

РЕШЕНИЕ НА СЪВЕТА

от 20 декември 2005 г.

относно изменение на Решение 2001/264/ЕО приемащо регламентите за
информационна сигурност на Съвета

(2005/952/ЕО)

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

Като взе предвид Договора за създаването на Европейската общност и по-специално третия параграф на член 207 от него,

Като взе предвид Решение 2004/338/ЕО, Евратом на Съвета от 22 март 2004 г., приемащо Процедурния правилник на Съвета¹ и по-специално Член 24 от него,

Като предвид, че:

- 1) Член 2, параграф 1 от Решение 2001/264/ЕО² предвижда, че Генералният секретар/Върховният представител, трябва да предприеме подходящи мерки, за да се осигури, че когато се разглежда класифицирана информация на ЕС, се спазват регламентите за сигурност на Съвета в рамките на Генералния секретариат на Съвета (ГСС) и *inter alia*, от външните изпълнители на ГСС.
- 2) Член 2, параграф 2 на Решение 2001/264/ЕО предвижда, че държавите членки трябва да вземат подходящи мерки, в съответствие с националните мерки, за да се осигури, че когато се разглежда класифицирана информация на ЕС, регламентите на Съвета за сигурност се спазват в рамките на техните служби и сгради, *inter alia*, от външните изпълнители на държавите членки.
- 3) Понастоящем Решение 2001/264/ЕС не включва елементи за това как неговите основни принципи и минимални стандарти трябва да се прилагат, където ГСС възлага с договор на външни субекти задачи, които включват, свързани са с и/или съдържат класифицирана информация на ЕС.
- 4) Затова е необходимо да се добавят специални общи минимални стандарти в тази връзка, към Решение 2001/264/ЕС.
- 5) Тези общи минимални стандарти трябва също да бъдат спазвани от държавите членки, за мерките, които трябва да бъдат взети, в съответствие с националните мерки, когато те възлагат с договор задачи, които включват, свързани са с и/или съдържат класифицирана информация на ЕС, на външни субекти, упоменати в Член 2, параграф 2 на Решение 2001/264/ЕО.

¹ ОВ L 106, 15.4.2004 г., стр. 22. Решение, както е изменено с Решение 2004/701/ЕС, Евратом (ОВ L 319, 20.10.2004 г., стр. 15).

² ОВ L 101, 11.4.2001 г., стр. 1. Решение, както е изменено последно с Решение 2005/571/ЕО (ОВ L 193, 23.7.2005 г., стр. 31).

б) Тези общи минимални стандарти трябва да се прилагат без да се нарушават релевантните актове, по-специално Директива 2004/18/ЕС³, Регламент (ЕС, Евратом) № 1605/2002⁴ и правилата за неговото прилагане и Споразумението за държавни поръчки (СДП) на СТО

РЕШИ:

Член 1

Към Част I, точка 8, на Приложението към Решение 2001/264/ЕО се добавя следното изречение:

„Такива минимални стандарти трябва също да включват минимални стандарти, които трябва да се прилагат, когато ГСС възлагат с договор задачи, които включват, свързани са с и/или съдържат класифицирана информация на ЕС, на промишлени или други икономически единици: тези общи минимални стандарти се съдържат в раздел XIII на част II.”

Текстът на приложението към настоящото решение, трябва да бъде добавен към раздел XIII на част II на Приложението към Решение 2001/264/ЕО.

Член 3

Настоящото решение влиза в сила в деня на неговото публикуване в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 20 декември 2005 година.

За Съвета
Председател
M. BECKETT

³ Директива 2004/18/ЕО на Европейския парламент и на Съвета от 31 март 2004 г. за координацията на процедурите за възлагане на договори за обществени поръчки за работи, договори за обществени поръчки за доставки и договори за обществени поръчки за услуги (ОВ L 134, 30.4.2004 г., стр. 114).

⁴ Регламент на Съвета (ЕО, Евратом) № 1605/2002 от 25 юни 2002 г. за Финансовия регламент, приложим за общия бюджет на Европейските общности (ОВ L 248, 16.9.2002 г., стр. 1).

ПРИЛОЖЕНИЕ

„РАЗДЕЛ XIII ОБЩИ МИНИМАЛНИ СТАНДАРТИ ЗА ПРОМИШЛЕНА СИГУРНОСТ

1. Този раздел разглежда аспектите, свързани със сигурността на промишлените дейности, които са единствени по рода си за договаряне и възлагане на договори, възлагащи задачи, които включват, свързани са и/или съдържат класифицирана информация на ЕС, и тяхното изпълнение от промишлени или други икономически единици, включително разгласяване на класифицирана информация на ЕС или достъп до такава по време на процедурата за възлагане на обществена поръчка (срок за подаване на оферти и преговорите преди сключването на договор).

ОПРЕДЕЛЕНИЯ

2. За целите на тези общи минимални стандарти, се прилагат определенията, дадени по-долу:

а) „Класифициран договор”: всеки договор за доставка на продукти, извършване на строителни работи или предоставяне на услуги, изпълнението на който изисква или включва достъп до на класифицирана информация на ЕС или генерирането на такава;

б) „Класифициран договор за подизпълнение”: договор, сключен от изпълнител с друг изпълнител (т.е. подизпълнител) за доставка на стоки, изпълнение на работи или предоставяне на услуги, изпълнението на който изисква или включва достъп до класифицирана информация на ЕС или генерирането на такава;

в) „Изпълнител”: физическо или юридическо лице с правоспособност да изпълнява договори;

г) „Назначен орган за информационна сигурност (НОИС)”: орган, отговарящ пред Националния орган за информационна сигурност на държава членка на ЕС, който отговаря за информирането на промишлени или други икономически единици за националната политика в областта на всички въпроси на промишлената сигурност и за предоставянето на указания и помощ при нейното прилагане. Функцията на Назначения орган по сигурността може да бъде изпълнявана от Националния орган по сигурността;

д) „Разрешително за информационна сигурност на съоръжение (РИСС)”: административно решение на Назначения орган по информационната сигурност/ Националния орган по информационната сигурност, че от гледна точка на информационната сигурност дадено съоръжение може да предостави адекватна защита на сигурността на класифицирана информация на ЕС на определено класификационно ниво на информационна сигурност и неговият персонал, който изисква достъп до класифицирана информация на ЕС има подходящото разрешение по отношение на информационната сигурност и е

инструктиран за съответните изисквания за информационна сигурност, необходими за достъпа и защитата на класифицираната информация на ЕС;

е) „Промислена или друг икономическа единица”: единица, занимаваща се с доставяне на стоки, извършване на строителни работи или предоставяне на услуги; като може да бъде промишлена, търговска, от сектора на услугите, научна, образователна и изследователска единица;

ж) „Промислена информационна сигурност”: прилагането на защитни мерки и процедури за предотвратяване, откриване или възстановяване от загуба или компрометирането на класифицирана информация на ЕС, разглеждана от изпълнител или подизпълнител в преговори преди сключване на договори и в договори;

з) „Национален орган по информационната сигурност”: Правителственият орган на държава членка на ЕС с главна отговорност за защитата на класифицирана информация на ЕС;

и) „Общо класификационно ниво на информационна сигурност на даден договор”: определяне на класификационно ниво на информационна сигурност на целия договор, въз основа на класификацията на информацията и/или материалите, които могат или трябва да бъдат или могат да бъдат генерирани, пускани или до които може да се осъществи достъп до който и да е елемент от цялостния договор. Общото класификационно ниво на информационна сигурност на даден договор не може да бъде по-ниско от най-високото класификационно ниво на който и да е от неговите елементи, но може да бъде по-високо поради съвкупния ефект;

й) „Клауза за аспектите, свързани с информационната сигурност”: набор от специални договорни условия, издадени от възложителя, който представлява неразделна част от даден класифициран договор, включващ достъп до или генериране на класифицирана информация на ЕС, който идентифицира изискванията за информационна сигурност или тези елементи на договора, които изискват защита на информационната сигурност.

к) „Наръчник за класификационното ниво на информационна сигурност”: документ, който описва елементите на програма или договор, които са класифицирани, определяйки приложимите класификационни нива на информационна сигурност. Наръчникът за класификационното ниво на информационна сигурност може да бъде разширяван през целия период на програмата или договора и елементите на информацията могат да бъдат прекласифицирани или да преминат в по-ниско ниво на информационна сигурност. Наръчникът за класификационното ниво на информационна сигурност трябва да бъде част от Клаузата за аспектите, свързани с информационната сигурност.

ОРГАНИЗАЦИЯ

3. Генералният секретариат на Съвета (ГСС) може да възложи с договор задачи, които включват, свързани са с и/или съдържат класифицирана информация на ЕС,

на промишлени или други икономически единици, регистрирани в дадена държава членка.

4. ГСС трябва да осигури спазването на всички изисквания, произтичащи от тези минимални стандарти, когато се възлагат класифицирани договори.

5. Всяка държава членка трябва да осигури нейният Национален орган за информационна сигурност да има подходящи структури за прилагане на тези минимални стандарти по промишлена сигурност. Те могат да включват един или повече назначени органи за информационна сигурност.

6. Главната отговорност за защита на класифицираната информация на ЕС в рамките на промишлените и други икономически единици се носи от тяхното ръководство.

7. Когато се възлага договор за изпълнение или договор за подизпълнение, който попада в обхвата на тези минимални стандарти ГСС и/или Националният орган за информационна сигурност/Назначеният орган за информационна сигурност, както е подходящо, незабавно уведомява Националния орган за информационна сигурност/Назначения орган за информационна сигурност на държавата членка, в която е регистриран изпълнителя или подизпълнителя.

КЛАСИФИЦИРАНИ ДОГОВОРИ

8. Класификационните нива на информационна сигурност на класифицираните договори трябва да вземат пред вид на следните принципи:

а) ГСС определя, както е подходящо, аспектите на договора, които изискват защита и последваща класификация за ниво на сигурност; когато прави това, ГСС трябва да вземе пред вид първоначалното класификационно ниво на информационна сигурност, определено от създателя на информацията, генерирана преди възлагането на договора.

б) общото класификационно ниво на информационна сигурност на договора не може да бъде по-ниско от най-високото класификационно ниво на който и да е от неговите елементи;

в) Класифицираната информация на ЕС, генерирана по договорни дейности се класифицира съгласно Наръчника за класификационното ниво на информационна сигурност;

г) Когато е подходящо, ГСС отговаря за промяната на общото класификационно ниво на информационна сигурност на договора, или на класификационното ниво на информационна сигурност на който и да е от неговите елементи, в консултация със създателя на информацията и за информирането на всички заинтересовани страни,

д) Класифицираната информация, дадена на изпълнителя или подизпълнителя или генерирана по договорна дейност не трябва да се използва за цели, различни от тези, определени от класифицирания договор и

не трябва да бъде оповестявана на трети страни без предварителното писмено съгласие на нейния създател.

9. Националните органи за информационна сигурност/Назначените органи за информационна сигурност на държавите членка отговарят за осигуряването на вземането на всички подходящи мерки от изпълнителите и подизпълнителите, на които са възложени класифицирани договори, обхващащи информация, класифицирана като CONFIDENTIEL UE или SECRET UE, за опазването на такава ЕС класифицирана информация, дадена на тях или генерирана от тях при изпълнението на класифицирания договор съгласно националните закони и регламенти. Неспазването на изискванията за сигурност може да доведе до прекратяване на договора.

10. Всички промишлени и други икономически единици, участващи в класифицирани договори, които включват достъп до информация, класифицирана като CONFIDENTIEL UE или SECRET UE, трябва да притежават „Разрешително за информационна сигурност на съоръжение” (РИСС) на национално ниво. РИСС се дава от Националния орган за информационна сигурност/Назначения орган за информационна сигурност на държавата членка, за да потвърди, че съоръжението може да предостави и гарантира адекватна защита на сигурността на класифицирана информация на ЕС на подходящото класификационно ниво на информационна сигурност.

11. Националният орган за информационна сигурност/Назначеният орган за информационна сигурност отговаря за даването в съответствие с неговите национални регламенти, на Разрешение за информационна сигурност на персонала (РИСП) на всички лица, наети в промишлени или други икономически единици, регистрирани в тази държава членка, чийто задължения изискват достъп до информация на ЕС, класифицирана като CONFIDENTIEL UE или SECRET UE, предмет на класифициран договор.

12. Класифицираните договори трябва да съдържат „Клауза за аспектите, свързани с информационната сигурност”, както е определено в точка 2, буква й). Клаузата за аспектите, свързани с информационната сигурност трябва да предвижда „Наръчник за класификационното ниво на информационна сигурност”.

13. Преди започването на преговорите по даден класифициран договор, ГСС се свързва с Националния орган за информационна сигурност/Назначения орган за информационна сигурност на държавите членки, в които са регистрирани съответните промишлени или други икономически единици, за да получи информация, че те притежават валиден РИСС, подходящ за класификационното ниво на информационна сигурност на договора.

14. Възложителят не трябва да сключва класифициран договор с предпочитан участник в търга, преди да е получил валиден сертификат РИСС.

15. Освен ако не се изисква от националните закони и регламенти на държавите членки, РИСС не се изисква за договори, съдържащи информация, класифицирана RESTREINT UE.

16. В случай на търгове във връзка с класифицирани договори, поканите за участие трябва да съдържат условие, изискващо участникът в търга, който не представи оферта или който не е избран, да върне всички документи в рамките на определен период от време.

17. Може да се наложи даден изпълнител да преговора за сключване класифицирани договори за подизпълнение с подизпълнители на различни нива. Изпълнителят трябва да осигури, че всички дейности по сключване на договора за подизпълнение се изпълняват в съответствие с общите минимални стандарти, предвидени в настоящия раздел. Изпълнителят обаче, не трябва да предава класифицирана информация или материали ЕС на даден подизпълнител, без предварителното писмено съгласие на техния създател.

18. Условието, при които изпълнителят може да възлага договор за подизпълнение, трябва да бъдат определени в търга и в договора. Договор за подизпълнение не може да бъде възлаган на икономически единици, които са регистрирани в държави, които не са членки на ЕС, без изричното писмено разрешение на ГСС.

19. През целия период на договора, спазването на всички негови разпоредби, свързани с информационната сигурност, се следят от съответните национални органи за информационна сигурност/Назначени органи за информационна сигурност, съгласувано с ГСС. Уведомяването за инциденти във връзка с информационната сигурност трябва да става в съответствие с разпоредбите, предвидени в Част II, Раздел X на тези регламенти за информационната сигурност. Промяната или отмяната на РИСС трябва незабавно да бъде съобщавана на ГСС и на всеки Национален орган за информационна сигурност/Назначен орган за информационна сигурност, който е бил уведомен за РИСС.

20. Когато даден класифициран договор за изпълнение или класифициран договор за подизпълнение се прекратява, ГСС и/или Националният орган за информационна сигурност/Назначения орган за информационна сигурност, както е уместно, надлежно нотифицира Националния орган за информационна сигурност/Назначения орган за информационна сигурност на държавите членки, в които е регистриран изпълнителя или подизпълнителя.

21. Общите минимални стандарти, предвидени в този Раздел, трябва да продължат да бъдат спазвани и поверителността на класифицираната информация трябва да се поддържа от изпълнителите и подизпълнителите след прекратяването и приключването на класифицирания договор за изпълнение или договор за подизпълнение.

22. Специални разпоредби за освобождаването от класифицирана информация в края на договора се предвиждат в Клаузата за аспектите, свързани с информационната сигурност или в други имащи отношение разпоредби, определящи изискванията за информационна сигурност.

ПОСЕЩЕНИЯ

23. Посещения на служители на ГСС в промишлени или други икономически единици в държави-членки, изпълняващи класифицирани договори, трябва да бъдат организирани със съответния Национален орган за информационна сигурност/Назначен орган за информационна сигурност. Посещенията от служители на промишлени или други икономически единици в рамките на класифициран договор ЕС трябва да бъдат организирани между съответните Националните органи за информационна сигурност/Назначените органи за информационна сигурност. Националните органи за информационна сигурност/Назначените органи, участващи в класифициран договор ЕС може да се споразумеят за процедура, с която посещенията на служителите на промишлени или друг икономически единици могат да бъдат организирани директно.

ПРЕДАВАНЕ И ТРАНСПОРТИРАНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

24. По отношение на предаването на класифицирана информация на ЕС, трябва да се прилагат разпоредбите на Част VII, Глава II и когато е подходящо – тези на Раздел XI на Регламентите за информационна сигурност. За да се допълнят такива разпоредби, се прилагат всякакви съществуващи процедури, които са в сила между държавите членки.

25. Международният транспорт на класифициран материал на ЕС, свързан с класифицирани договори, се извършва съгласно националните процедури на държавите членки. Следните принципи се прилагат, когато се проучват мерките за информационна сигурност за международния транспорт:

- а) информационната сигурност се осигурява на всички етапи по време на транспорта и при всички обстоятелства, от пункта на произход до крайното местоназначение;
- б) степента на защита, дадена на дадена пратка се определя от най-високото класификационно ниво на информационна сигурност на материала, който се съдържа в нея;
- в) когато е подходящо, за фирмите, предоставящи транспорт се получава Разрешително за информационна сигурност на съоръжение. В подобни случаи, персоналът, обработващ пратката, трябва да има документ, за съответното ниво на информационна сигурност в съответствие с общите минимални стандарти, предвидени в този раздел;
- г) пътуванията се извършват от пункт до пункт, доколкото е възможно и се приключват колкото е възможно по-бързо, доколкото позволяват обстоятелствата;
- д) когато е възможно, маршрутите трябва да бъдат само през държави-членки на ЕС. Маршрути през държави, които не са членки на ЕС трябва да се използват само когато са оторизирани от Националния орган за

информационна сигурност/Назначения орган за информационна сигурност на държавите както на изпращача, така и на получателя;

е) преди всякакво движение на класифициран материал на ЕС, трябва да бъде изготвен транспортен план от изпращача и същият следва да бъде одобрен от съответните Национални органи за информационна сигурност/Назначени органи за информационна сигурност.”