането организация или структура, или е по покана на структурата, която ще бъде посетена.
9. **THE VISIT RELATES TO:**	Посочва се пълното наименование на проекта, договора или поканата за представяне на оферти, като се използват само обичайните им съкращения.

10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION**	Дава се кратко описание на причината(ите) за посещението. Да не се използват неразписани съкращения. Забележки: В случай на периодични посещения първите думи като елемент на данните в тази точка трябва да са „Периодични посещения“ (напр. „Периодични посещения за обсъждане на ___“)
11. **ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED**	Посочва се SECRET UE/EU SECRET (S-UE/EU-S) или CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), според случая.
12. **PARTICULARS OF VISITOR**	Забележка: когато в посещението участват повече от двама посетители, трябва да се използва приложение 2.
13. **THE SECURITY OFFICER OF THE REQUESTING ENTITY**	В тази точка се посочват името, телефонният номер, факс номерът и адресът на електронна поща на служителя по сигурността на отправящата искането структура.
14. **CERTIFICATION OF SECURITY CLEARANCE**	Това поле се попълва от удостоверяващия орган. Бележки за удостоверяващия орган: а. Посочват се име, адрес, телефонен номер, факс номер и адрес на електронна поща (може да бъдат отпечатани предварително). б. Тази точка трябва да бъде подписана и подпечатана (ако е приложимо).
15. **REQUESTING SECURITY AUTHORITY**	Това поле се попълва от НОС/ООС. Бележка за НОС/ООС: а. Посочват се име, адрес, телефонен номер, факс номер и адрес на електронна поща (може да бъдат отпечатани предварително). б. Тази точка трябва да бъде подписана и подпечатана (ако е приложимо).

Всички полета трябва да бъдат попълнени и формулярът да бъде изпратен по междуправителствени канали ([2]).

([2]) Ако е било договорено, че посещенията, свързани с достъп или потенциален достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, могат да бъдат организирани директно, попълненият формуляр може да бъде подаден директно до служителя по сигурността на субекта, който ще бъде посетен.

REQUEST FOR VISIT

(MODEL)

TO: _____

1. **TYPE OF VISIT REQUEST**	2. **TYPE OF INFORMATION**	3. **SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____

4. **ADMINISTRATIVE DATA:**

Requester:	NSA/DSA RFV Reference No_____
To:	Date *(dd/mm/yyyy)*: _____/_____/_____

5. **REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. **ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED** *(Annex 1 to be completed)*

7. **DATE OF VISIT** *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. **TYPE OF INITIATIVE:**

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. **THE VISIT RELATES TO CONTRACT:**

10. **SUBJECT TO BE DISCUSSED/REASONS/PURPOSE** *(Include details of host entity and any other relevant information. Abbreviations should be avoided):*

11. **ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:**

12. **PARTICULARS OF VISITOR(S)** *(Annex 2 to be completed)*

13. **THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:**

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL:**

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. **REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:**

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

STAMP

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. **REMARKS** *(Mandatory justification required in the case of an emergency visit)*:

<Място, запазено за позоваване на приложимото законодателство в областта на личните данни и връзка към задължителната информация, предоставяна на субекта на данните, напр. как се прилага член 13 от Общия регламент относно защитата на данните ([3]).>

([3]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

ANNEX 1 to RFV FORM

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED

1.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

2.

NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

<Място, запазено за позоваване на приложимото законодателство в областта на личните данни и връзка към задължителната информация, предоставяна на субекта на данните, напр. как се прилага член 13 от Общия регламент относно защитата на данните ([1]).>

([1]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*: ____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

<Място, запазено за позоваване на приложимото законодателство в областта на личните данни и връзка към задължителната информация, предоставяна на субекта на данните, напр. как се прилага член 13 от Общия регламент относно защитата на данните ([1]).>

([1]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

Допълнение Г

ИНФОРМАЦИОНЕН ФОРМУЛЯР ЗА УДОСТОВЕРЕНИЕ ЗА СИГУРНОСТ НА СТРУКТУРА (ИФУСС)

(ОБРАЗЕЦ)

1. **Въведение**

1.1. Прилага се образец на информационен формуляр за удостоверение за сигурност на структура (ИФУСС) с цел бърз обмен на информация между националния орган по сигурността (НОС) или определения орган по сигурността (ООС), други компетентни национални органи по сигурността и Комисията (в качеството ѝ на възложител) по отношение на удостоверението за сигурност на структура (УСС) на дадена структура, която участва в класифицирани оферти, договори или договори за подизпълнение.

1.2. ИФУСС е валиден само ако е подпечатан от съответния НОС/ООС или друг компетентен орган.

1.3. ИФУСС съдържа раздел за искане и раздел за отговор и може да се използва за посочените по-горе цели или за всякакви други цели, за които се изисква конкретна структура да е със статут на УСС. Причината за запитването трябва да бъде посочена от отправящия искането НОС/ООС в поле 7 на раздела за искане.

1.4. Данните, съдържащи се в ИФУСС, обикновено не се класифицират, поради което е за предпочитане изпращането на ИФУСС между НОС/ООС/Комисията да се извършва чрез електронни средства.

1.5. НОС/ООС трябва да положат всички усилия, за да отговорят на искане с ИФУСС в срок от десет работни дни.

1.6. В случай че във връзка с това уверение бъде прехвърлена класифицирана информация или възложен договор, издаващият го НОС/ООС трябва да бъде уведомен.

Процедури и указания за използването на информационния формуляр за удостоверение за сигурност на структура (ИФУСС)

Тези подробни указания са предназначени за НОС/ООС или за възложителя на Комисията, който попълва ИФУСС. За предпочитане е искането да бъде изписано с главни букви.

ЗАГЛАВНА ЧАСТ	Отправящият искането посочва пълното название на НОС/ООС и името на държавата.
1. **ВИД НА ИСКАНЕТО**	Отправящият искането възложител избира подходящото поле за отметка за вида искане чрез ИФУСС. Посочва се необходимото ниво на разрешение за достъп до класифицирана информация. Използват се следните съкращения: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C КИС = Комуникационни и информационни системи за обработване на класифицирана информация

2. **ИНФОРМАЦИЯ ЗА ОБЕКТА**	Полета 1—6 не се нуждаят от обяснение. В поле 4 трябва да се използва стандартният двубуквен код на държавата. Поле 5 не е задължително.
3. **ПРИЧИНА ЗА ИСКАНЕТО**	Да се посочат конкретната причина за искането, показателите по проекта, номерът на договора или поканата за представяне на оферти. Да се посочат необходимостта от капацитет за съхранение, нивото на класификация за сигурност на КИС и т.н. Трябва да се включат всички срокове/дати на изтичане на валидност/дати на възлагане на договора, които могат да са от значение за изготвянето на УСС.
4. **ОТПРАВЯЩ ИСКАНЕТО НОС/ООС**	Да се посочат името на лицето, отправящо фактически искането (от името на НОС/ООС), и датата на искането с цифри във формат (дд/мм/гггг).
5. **РАЗДЕЛ ЗА ОТГОВОР**	Полета 1—5: да се изберат подходящите полета. Поле 2: ако е в ход УСС, се препоръчва да се съобщи на отправящия искането (ако е известно) колко време ще отнеме обработването. Поле 6: а) въпреки че отговорът се различава по държава или дори по структури, се препоръчва да се посочи датата, на която изтича срокът на валидност на УСС. б) в случаите, когато срокът на валидност на уверението за издаване на УСС е неограничен, това поле може да бъде зачеркнато. в) в съответствие със съответните национални правила и разпоредби, отправящият искането или изпълнителят или подизпълнителят е отговорен за подаването на искане за подновяване на УСС.
6. **ЗАБЕЛЕЖКИ**	Може да се използва за допълнителна информация по отношение на УСС, структурата или горните полета.
7. **ИЗДАВАЩ УДОСТОВЕРЕНИЕТО НОС/ООС**	Да се посочат наименованието на предоставящия орган (от името на НОС/ООС) и датата на отговора с цифри във формат (дд/мм/гггг).

ИНФОРМАЦИОНЕН ФОРМУЛЯР ЗА УДОСТОВЕРЕНИЕ ЗА СИГУРНОСТ НА СТРУКТУРА (ИФУСС)

(ОБРАЗЕЦ)

Всички полета трябва да бъдат попълнени и формулярът да бъде предаден по междуправителствените канали или по каналите за комуникация между правителства и международни организации.

ИСКАНЕ ЗА УВЕРЕНИЕ ЗА ИЗДАВАНЕ НА УДОСТОВЕРЕНИЕ ЗА СИГУРНОСТ НА СТРУКТУРА

ДО: _____

(НОС/ООС Държава)

Да се попълнят полетата за отговор, както е приложимо:

[] Да се предостави уверение за издаване на УСС на ниво на класификация за сигурност: [] S-UE/EU-S [] C-UE/EU-C

за структурите, посочени по-долу

[] включително безопасното съхраняване на класифициран(а) материал/информация

[] включително комуникационните и информационните системи (КИС) за обработване на класифицирана информация

[] Да се започне, директно или при съответно искане на изпълнител или подизпълнител, процесът на получаване на УСС до и включително на нивото на ..... с ..... ниво на безопасно съхраняване и ..... ниво на КИС, ако в момента структурата не притежава тези нива на капацитет.

Да се потвърди точността на данните на посочената по-долу структура и да се направят необходимите поправки/допълнения.

1.	Пълно наименование на структурата:	Поправки/Допълнения:
	.....	.....
2.	Пълен адрес на структурата:	
	.....	.....
3.	Пощенски адрес (ако е различен от този в т. 2)	
	.....	.....
4.	Пощенски код/град/държава	
	.....	.....
5.	Име на служителя по сигурността	
	.....	.....
6.	Телефон/факс/адрес на електронна поща на служителя по сигурността	
	.....	.....

7. Настоящото искане се прави по следната(ите) причина(и): (да се предоставят подробности за преддоговорния етап (подбора на предложения), договора или договора за подизпълнение, програмата/проекта и др.)

.....

Отправящ искането НОС/ООС/възложител на Комисията: Наименование: ..... Дата: (дд/мм/гггг) .....

ОТГОВОР (в срок от десет работни дни)

С настоящото се удостоверява, че:

1. [] горепосочената структура притежава УСС до и включително на нивото на [] S-UE/EU-S

   [] C-UE/EU-C.

2. Горепосочената структура е в състояние да съхранява безопасно класифицирана информация/материал:

   [] да, ниво: ..... [] не.

3. Горепосочената структура има акредитирани/одобрени КИС:

   [] да, ниво: ..... [] не.

4. [] във връзка с горепосоченото искане е започнат процесът по издаване на УСС. Ще бъдете уведомени за издаването или отказа за издаване на УСС.

5. [] горепосочената структура не разполага с УСС.

6. Валидността на настоящото уверение за издаване на УСС изтича на: ..... (*дд/мм/гггг*) или според указаното от НОС/ООС, ако е различно. Ще бъдете информирани в случай на по-ранна промяна на статуса на горепосочената информация или при евентуални промени в нея.

7. Забележки:

   .....

Издаващ удостоверението НОС/ООС Наименование: ..... Дата: (дд/мм/гггг) .....

<Място, запазено за позоваване на приложимото законодателство в областта на личните данни и връзка към задължителната информация, предоставяна на субекта на данните, напр. как се прилага член 13 от Общия регламент относно защитата на данните ([2]).>

([2]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

Допълнение Д

Минимални изисквания за защита на КИЕС в електронен формат на ниво RESTREINT UE/EU RESTRICTED, с която се работи в КИС на изпълнител

Общи положения

1. Изпълнителят е отговорен да гарантира, че защитата на информацията с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED отговаря на минималните изисквания за сигурност, установени в настоящата клауза за сигурност, както и на другите допълнителни изисквания, поставени от възложителя или, ако е приложимо, от националния орган по сигурността (НОС) или определения орган по сигурността (ООС).

2. Изпълнителят носи отговорност за изпълнението на изискванията за сигурност, посочени в настоящия документ.

3. За целите на настоящия документ понятието „комуникационна и информационна система“ (КИС) обхваща цялото оборудване, използвано за работа с КИЕС и нейното съхранение и предаване, включително работни станции, принтери, копирни машини, факс машини, сървъри, системи за управление на мрежи, мрежови контролери и комуникационни контролери, лаптопи, преносими компютри, таблети, смартфони и преносими устройства за съхранение на данни, като например USB устройства, компактни дискове, SD карти и др.

4. Специалното оборудване, като например криптографските продукти, трябва да бъде защитено в съответствие с неговите специфични оперативни процедури за сигурност (SecOPS).

5. Изпълнителите трябва да създадат организация, отговорна за управлението на сигурността на КИС, която работи с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, и да назначат служител по сигурността, отговарящ за съответната структура.

6. За съхраняването или обработването на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED не се разрешава използването на ИТ решения (хардуер, софтуер или услуги), които са лична собственост на персонала на изпълнителя.

7. Акредитацията на КИС на изпълнителя, която работи с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, трябва да бъде одобрена от органа по акредитиране на сигурността (ОАС) на съответната държава членка или да бъде делегирана на служителя по сигурността на изпълнителя, ако това се разрешава от националните законови и подзаконови актове.

8. Единствено информацията с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, която е криптирана посредством одобрени криптографски продукти, може да се обработва, съхранява или предава (по жичен или безжичен път) като всяка друга некласифицирана информация съгласно договора. Тези криптографски продукти трябва да са одобрени от ЕС или от държава членка.

9. Външните структури, осъществяващи поддръжка/ремонт, трябва да са договорно задължени да спазват приложимите разпоредби за работа с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, както е посочено в настоящия документ.

10. По искане на възложителя или на съответния НОС/ООС/ОАС изпълнителят трябва да представи доказателства за спазването на договорната клауза относно сигурността. Когато, за да се гарантира спазването на тези изисквания, се изискват също одит и инспекция на процесите и структурите на изпълнителя, изпълнителите трябва да разрешат на представители на възложителя, НОС/ООС/ОАС или на съответния орган по сигурността на ЕС да извършат такъв одит и инспекция.

Физическа сигурност

11. Зоните, в които се използват КИС за показване, съхраняване, обработване или предаване на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, и зоните, в които се помещават сървъри, системи за управление на мрежи, мрежови контролери и комуникационни контролери за такива КИС, трябва да се обособят като отделни и и контролирани зони с целесъобразна система за контрол на достъпа. Достъпът до тези отделни и контролирани зони трябва да бъде ограничен до физическите лица, на които е дадено специално разрешение. Без да се засяга точка 8, оборудването, описано в точка 3, трябва да се съхранява в такива отделни и контролирани зони.

12. Трябва да се прилагат механизми и/или процедури за сигурност, за да се регулира въвеждането или свързването на преносими носители на информация (като USB устройства, запаметяващи устройства с голям капацитет или записваеми компактни дискове) към компоненти на КИС.

Достъп до КИС

13. Достъпът до КИС на изпълнителя, в която се работи с КИЕС, се разрешава при строго спазване на принципа „необходимост да се знае“ и на упълномощаване на персонала.

14. Всички КИС трябва да разполагат с актуални списъци на упълномощените потребители. В началото на всяка сесия всички потребители трябва да преминат проверка на идентичността.

15. Паролите, които са част от повечето мерки за сигурност чрез идентификация и автентификация, трябва да бъдат съставени от най-малко девет знака и трябва да включват цифрови и „специални“ символи (ако системата позволява това), както и буквени символи. Паролите трябва да се сменят най-малко веднъж на всеки 180 дни. Те трябва да бъдат променени възможно най-бързо, ако са били компрометирани или разкрити на неупълномощено лице или ако има съмнение за такова компрометиране или разкриване.

16. Всички КИС трябва да имат вътрешни механизми за контрол на достъпа, които да не позволяват на неупълномощени потребители да имат достъп или да променят информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, или да променят механизмите за сигурност на системите. Сесията на потребителите в КИС трябва автоматично да се прекратява, ако терминалите им не са активни в продължение на предварително определен период от време, или КИС трябва да активират защитен с парола екран след 15 минути бездействие.

17. Всеки потребител на КИС получава уникален потребителски профил и потребителско име. Потребителските профили трябва да се заключват автоматично при направени пет последователни неуспешни опита за влизане в системата.

18. Всички потребители на КИС трябва да бъдат осведомени за своите отговорности и за процедурите, които трябва да спазват с оглед на защитата на информацията с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED. Отговорностите и процедурите, които трябва да се спазват, трябва да бъдат документирани, а потребителите да потвърдят писмено, че са запознати с тях.

19. На разположение на потребителите и администраторите трябва да има специфични оперативни процедури за сигурност (SecOPS), които трябва да включват описания на свързаните със сигурността роли и съответния списък със задачи, инструкции и планове.

Отчитане, одитиране и реагиране при инциденти

20. Всеки достъп до КИС трябва да се регистрира.

21. Трябва да се регистрират следните събития:

    а) всички опити за влизане в КИС, независимо дали са успешни, или неуспешни;

    б) прекъсването на сесията (включително при пресрочване на времето за бездействие, когато е приложимо);

    в) създаването, заличаването или промяната на правата и привилегиите по отношение на достъпа;

    г) създаването, заличаването или промяната на пароли.

22. За всички изброени по-горе събития трябва да се съобщава най-малко следната информация:

    а) вид събитие;

    б) потребителско име;

    в) дата и час;

    г) идентификационен номер на устройството.

23. Отчетните записи следва да са в помощ на служителя по сигурността при проучването на евентуални инциденти, свързани със сигурността. Те могат да бъдат използвани и в подкрепа на съдебни разследвания в случай на инцидент, свързан със сигурността. Всички записи, свързани със сигурността, следва да се проверяват редовно, за да се установят евентуални инциденти, свързани със сигурността. Отчетните записи трябва да бъдат защитени от неразрешено заличаване или промяна.

24. Изпълнителят трябва да има установена стратегия за реагиране при инциденти, свързани със сигурността. Потребителите и администраторите трябва да бъдат инструктирани как да реагират при инциденти, как да докладват за тях и какво да правят в случай на извънредна ситуация.

25. При компрометиране или предполагаемо компрометиране на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED трябва да се докладва на възложителя. Докладът трябва да съдържа описание на засегнатата информация и описание на обстоятелствата на компрометирането или предполагаемото компрометиране. Всички потребители на КИС трябва да бъдат информирани как да докладват за всеки действителен или предполагаем инцидент, свързан със сигурността, на служителя по сигурността.

Мрежи и взаимосвързаност

26. Когато КИС на изпълнител, работеща с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, е свързана с КИС, която не е акредитирана, това значително увеличава заплахата както за сигурността на КИС, така и за информацията с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, с която се работи в тази КИС. Това включва интернет и други публични или частни КИС, като например други КИС, собственост на изпълнителя или подизпълнителя. В този случай изпълнителят трябва да извърши оценка на риска, за да определи допълнителните изисквания за сигурност, които трябва да бъдат изпълнени като част от процеса по акредитиране на сигурността. Изпълнителят предоставя на възложителя и, когато това се изисква от националните законови и подзаконови актове, на компетентния ОАС декларация за съответствие, удостоверяваща, че КИС на изпълнителя и съответните връзки между тях са акредитирани за работа с КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED.

27. Дистанционният достъп от други системи до LAN услуги (напр. достъп от разстояние до електронна поща и дистанционна системна поддръжка) е забранен освен ако възложителят е въвел и одобрил специални мерки за сигурност и, когато това се изисква от националните законови и подзаконови актове, те са одобрени от компетентния ОАС.

Управление на конфигурацията

28. Трябва да съществува и редовно да се поддържа подробна хардуерна и софтуерна конфигурация, както е описана в документацията за акредитацията/одобрението (включително схемите на системите и мрежите).

29. Служителят по сигурността на изпълнителя трябва да извършва проверки на хардуерната и софтуерната конфигурация, за да гарантира, че не е бил въведен неразрешен хардуер или софтуер.

30. Промените в конфигурацията на КИС на изпълнителя трябва да бъдат оценени с оглед на последиците от тях за сигурността и трябва да бъдат одобрени от служителя по сигурността, а когато това се изисква от националните законови и подзаконови актове — от ОАС.

31. Системата трябва да бъде внимателно обследвана за всички слабости по отношение на сигурността поне веднъж на всеки три месеца. Софтуерът за откриване на зловреден софтуер трябва да бъде инсталиран и да се актуализира постоянно. Ако е възможно, този софтуер следва да има национално или международно признато одобрение, в противен случай следва да бъде широко приет промишлен стандарт.

32. Изпълнителят трябва да изготви план за непрекъснатост на работата. Трябва да бъдат установени процедури за създаването на резервни копия, с които да се определи следното:

а) честотата на създаване на резервните копия;

б) изискванията за съхранение на място (огнеупорни контейнери) или извън обекта;

в) контролът на упълномощения достъп до резервните копия.

Трайно заличаване от електронни средства и унищожаване

33. Преди да бъдат изведени от експлоатация, КИС или носителите на информация, които в някакъв момент са съдържали данни с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, трябва да бъдат изцяло подложени на следния процес на трайно заличаване:

а) флаш памет (напр. USB устройства, SD карти, полупроводникови дискови устройства, хибридни твърди дискове) трябва да бъдат презаписани поне три пъти и след това да бъдат проверени, за да се гарантира, че оригиналното съдържание не може да бъде възстановено, или да бъдат изтрити с помощта на одобрен софтуер за изтриване;

б) магнитни носители (напр. твърди дискове) трябва да бъдат презаписани или размагнитени;

в) оптичните носители (например CD и DVD) трябва да бъдат нарязани или раздробени;

г) за всички други носители на информация следва да бъде консултиран възложителят или, ако е целесъобразно, НОС/ООС/ОАС относно изискванията за сигурност, които трябва да бъдат изпълнени.

34. Информацията с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED трябва да се заличава трайно от всички носители на информация, преди те да бъдат предадени на лице, което няма разрешение за достъп до информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED (например за поддръжка).

ПРИЛОЖЕНИЕ IV

Разрешения за достъп на служител и удостоверения за сигурност на структура за изпълнители, свързани с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, и НОС/ООС, които изискват да бъдат уведомени за класифицирани договори на ниво RESTREINT UE/EU RESTRICTED ([1])

Държава членка	УСС		Уведомяване на НОС/ООС за договор или договор за подизпълнение, свързан с информация с ниво на класификация за сигурност R-UE/EU-R		РДС	
	ДА	НЕ	ДА	НЕ	ДА	НЕ
Белгия		X		X		X
България		X		X		X
Чехия		X		X		X
Дания	X		X		X	
Германия		X		X		X
Естония	X		X			X
Ирландия		X		X		X
Гърция	X			X	X	
Испания		X	X			X
Франция		X		X		X
Хърватия		X	X			X
Италия		X	X			X
Кипър		X	X			X
Латвия		X		X		X

([1]) Тези национални изисквания за УСС/РДС и уведомленията за договори, свързани с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, не трябва да налагат допълнителни задължения на другите държави членки или изпълнителите, намиращи се под тяхна юрисдикция.
Забележка: уведомленията за договори, свързани с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, са задължителни.

Държава членка	УСС		Уведомяване на НОС/ООС за договор или договор за подизпълнение, свързан с информация с ниво на класификация за сигурност R-UE/EU-R		РДС	
	ДА	НЕ	ДА	НЕ	ДА	НЕ
Литва	X		X			X
Люксембург	X		X		X	
Унгария		X		X		X
Малта		X		X		X
Нидерландия	X (само за свързани с отбраната договори)		X (само за свързани с отбраната договори)			X
Австрия		X		X		X
Полша		X		X		X
Португалия		X		X		X
Румъния		X		X		X
Словения	X		X			X
Словакия	X		X			X
Финландия		X		X		X
Швеция	X (само за свързани с отбраната договори)		X (само за свързани с отбраната договори)		X (само за свързани с отбраната договори)	
Обединено кралство		X		X		X

ПРИЛОЖЕНИЕ V

СПИСЪК НА НАЦИОНАЛНИТЕ ОРГАНИ ПО СИГУРНОСТТА/ОПРЕДЕЛЕНИТЕ ОРГАНИ ПО СИГУРНОСТТА, ОТГОВАРЯЩИ ЗА РАБОТАТА ПО ПРОЦЕДУРИТЕ, СВЪРЗАНИ С ИНДУСТРИАЛНАТА СИГУРНОСТ

БЕЛГИЯ

National Security Authority
FPS Foreign Affairs
Rue des Petits Carmes 15
1000 Brussels
Телефон: +32 25014542 (секретариат)
Факс: +32 25014596
Електронна поща: nvo-ans@diplobel.fed.be

БЪЛГАРИЯ

1. State Commission on Information Security - National Security Authority/Държавна комисия по сигурността на информацията — Национален орган по сигурността
   4 Kozloduy Street/ул. „Козлодуй“ № 4
   1202 Sofia/София
   Телефон: +359 29835775
   Факс: +359 29873750
   Електронна поща: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)/Служба „Военна информация“ към Министерството на отбраната (служба за сигурност)
   3 Dyakon Ignatiy Street/ул. „Дякон Игнатий“ № 3
   1092 Sofia/София
   Телефон: +359 29227002
   Факс: +359 29885211
   Електронна поща:office@iksbg.org

3. State Intelligence Agency (security service)/Държавна агенция „Разузнаване“ (служба за сигурност)
   12 Hajdushka Polyana Street/ул. „Хайдушка поляна“ № 12
   1612 Sofia/София
   Телефон: +359 29813221
   Факс: +359 29862706
   Електронна поща: office@dar.bg

4. State Agency for Technical Operations (security service)/Държавна агенция „Технически операции“ (служба за сигурност)
   29 Shesti Septemvri Street/ул. „6-ти септември“ № 29
   1000 Sofia/София
   Телефон: +359 29824971
   Факс: +359 29461339
   Електронна поща: dato@dato.bg

   (Компетентните органи, изброени по-горе, провеждат процедурите за проверка с оглед на издаването на УСС на юридически лица, които кандидатстват за сключване класифициран договор, и на РДС за физически лица, които изпълняват класифициран договор за нуждите на тези органи.)

5. State Agency National Security (security service)/Държавна агенция „Национална сигурност“(служба за сигурност)
   45 Cherni Vrah Blvd./бул. „Черни връх“ № 45
   1407 Sofia/София
   Телефон: +359 28147109
   Факс: +359 29632188, +359 28147441
   Електронна поща: dans@dans.bg

   (Горепосочената служба за сигурност провежда процедурите за проверка на издаването на УСС и РДС за всички други юридически и физически лица в страната, които кандидатстват за сключване на класифициран договор или които изпълняват класифициран договор.)

ЧЕХИЯ

National Security Authority
Industrial Security Department
PO BOX 49
150 06 Praha 56
Телефон: +420 257283129
Електронна поща: sbr@nbu.cz

ДАНИЯ

1. Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Телефон: +45 33148888
Факс: +45 33430190

2. Forsvarets Efterretningstjeneste
(Danish Security Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Телефон: +45 33325566
Факс: +45 33931320

ГЕРМАНИЯ

1. За въпроси, свързани с политиката за индустриална сигурност, УСС, планове за пренос (с изключение на криптографска/поверителна търговска информация):
Federal Ministry of Economic Affairs and Energy
Industrial Security Division - ZB3
Villemombler Str. 76
53123 Bonn
Телефон: +49 228996154028
Факс: +49 228996152676
Електронна поща: dsagermany-zb3@bmwi.bund.de (служебна електронна поща)

2. За стандартни искания за посещения от/в германски дружества:
Federal Ministry of Economic Affairs and Energy
Industrial Security Division – ZB2
Villemombler Str. 76
53123 Bonn
Телефон: +49 228996152401
Факс: +49 228996152603
Електронна поща: zb2-international@bmwi.bund.de (служебна електронна поща)

3. Планове за пренос на криптографски материали:
Federal Office for Information Security (BSI)
National Distribution Agency/NDA-EU DEU
Mainzer Str. 84
53179 Bonn
Телефон: +49 2289995826052
Факс: +49 228991095826052
Електронна поща: NDAEU@bsi.bund.de

ЕСТОНИЯ

National Security Authority Department
Estonian Foreign Intelligence Service
Rahumäe tee 4B
11316 Tallinn
Телефон: +372 6939211
Факс: +372 6935001
Електронна поща:nsa@fis.gov.ee

ИРЛАНДИЯ

National Security Authority Ireland
Department of Foreign Affairs and Trade
76-78 Harcourt Street
Dublin 2
D02 DX45
Телефон: +353 14082724
Електронна поща: nsa@dfa.ie

ГЪРЦИЯ

Hellenic National Defence General Staff
E' Division (Security INTEL, CI BRANCH)
E3 Directorate
Industrial Security Office
227-231 Mesogeion Avenue
15561 Holargos, Athens
Телефон: +30 2106572022, +30 2106572178
Факс: +30 2106527612
Електронна поща: daa.industrial@hndgs.mil.gr

ИСПАНИЯ

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Calle Argentona 30
28023 Madrid
Телефон: +34 913725000
Факс: +34 913725808
Електронна поща: nsa-sp@areatec.com
За въпроси, свързани с разрешенията за достъп на служител до класифицирана информация: asip@areatec.com
За планове за пренос и международни посещения: sp-ivtco@areatec.com

ФРАНЦИЯ

Национален орган по сигурността (НСО) (за политиката и прилагането в области, различни от отбранителната промишленост)
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 boulevard de la Tour-Maubourg
75700 Paris 07 SP
Телефон: +33 171758193
Факс: +33 171758200
Електронна поща: ANSFrance@sgdsn.gouv.fr

Определен орган по сигурността (за прилагане в отбранителната промишленост)
Direction Générale de l'Armement
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)
60 boulevard du général Martial Valin
CS 21623
75509 Paris CEDEX 15
Телефон: +33 988670421
Електронна поща: За формуляри и изходящи искания за посещения: dga-ssdi.ai.fct@intradef.gouv.fr
за входящи искания за посещения: dga-ssdi.visit.fct@intradef.gouv.fr

ХЪРВАТИЯ

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Телефон: +385 14681222
Факс: +385 14686049
Електронна поща: NSACroatia@uvns.hr

ИТАЛИЯ

Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna 15
00187 Roma
Телефон: +39 0661174266
Факс: +39 064885273

КИПЪР

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Λεωφόρος Στροβόλου, 172-174
Στρόβολος, 2048, Λευκωσία
Τηλέφωνα: +357 22807569, +357 22807764
Τηλεομοιότυπο: +357 22302351
Електронна поща: cynsa@mod.gov.cy

Ministry of Defence
National Security Authority (NSA)
172-174, Strovolos Avenue
2048 Strovolos, Nicosia
Телефон: +357 22807569, +357 22807764
Факс: +357 22302351
Електронна поща: cynsa@mod.gov.cy

ЛАТВИЯ

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
Riga LV-1001
Телефон: +371 67025418, +371 67025463
Факс: +371 67025454
Електронна поща: ndi@sab.gov.lt, ndi@zd.gov.lv

ЛИТВА

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania)
National Security Authority
Gedimino 40/1
LT-01110 Vilnius
Телефон: +370 70666703, +370 70666701
Факс: +370 70666700
Електронна поща: nsa@vsd.lt

ЛЮКСЕМБУРГ

Autorité Nationale de Sécurité
207, route d'Esch
L-1471 Luxembourg
Телефон: +352 24782210
Електронна поща: ans@me.etat.lu

УНГАРИЯ

National Security Authority of Hungary
H-1399 Budapest P.O. Box 710/50
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Телефон: +36 13911862
Факс: +36 13911889
Електронна поща: nbf@nbf.hu

МАЛТА

Director of Standardisation
Designated Security Authority for Industrial Security
Standards & Metrology Institute
Malta Competition and Consumer Affairs Authority
Mizzi House
National Road
Blata I-Bajda HMR9010
Телефон: +356 23952000
Факс: +356 21242406
Електронна поща:certification@mccaa.org.mt

НИДЕРЛАНДИЯ

1. Ministry of the Interior and Kingdom Relations
PO Box 20010
2500 EA The Hague
Телефон: +31 703204400
Факс: +31 703200733
Електронна поща: nsa-nl-industry@minbzk.nl

2. Ministry of Defence
Industrial Security Department
PO Box 20701
2500 ES The Hague
Телефон: +31 704419407
Факс: +31 703459189
Електронна поща:indussec@mindef.nl

АВСТРИЯ

1. Federal Chancellery of Austria
Department I/12, Office for Information Security
Ballhausplatz 2
1014 Vienna
Телефон: +43 153115202594
Електронна поща: isk@bka.gv.at

2. DSA in the military sphere:
BMLVS/Abwehramt
Postfach 2000
1030 Vienna
Електронна поща: abwa@bmlvs.gv.at

ПОЛША

Internal Security Agency
Department for the Protection of Classified Information
Rakowiecka 2A
00-993 Warsaw
Телефон: +48 225857944
Факс: +48 225857443
Електронна поща: nsa@abw.gov.pl

ПОРТУГАЛИЯ

Gabinete Nacional de Segurança
Serviço de Segurança Industrial
Rua da Junqueira № 69
1300-342 Lisbon
Телефон: +351 213031710
Факс: +351 213031711
Електронна поща: sind@gns.gov.pt, franco@gns.gov.pt

РУМЪНИЯ

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS
Romanian NSA - ORNISS - National Registry Office for Classified Information
4th Mures Street
012275 Bucharest
Телефон: +40 212075115
Факс: +40 212245830
Електронна поща: relatii.publice@orniss.ro, nsa.romania@nsa.ro

СЛОВЕНИЯ

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Телефон: +386 14781390
Факс: +386 14781399
Електронна поща: gp.uvtp@gov.si

СЛОВАКИЯ

Národný bezpečnostný úrad
(National Security Authority)
Security Clearance Department
Budatínska 30
851 06 Bratislava
Телефон: +421 268691111
Факс: +421 268691700
Електронна поща: podatelna@nbu.gov.sk

ФИНЛАНДИЯ

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Електронна поща: NSA@formin.fi

ШВЕЦИЯ

1. National Security Authority
   Utrikesdepartementet (Ministry for Foreign Affairs)
   UD SÄK/NSA
   SE-103 39 Stockholm
   Телефон: +46 84051000
   Факс: +46 87231176
   Електронна поща: ud-nsa@gov.se

2. DSA
   Försvarets Materielverk (Swedish Defence Materiel Administration)
   FMV Säkerhetsskydd
   SE-115 88 Stockholm
   Телефон: +46 87824000
   Факс: +46 87826900
   Електронна поща: security@fmv.se

ОБЕДИНЕНО КРАЛСТВО

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Телефон: +44 2072765497, +44 2072765645
Електронна поща: UK-NSA@cabinet-office.x.gsi.gov.uk