РЕШЕНИЕ (ЕС, Евратом) 2018/559 НА КОМИСИЯТА

от 6 април 2018 година

относно установяване на правилата за прилагане на член 6 от Решение (ЕС, Евратом) 2017/46 на Комисията относно сигурността на комуникационните и информационните системи в Европейската комисия

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,

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 ([1]), и по-специално член 6 от него,

като има предвид, че:

(1) С приемането на Решение (ЕС, Евратом) 2017/46 се създаде необходимост Комисията да преразгледа, актуализира и консолидира правилата за прилагане, свързани с отменения Решение C(2006) 3602 на Комисията относно сигурността на комуникационните и информационните системи, използвани от Комисията.

(2) Членът на Комисията, отговарящ за сигурността, в пълно съответствие с вътрешния процедурен правилник, бе оправомощен да установи правила за прилагане в съответствие с член 13 от Решение (ЕС, Евратом) 2017/46 ([2]).

(3) Следователно правилата за прилагане на Комисията, които се съдържат в Решение C(2006) 3602, следва да бъдат отменени,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

ГЛАВА 1

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и обхват

1. Предметът и обхватът на настоящото решение са определени в член 1 от Решение (ЕС, Евратом) 2017/46.

2. Разпоредбите на настоящото решение се прилагат за всички комуникационни и информационни системи (КИС). Въпреки това отговорностите, определени в настоящото решение, не се прилагат по отношение на КИС, обработващи класифицирана информация на ЕС. Съответните отговорности за тези системи се определят от собственика на системата и от органа по сигурността на Комисията в съответствие с Решение (ЕС, Евратом) 2015/444 на Комисията ([3]).

3. В глава 2 от настоящото решение е направен преглед на практическото прилагане на организацията и отговорностите, свързани с информационната сигурност. В глава 3 от настоящото решение е направен преглед на процесите, свързани с член 6 от Решение (ЕС, Евратом) 2017/46.

Член 2

Определения

Определенията в член 2 от Решение (ЕС, Евратом) 2017/46 се прилагат към настоящото решение. За целите на настоящото решение се прилагат също следните определения:

1. „Орган за криптографско одобрение“ (ОКО) е функция, поета от органа по сигурността на Комисията, която попада под ръководството на генералния директор на ГД „Човешки ресурси и сигурност“;

([1]) ОВ L 6, 11.1.2017 г., стр. 40.
([2]) Решение C(2017)7428 на Комисията от 8 ноември 2017 г. за предоставяне на правомощия за приемането на правила за прилагане, стандарти и насоки по отношение на сигурността на комуникационните и информационните системи в Европейската комисия.
([3]) Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 година относно правилата за сигурност за защита на класифицираната информация на ЕС (ОВ L 72, 17.3.2015 г., стр. 53).

2. „Външна мрежова връзка“ означава електронна съобщителна връзка между вътрешната мрежа на Комисията и всяка друга мрежа, включително интернет. Това определение изключва мрежи на трети страни, предоставяни по договор като част от вътрешната мрежа на Комисията.

3. „Доверително съхранение (ескроу) на ключове“ означава процедура за съхраняване на копия на криптографски ключове при една или повече отделни страни, като се осигурява разделяне на задълженията, за да се даде възможност за възстановяване на ключовете в случай на загуба на оперативното копие. Ключовете може да бъдат разделени на две или повече части, като всяка една от тях се предоставя на различна страна, за да се гарантира, че нито една страна не притежава целия ключ.

4. „RASCI“ е съкращение за разпределяне на отговорност въз основа на следните индикатори за възлагане:

а) „отговорен“ (responsible (R) означава да има задължението да извършва действия и да взема решения за постигането на необходимите резултати;

б) „подотчетен“ (accountable (A) означава да отговаря за действия, решения и постигнати резултати;

в) „подкрепящ“ (supports (S) означава да има задължението да работи с лицето, отговорно да изпълни задачата;

г) „консултиран“ (consulted (C) означава да е търсен за съвет или становище;

д) „информиран“ (informed (I) означава редовно да е снабдяван с релевантна актуализирана информация.

ГЛАВА 2

ОРГАНИЗАЦИЯ И ОТГОВОРНОСТИ

Член 3

Функции и отговорности

Функциите и отговорностите, свързани с членове 4—8 от настоящото решение, са определени в приложението в съответствие с модела RASCI.

Член 4

Привеждане в съответствие с политиката на Комисията за информационна сигурност

1. Генерална дирекция „Човешки ресурси и сигурност“ прави преглед на политиката за информационна сигурност на Комисията и свързаните с нея стандарти и насоки, за да се гарантира, че те са в съответствие с общите политики за сигурност на Комисията, и по-специално с Решение (ЕС, Евратом) 2015/443 на Комисията ([1]) и Решение (ЕС, Евратом) 2015/444.

2. При поискване от други служби на Комисията, генерална дирекция „Човешки ресурси и сигурност“ може да направи преглед на техните политики за информационна сигурност или друга документация, свързана с информационната сигурност, за да осигури съответствието им с политиката за информационна сигурност на Комисията. Началникът на съответната служба на Комисията е длъжен да гарантира, че всички несъответствия са отстранени.

3. В рамките на задълженията си в областта на сигурността на информацията генерална дирекция „Човешки ресурси и сигурност“ си сътрудничи с генерална дирекция „Информатика“, за да гарантира, че процесите на информационна сигурност отчитат в пълна степен класификацията и принципите на сигурността, установени в Решение (ЕС, Евратом) 2015/443, и по-специално членове 3 и 9 от него.

ГЛАВА 3

ПРОЦЕСИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Член 5

Криптографски технологии

1. Използването на криптографски технологии за защита на класифицираната информация на Европейския съюз (КИЕС) трябва да е в съответствие с Решение (ЕС, Евратом) 2015/444.

2. Решенията относно използването на криптографски технологии за защитата на некласифицирана информация се вземат от собственика на всяка КИС, като се вземат предвид както рисковете, които трябва да бъдат смекчени чрез криптирането, така и рисковете, които то поражда.

3. Предварително одобрение от Органа за криптографско одобрение (ОКО) се изисква за всяка употреба на криптографски технологии, освен ако криптирането се използва само за да се защити поверителността на некласифицираната информация при нейното предаване и се използват стандартни мрежови съобщителни протоколи.

([1]) Решение (ЕС, Евратом) 2015/443 на Комисията от 13 март 2015 година относно сигурността в Комисията (ОВ L 72, 17.3.2015 г., стр. 41).

4. С изключението, посочено в параграф 3 от настоящия член, Службите на Комисията осигуряват доверително съхранение (ескроу) на резервни копия от ключовете за декриптиране за целите на възстановяването на съхраняваните данни, в случай че ключовете за декриптиране не са достъпни. Възстановяването на криптирани данни посредством резервни копия на ключовете за декриптиране се извършва само с разрешение, предоставено в съответствие със стандарта, определен от ОКО.

5. Исканията за одобрение за използването на криптографски технологии се документират официално и в тях се включва подробна информация за КИС и информацията, които следва да бъдат защитени, технологиите, които се използват, и свързаните с тях оперативни процедури за сигурност. Тези искания за одобрение се подписват от собственика на системата.

6. Исканията за одобрение за използването на криптографски технологии се оценяват от ОКО в съответствие с публикуваните стандарти и изисквания.

Член 6

Проверки на информационната сигурност

1. Генерална дирекция „Човешки ресурси и сигурност“ извършва проверки на информационната сигурност, за да провери дали мерките за информационна сигурност са в съответствие с политиките на Комисията в тази област и да провери интегритета на тези мерки за контрол.

2. Генерална дирекция „Човешки ресурси и сигурност“ може да извърши проверка на информационната сигурност:

а) по собствена инициатива;

б) по искане на Управителния съвет за информационна сигурност (УСИС);

в) по искане, получено от собственик на система;

г) вследствие на инцидент, свързан със сигурността; или

д) след установяването на висока степен на риск за дадена система.

3. Собствениците на данни могат да поискат проверка на информационната сигурност, преди да съхранят своята информация в КИС.

4. Резултатите от проверката трябва да бъдат документирани в официален доклад, предназначен за собственика на системата, с копие до ЛСИС, в който се съдържат констатации и препоръки за подобряване на съответствието на КИС с политиката за информационна сигурност. Генерална дирекция „Човешки ресурси и сигурност“ докладва за значителни проблеми и препоръки на Управителния съвет по информационна сигурност (УСИС).

5. Генерална дирекция „Човешки ресурси и сигурност“ следи изпълнението на препоръките.

6. Когато е целесъобразно, проверките на информационната сигурност включват инспектирането на услуги, помещения и оборудване, предоставени на собственика на системата, като това може да са вътрешни или външни доставчици на услуги.

Член 7

Достъп от външни мрежи

1. Генерална дирекция „Човешки ресурси и сигурност“ определя правилата за разрешаване на достъп между КИС на Комисията и външни мрежи под формата на стандарт.

2. В правилата трябва да се прави разлика между различните видове външни мрежови връзки и да се установят подходящи правила за сигурност за всеки вид връзка, включително дали се изисква предварително разрешение за връзка от съответния орган, както е посочено в параграф 4 от настоящия член.

3. Ако се изисква разрешение, то се издава въз основа на официален процес за искане и получаване на одобрение. Одобрението е валидно за определен срок и се получава преди активирането на връзката.

4. Генерална дирекция „Човешки ресурси и сигурност“ носи общата отговорност за одобряването на исканията, но може по своя преценка да делегира отговорността за одобряването на някои видове връзки в съответствие с член 17, параграф 3 от Решение (ЕС, Евратом) 2015/443 и при спазване на условията, определени съгласно параграф 8 от настоящия член.

5. Одобряващият орган може да наложи допълнителни изисквания за сигурност като предварително условие за получаването на одобрение, за да се защитят КИС и мрежите на Комисията от рисковете, свързани с неразрешен достъп или други нарушения на сигурността.

6. Генерална дирекция „Информатика“ е стандартният доставчик на мрежови услуги за Комисията. Всяка друга служба на Комисията, експлоатираща мрежа, която не е предоставена от генерална дирекция „Информатика“, трябва първо да получи съгласието на УСИС. Службата на Комисията следва да документира оперативната обосновка за искането и да демонстрира, че контролът на мрежата е достатъчен, за да отговори на изискванията за контрол на входящите и изходящи потоци от информация.

7. Собственикът на КИС определя изискванията за сигурност за външен достъп до тази КИС и с подкрепата на ЛСИС гарантира прилагането на подходящи мерки за защита на нейната сигурност.

8. Мерките за сигурност, които се прилагат за външни мрежови връзки, се основават на принципите „необходимост да се знае“ и „най-малко привилегии“, които гарантират, че лицата получават само информацията и правата на достъп, които са им нужни, за да изпълняват служебните си задължения към Комисията.

9. Всички външни мрежови връзки се филтрират и наблюдават с цел откриване на евентуални пробиви в сигурността.

10. Когато връзките са създават, за да се даде възможност дадена КИС да бъде възложена на външни изпълнители, разрешението ще зависи от успешното приключване на процедурата, описана в член 8.

Член 8

Възлагане на КИС на външни изпълнители

1. За целите на настоящото решение за дадена КИС се счита, че е възложена на външен изпълнител, когато тя се предоставя въз основа на договор с трета страна изпълнител, съгласно който КИС се намира в помещения, които са извън Комисията. Това включва възлагането на външен изпълнител на една или няколко КИС или други информационни услуги, центрове за електронно обработване на данни в помещения извън Комисията, и обработката на масиви от данни на Комисията от външни изпълнители.

2. Възлагането на външни изпълнители на дадена КИС отчита чувствителността или класификацията на обработваната информация, както следва:

а) КИС, които работят с КИЕС, се акредитират в съответствие с Решение (ЕС, Евратом) 2015/444, като предварително трябва да се извърши консултация с органа по акредитиране на сигурността на Комисията (ОАС). Системите, обработващи КИЕС, не се възлагат на външни изпълнители.

б) Собственикът на КИС, която обработва некласифицирана информация, въвежда пропорционални мерки за посрещане на свързаните със сигурността нужди в съответствие с приложимите правни задължения или чувствителността на информацията, като взима предвид рисковете, свързани с възлагането на дейности на външни доставчици. Генерална дирекция „Човешки ресурси и сигурност“ може да наложи допълнителни изисквания.

в) При възложените на външни изпълнители проекти за разработка се взема предвид чувствителността на разработения код и всички данни от изпитванията, използвани по време на разработката.

3. Следните принципи се прилагат за възложените на външни изпълнители КИС в допълнение към тези, посочени в член 3 от Решение (ЕС, Евратом) 2017/46:

а) договореностите за възлагане на изпълнението се изготвят така, че да се избегне зависимост от определени доставчици;

б) възлагането на външни изпълнители на дейности, свързани със сигурността, се извършва по начин, свеждащ до минимум възможностите за персонала на трети страни да разполага с достъп до информация на Комисията или да извършва промени в нея;

в) персоналът на трети страни, който има достъп до възложени на външни изпълнители КИС, подписва споразумения за поверителност;

г) възлагането на външни изпълнители на дадена КИС се посочва в инвентарния опис на комуникационните и информационни системи.

4. С участието на собственика на данните собственикът на системата:

а) оценява и документира рисковете, свързани с възлагането на външен изпълнител;

б) определя съответните изисквания за сигурност;

в) консултира се със собствениците на всички други свързани КИС, за да гарантира, че са включени и техните изисквания за сигурност;

г) гарантира въвеждането в договора за възлагане на външен изпълнител на подходящи права и изисквания за сигурност;

д) изпълнява всички други изисквания, определени в подробната процедура, посочена в параграф 8 от настоящия член.

Тези действия трябва да бъдат завършени преди подписването на договора или друго споразумение за възлагане на външни изпълнители на една или повече КИС.

5. Собствениците на системи управляват рисковете, свързани с възлагането на дейности на външни изпълнители, през целия жизнен цикъл на КИС, за да отговорят на установените изисквания за сигурност.

6. Собствениците на системи гарантират, че третите страни — изпълнители, са задължени да информират незабавно Комисията за всички инциденти, свързани с информационната сигурност, които засягат КИС на Комисията, възложена на външен изпълнител.

7. Собственикът на система отговаря за осигуряване на съответствието на КИС, договора за възлагане на външен изпълнител и договореностите за сигурност с правилата на Комисията по отношение на информационната сигурност и сигурността на информационните системи.

8. В съответствие с член 10 по-долу генерална дирекция „Човешки ресурси и сигурност“ установява подробен стандарт, свързан с отговорностите и дейностите, посочени в точки 1 — 7.

ГЛАВА 4

РАЗНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 9

Прозрачност

Настоящото решение се довежда до вниманието на служителите на Комисията и на всички лица, за които то се прилага, и се публикува в *Официален вестник на Европейския съюз*.

Член 10

Стандарти

1. Разпоредбите на настоящото решение при необходимост се доразвиват в стандарти и/или насоки, които се приемат в съответствие с Решение (ЕС, Евратом) 2017/46 и с Решение C(2017) 7428. Стандартите и насоките за информационна сигурност предоставят допълнителни подробности относно тези правила за прилагане и Решение (ЕС, Евратом) 2017/46 за специфични области на сигурност съгласно стандарт ISO 27001:2013, приложение А. Тези стандарти и насоки се основават на най-добрите практики в отрасъла и са подбрани така, че да отговарят на информационната среда на Комисията.

2. При необходимост стандартите се разработват в съответствие със стандарт ISO 27001:2013, приложение А, в следните области:

1) организация на информационната сигурност;

2) сигурност на човешките ресурси;

3) управление на активи;

4) контрол на достъпа;

5) криптография;

6) физическа сигурност и сигурност на средата;

7) оперативна сигурност;

8) сигурност на комуникациите;

9) придобиване, разработка и поддръжка на системи;

10) отношения с доставчиците;

11) управление на инцидентите, свързани със сигурността на информацията;

12) аспекти на информационната сигурност при управлението на непрекъснатостта на дейностите;

13) съответствие.

3. УСИС одобрява стандартите, упоменати в параграфи 1 и 2 от настоящия член, преди те да бъдат приети.

4. Правилата за прилагане на Решение C(2006) 3602, свързани с приложното поле на настоящото решение, се отменят.

5. Стандартите и насоките, приети съгласно Решение C(2006) 3602 от 16 август 2006 г., остават в сила, доколкото не противоречат на настоящите правила за прилагане, докато не бъдат отменени или заменени със стандарти или насоки, които да бъдат приети съгласно член 13 от Решение (ЕС, Евратом) 2017/46.

Член 11

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 6 април 2018 година.

За Комисията,
от името на председателя,
Günther OETTINGER
Член на Комисията

ПРИЛОЖЕНИЕ

ФУНКЦИИ И ОТГОВОРНОСТИ (RASCI)

Моделът RASCI разпределя функции, използвайки следните съкращения:

а) R — отговорен

б) A — подотчетен

в) S — подкрепящ

г) C — консултиран

д) I — информиран

Функция / Процес	УСИС	ГД „Човешки ресурси“ (дирекция „Сигурност“)	Служби на Комисията	Собственик на система	Собственик на данни	ЛСИС	ГД „Информатика“	Изпълнители
Привеждане в съответствие с политиката на Комисията за сигурност на информацията		**R/A**	**S**				**S**	
Криптографски технологии		**C**	**A**	**R**	**I**	**C**		
Проверки на информационната сигурност	**I**	**A/R**		**S**	**I**	**I**	**S**	
Достъп от външни мрежи	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Възлагане на КИС на външни изпълнители		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] УСИС бива консултиран във връзка с функционирането на вътрешните мрежи от служби на Комисията, различни от генерална дирекция „Информатика“.

[2] Собственикът на КИС, която е възложена на външен изпълнител, е отговорен, а собственикът на всяка друга КИС, с която възложена на външен изпълнител КИС е свързана, бива консултиран.