II

*(Съобщения)*

# СЪОБЩЕНИЯ НА ИНСТИТУЦИИТЕ, ОРГАНИТЕ, СЛУЖБИТЕ И АГЕНЦИИТЕ НА ЕВРОПЕЙСКИЯ СЪЮЗ

# ЕВРОПЕЙСКИ ПАРЛАМЕНТ

## РЕШЕНИЕ НА БЮРОТО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

**от 15 април 2013 г.**

**относно правилника относно обработката на поверителна информация от Европейския парламент**

(2014/C 96/01)

БЮРОТО НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ,

като взе предвид член 23, параграф 12 от Правилника за дейността на Европейския парламент,

като има предвид, че:

(1) С оглед на Рамково споразумение за отношенията между Европейския парламент и Европейската комисия ([1]), подписано на 20 октомври 2010 г. (наричано по-долу „Рамково споразумение“), и на Междуинституционалното споразумение между Европейския парламент и Съвета относно изпращането на Европейския парламент и обработването от него на класифицирана информация, с която Съветът разполага по въпроси, които не са от областта на общата външна политика и политика на сигурност ([2]), подписано на 12 март 2014 г., (наричано по-долу „Междуинституционално споразумение“), е необходимо да се определят конкретни правила относно обработването на поверителна информация от Европейския парламент.

(2) Договорът от Лисабон предоставя нови правомощия на Европейския парламент и с цел развитие на дейностите на Парламента в областите, които изискват известна степен на поверителност, е необходимо да се установят основни принципи, минимални стандарти на сигурност и подходящи процедури за обработката на поверителна, в това число на класифицирана информация, от Европейския парламент.

(3) Правилникът, установен с настоящото решение, цели да се гарантират стандарти на защита и съвместимост, които са равностойни на правилата, приети от други институции, органи, служби и агенции, учредени по силата или на основание на Договорите, или от държавите членки, с оглед улесняване на гладкото протичане на процеса на вземане на решения в Европейския съюз.

(4) Разпоредбите на настоящото решение се приемат, без да се засягат разпоредбите на настоящите и бъдещите правила относно достъпа до документи, приети в съответствие с член 15 от Договора за функционирането на Европейския съюз (ДФЕС).

([1]) ОВ L 304, 20.11.2010 г., стр. 47.
([2]) ОВ C 95, 1.4.2014 г., стр. 1.

(5) Разпоредбите на настоящото решение се приемат, без да се засягат разпоредбите на настоящите и бъдещите правила относно защитата на личните данни, приети в съответствие с член 16 от ДФЕС,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

*Член 1*

**Цел**

Настоящото решение урежда управлението и обработката на поверителна информация от Европейския парламент, включително създаването, получаването, предаването и съхраняването на такава информация с оглед подходящата защита на нейния поверителен характер. Решението е в прилагане на Междуинституционалното споразумение и на Рамковото споразумение, и по-специално на приложение II от последното.

*Член 2*

**Определения**

За целите на настоящото решение:

а) „информация“ означава всяка писмена или устна информация, независимо от носителя и автора;

б) „поверителна информация“ означава „класифицирана информация“ и некласифицирана „друга поверителна информация“;

в) „класифицирана информация“ означава „класифицирана информация на ЕС“ и „еквивалентна класифицирана информация“;

г) „класифицирана информация на ЕС“ (EUCI) означава всяка информация и материали, класифицирани като „TRÈS SECRET UE/EU TOP SECRET“ („СТРОГО СЕКРЕТНО ЕС“), „SECRET UE/EU SECRET“ („СЕКРЕТНО ЕС“), „CONFIDENTIEL UE/EU CONFIDENTIAL“ („ПОВЕРИТЕЛНО ЕС“) или „RESTREINT UE/EU RESTRICTED“ („ЗА СЛУЖЕБНО ПОЛЗВАНЕ ЕС“), чието неразрешено разкриване би могло или не да накърни в различни степени интересите на Съюза или на една или повече от неговите държави членки, независимо дали подобна информация произхожда от институции, органи, служби и агенции, създадени по силата и въз основа на Договорите. В тази връзка информацията, класифицирана като степен:

— „TRÈS SECRET UE/EU TOP SECRET“ е класифициране на информация и материал, неразрешеното разкриване на които би причинило изключително тежко накърняване на основополагащите интереси на Съюза или на една или повече държави членки,

— „SECRET UE/EU SECRET“ е информация и материал, неразрешеното разкриване на които би навредило сериозно на основополагащите интереси на Съюза или на една или повече държави членки;

— „CONFIDENTIEL UE/EU CONFIDENTIAL“ е информация и материал, неразрешеното разкриване на които би навредило на основополагащите интереси на Съюза или на една или повече държави членки;

— „RESTREINT UE/EU RESTRICTED“ е класифициране на информация и материал, неразрешеното разкриване на които би се отразило неблагоприятно на интересите на Съюза или на една или повече държави членки;

д) „еквивалентна класифицирана информация“ означава класифицирана информация от държави членки, трети държави или международни организации, която е обозначена с маркировка за сигурност, която е еквивалентна на маркировките за сигурност, използвани за класифицирана информация на ЕС, и която е била предоставена на Европейския парламент от Съвета или Комисията;

е) „друга поверителна информация“ означава всяка друга некласифицирана поверителна информация, включително информация, обхваната от разпоредбите за защита на личните данни или от задължението за професионална тайна, която е създадена в Европейския парламент или е предадена на Европейския парламент от други институции, органи, служби и агенции, създадени по силата и въз основа на Договорите или от държави членки;

ж) „документ“ означава всяка записана информация независимо от формата, под която се материализира, или нейните характеристики;

з) „материал“ означава всеки документ или елемент от съоръжение или оборудване, който е произведен или е в процес на производство;

и) „необходимост да се знае“ означава необходимостта на дадено лице да има достъп до поверителна информация, така че да бъде в състояние да изпълни официалната си функция или задача;

й) „разрешение“ означава решение, прието от председателя, ако засяга членове на Европейския парламент, или от генералния секретар, ако засяга длъжностни лица на Европейския парламент и други служители на Европейския парламент, които работят за политически групи, за предоставяне на индивидуален достъп до класифицирана информация до определено ниво въз основа на положителен резултат от проверка (проучване) за надеждност, извършена от национален орган съгласно националното законодателство и разпоредбите, установени в приложение I, част 2;

к) „понижаване на класификацията“ означава понижаване на нивото на класификация;

л) „премахване на класификацията“ означава премахване на всички нива на класификация;

м) „маркировка“ означава знак, положен върху „друга поверителна информация“, чиято цел е да се посочат предварително определени специални инструкции относно нейната обработка или областта, обхваната от даден документ; маркировка може да бъде положена върху класифицирана информация, за да се наложат допълнителни изисквания за нейното обработване;

н) „снемане на маркировка“ означава премахване на всякакви маркировки;

о) „създател на информацията“ означава надлежно оправомощен автор на поверителна информация;

п) „насоки за сигурност“ означава мерки по прилагане, така както са установени в приложение II;

р) „инструкции за обработка“ означава технически инструкции, издадени за службите на Парламента във връзка с управлението на поверителна информация.

*Член 3*

**Основни принципи и минимални стандарти**

1. Обработката на поверителна информация от Европейския парламент следва основните принципи и минималните стандарти, предвидени в приложение I, част 1.

2. Европейският парламент създава система за управление на сигурността на информацията (СУСИ) в съответствие с основните принципи и минималните стандарти. СУСИ се състои от насоките за сигурност, инструкциите за обработка и приложимите членове от Правилника за дейността. СУСИ има за цел улесняване на парламентарната и административната работа, като същевременно се гарантира защитата на всяка поверителна информация, обработвана от Европейския парламент, при пълно спазване на правилата, установени от създателя на такава информация, както е предвидено в насоките за сигурност. СУСИ

Обработката на поверителна информация посредством автоматизирани и комуникационни и информационни системи (КИС) на Европейския парламент се осъществява в съответствие с понятието за осигуреност на информацията (ОИ) съгласно предвиденото в насока за сигурност 3.

3. Членовете на Европейския парламент могат да правят справки с класифицирана информация включително до ниво „RESTREINT UE/EU RESTRICTED“, без да са били подложени на проверка за надеждност.

4. Когато съответната информация е класифицирана с ниво „CONFIDENTIEL UE/EU CONFIDENTIAL“ или с еквивалентно ниво, достъп до нея се предоставя на тези членове на Европейския парламент, на които е било предоставено разрешение от председателя съгласно параграф 5, или след подписване от тяхна страна на клетвена декларация за неразкриване на съдържанието на тази информация на трети лица, за спазване на задължението за защита на информацията, класифицирана с ниво „CONFIDENTIEL UE/EU CONFIDENTIAL“, и за това, че са запознати с последиците, ако не изпълнят тези изисквания.

5. Когато съответната информация е класифицирана с ниво „SECRET UE/EU SECRET“ или „TRÈS SECRET/EU TOP SECRET“ или с еквивалентно ниво, достъп до нея се предоставя на тези членове на Европейския парламент, на които е било предоставено разрешение от председателя, след като:

а) са били подложени на проверка за надеждност в съответствие с приложение I, част 2 от настоящото решение или

б) е било получено уведомление от компетентен национален орган, че съответните членове са били надлежно оправомощени по силата на техните функции в съответствие с националното право.

6. Преди да им бъде предоставен достъп до класифицирана информация, членовете на Европейския парламент биват информирани за задължението си да опазват такава информация и декларират, че са запознати с това задължение в съответствие с приложение I. Те биват информирани също така и за средствата за осигуряване на защитата на информацията.

7. Длъжностните лица на Европейския парламент и другите служители на Парламента, които работят за политически групи, могат да ползват поверителна информация за справка, ако имат установена „необходимост да знаят“, и могат да ползват класифицирана информация с ниво, по-високо от „RESTREINT UE/EU RESTRICTED“, за справка, ако са били подложени на подходящо равнище на проверка за надеждност. Достъп до класифицирана информация се предоставя единствено, ако те са били информирани и са получили писмени инструкции относно своите отговорности по отношение опазването на такава информация, както и относно средствата за осигуряване на защита на информацията, а също така и ако те са подписали декларация за това, че са получили тези инструкции и се ангажират да ги спазват в съответствие с настоящите правила.

*Член 4*

**Създаване на поверителна информация и административна обработка от Европейския парламент**

1. Председателят на Европейския парламент, председателите на съответните парламентарни комисии и генералният секретар и/или друго лице, надлежно оправомощено от него в писмен вид, могат да създават поверителна информация и/или класифицирана информация съгласно предвиденото в насоките за сигурност.

2. При създаване на класифицирана информация създателят на информация прилага подходящото ниво на класификация в съответствие с международните стандарти и определенията, посочени в приложение I. Създателят определя също така по правило адресатите, които следва да бъдат оправомощени да ползват информацията за справка в съответствие с нивото на класификация. Информацията се предава на Отдела за класифицирана информация (ОКИ), когато документът е депозиран в тази служба.

3. Друга поверителна информация, обхваната от професионалната тайна, се обработва в съответствие с приложения I и II и инструкциите за обработка.

*Член 5*

**Получаване на поверителна информация от Европейския парламент**

1. Поверителната информация, получена от Европейския парламент, се предава, както следва:

а) информацията, класифицирана с ниво „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и „другата поверителна информация“ — на секретариата на парламентарния орган/титуляря на мандатна длъжност, внесъл искането за това, или направо на Отдела за класифицирана информация;

б) информацията, класифицирана с ниво „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ или „TRÈS SECRET UE/EU TOP SECRET“ или с еквивалентно ниво — на ОКИ.

2. Регистрацията, съхранението и проследяването на поверителната информация се извършва според случая както от секретариата на парламентарния орган/титуляря на мандатна длъжност, който е получил информацията, така и от ОКИ.

3. Съгласуваните условия, които се определят по взаимно съгласие с оглед да се запази поверителността на информацията в случай на поверителна информация, предадена от Комисията, съобразно приложение II, точка 3.2 от рамковото споразумение, или в случай на поверителна информация, изпратена от Съвета съгласно член 5, параграф 4 от Междуинституционалното споразумение, се депозират заедно с поверителната информация в секретариата на парламентарния орган/титуляря на мандатна длъжност или в ОКИ, според случая.

4. Тези условия, посочени в параграф 3, могат също така да се прилагат mutatis mutandis за предаването на поверителна информация от други институции, органи, служби и агенции, създадени по силата или въз основа на Договорите, или от държавите членки.

5. За да осигури степен на защита в съответствие с нивото на класификация „TRES SECRET UE/EU TOP SECRET“ или с еквивалентно ниво на класификация, Председателският съвет създава контролна комисия. Информацията, класифицирана с ниво „TRES SECRET UE/EU TOP SECRET“, или с еквивалентно ниво на класификация се съобщава на Европейския парламент при допълнителни условия, които се договарят между Европейския парламент и институцията на Съюза, от която се получава информацията.

*Член 6*

**Съобщаване от Европейския парламент на класифицирана информация на трети страни**

Европейският парламент може, при условие че е налице предварително писмено съгласие на създателя на информацията или институцията на Съюза, която е съобщила класифицираната информация на Европейския парламент, според случая, да предаде такава класифицирана информация на трети страни, при условие че те гарантират, че при обработката на такава информация в рамките на техните служби и помещения се спазват правила, които са равностойни на правилата, предвидени в настоящото решение.

*Член 7*

**Обезопасени съоръжения**

1. За целите на управлението на поверителна информация Европейският парламент създава обезопасена зона и обезопасени читални.

2. В обезопасената зона се предоставят съоръжения за регистрация, извършване на справки, архивиране, предаване и обработване на класифицирана информация. В нея се включват наред с другото читалня и заседателна зала за ползване на класифицирана информация за справка, като управлението на тази зона се поема от ОКИ.

3. Могат да се създават обезопасени читални извън обезопасената зона, за да се позволи извършването на справки с информация, класифицирана с ниво „RESTREINT EU/EU RESTRICTED“ или с еквивалентно ниво на поверителност и „друга поверителна информация“. Обезопасените читални се управляват от компетентните служби на секретариатите на парламентарния орган/титуляря на мандатна длъжност или от ОКИ, според случая. В тях не се разполагат фотокопирни машини, телефони, факсмашини, скенери или каквито и да е други технически средства за възпроизвеждане или разпространяване на документи.

*Член 8*

**Регистрация, обработка и съхранение на поверителна информация**

1. Информация, класифицирана с ниво „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и „друга поверителна информация“ се регистрира и съхранява от компетентните служби на секретариатите на парламентарния орган/титуляря на мандатна длъжност или от ОКИ, в зависимост от това кой е получил информацията.

2. За обработването на информация, класифицирана с ниво „RESTREINT EU/EU RESTRICTED“ или с еквивалентно ниво и на „друга поверителна информация“ се прилагат следните условия:

а) документите се предават лично на ръководителя на секретариата, който ги регистрира и предоставя потвърждение за получаването им;

б) когато тези документи не се ползват, те се съхраняват под ключ и за тях носи отговорност секретариатът;

в) в никакъв случай информацията не може да се записва на друг носител или да се предоставя на който и да било; такива документи могат да бъдат размножавани единствено посредством целесъобразно акредитирано оборудване, както е определено в насоките за сигурност;

г) достъпът до такава информация е ограничен до адресатите им или до институцията на Съюза, която е съобщила информацията на Европейския парламент, в съответствие с условията, посочени в член 4, параграф 2 или в член 5, параграфи 3, 4 и 5;

д) секретариатът на парламентарния орган/титулярят на мандатна длъжност съхранява списък на лицата, които са ползвали информацията за справка, като се отбелязват датата и часът на тази справка и предават списъка на ОКИ в момента на депозирането на информацията в този отдел.

3. Информация, класифицирана с ниво „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ или „TRÈS SECRET UE/EU TOP SECRET“ или с еквивалентно ниво, се регистрира, обработва и съхранява от ОКИ в обезопасената зона в съответствие с конкретното ниво на класификация и съгласно определеното в насоките за сигурност.

4. В случай на неспазване на правилата, установени в параграфи 1–3 отговорното длъжностно лице от секретариата на парламентарния орган/титулярят на мандатна длъжност или ОКИ, според случая, информира генералния секретар, който отнася въпроса на вниманието на председателя на Парламента, в случай че е засегнат член на Европейския парламент.

*Член 9*

**Достъп до защитени съоръжения**

1. Единствено следните лица имат достъп до обезопасената зона:

а) лицата, на които съгласно член 3, параграфи 4—7 е разрешено да правят справки в информацията, съхранявана в обезопасената зона, и които са подали заявление по реда на член 10, параграф 1;

б) лицата, на които съгласно член 4, параграф 1 е разрешено да създават класифицирана информация, и които са подали заявление по реда на член 10, параграф 1;

в) длъжностните лица на Европейския парламент от ОКИ;

г) длъжностни лица на Европейския парламент, които отговарят за управлението на ОКИ;

д) длъжностни лица на Европейския парламент, отговорни за охраната и пожарната безопасност, при необходимост;

е) почистващ персонал, но единствено в присъствието на длъжностно лице, работещо в ОКИ, и под негово тясно наблюдение.

2. ОКИ има право да откаже достъп до обезопасената зона на всяко лице, което не е оправомощено да има достъп до нея. Всяко оспорване на решението на ОКИ се подава до председателя на Европейския парламент, когато заявлението за достъп е свързано с членовете на Европейския парламент, а в останалите случаи — до генералния секретар.

3. Генералният секретар може да разреши провеждането на заседание за ограничен брой лица в заседателната зала в обезопасената зона.

4. Единствено следните лица имат достъп до обезопасената читалня:

а) членове на Европейския парламент, длъжностни лица на Европейския парламент и други служители на Парламента, работещи за политически групи, които са надлежно идентифицирани за целите на извършването на справки или създаването на поверителна информация;

б) длъжностни лица на Европейския парламент, които отговарят за управлението на ОКИ, длъжностни лица от секретариата на парламентарния орган/титуляря на мандатна длъжност, които са получили информацията, а също и длъжностни лица от ОКИ;

в) при необходимост, длъжностни лица на Европейския парламент, отговорни за охраната и пожарната безопасност.

г) персонал, отговарящ за почистването, единствено в присъствието и под зоркото наблюдение на длъжностно лице, работещо в секретариата на парламентарния орган/титуляря на мандатна длъжност или в ОКИ, според случая.

5. Компетентният секретариат на парламентарния орган/титуляря на мандатна длъжност или ОКИ, според случая, има право да откаже достъп до обезопасената читалня на всяко неоправомощено да има достъп до нея лице. Всяко възражение срещу отказ на достъп се подава до председателя на Европейския парламент, когато заявлението за достъп е свързано с член на Европейския парламент, а в останалите случаи — до генералния секретар.

*Член 10*

**Извършване на справки или създаване на информация в защитени съоръжения**

1. Лице, което желае да извърши справки или да създаде поверителна информация в обезопасената зона изпраща предварително своето име на ОКИ. ОКИ проверява самоличността на лицето и проверява дали лицето има разрешение в съответствие с член 3, параграфи 3—7, член 4, параграф 1 или с член 5, параграфи 3—5 да прави такива справки или да създава поверителна информация.

2. Лице което желае в съответствие с член 3, параграфи 3 и 7, да прави справка в поверителна информация, класифицирана с ниво „RESTREINT EU/EU RESTRICTED“ или с еквивалентно ниво или „друга поверителна информация“ в обезопасена читалня, съобщава предварително своето име на компетентните служби на секретариатите на парламентарния орган/титуляря на мандатна длъжност или в ОКИ.

3. Освен при извънредни обстоятелства (например когато са подадени многобройни заявления за извършване на справка в кратък период от време), само на едно лице се разрешава да ползва поверителната информация за справка в обезопасеното съоръжение, в присъствието на длъжностно лице от секретариата на парламентарния орган/титуляря на мандатна длъжност или ОКИ.

4. При извършването на справката са забранени външни контакти (включително посредством използването на телефони или на други технически средства), воденето на бележки и фотокопирането или фотографирането на поверителната информация, предмет на справката.

5. Преди да се разреши на лицето да напусне обезопасеното съоръжение, длъжностното лице от секретариата на парламентарния орган/титуляря на мандатна длъжност или ОКИ, се уверява в наличността на информацията за справка и проверява дали тя е непокътната и пълна.

6. В случай на неспазване на гореизложените правила длъжностното лице от секретариата на парламентарния орган/титуляря на мандатна длъжност или от ОКИ информира генералния секретар, който отнася въпроса на вниманието на председателя, когато е засегнат член на Европейския парламент.

*Член 11*

**Минимални стандарти за ползване на поверителна информация за справка по време на заседания при закрити врата извън обезопасените съоръжения**

1. Справки в информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и „друга поверителна информация“ може да правят членове на парламентарни комисии или на други политически и административни органи на Европейския парламент по време на заседания при закрити врата извън обезопасените съоръжения.

2. В случаите, предвидени в параграф 1, секретариатът на парламентарния орган/титулярят на мандатна длъжност, отговорен за заседанието, гарантира, че са изпълнени следните условия:

а) единствено лицата, които са определени от председателя на компетентната комисия или орган да участват в заседанието, имат право на достъп до заседателната зала;

б) всички документи са номерирани, раздават се в началото на заседанието и се събират отново в края, като не се вземат никакви бележки, нито се правят фотокопия или снимки от тях;

в) в протокола от заседанието не се отразява съдържанието на разискваната информация; в протокола може да бъде вписано само съответното решение, ако има такова;

г) поверителна информация, предоставена устно на получатели в Европейския парламент, подлежи на степен на защита, равностойна о на тази, прилагана по отношение на поверителната информация в писмена форма;

д) в заседателните зали не могат да се съхраняват допълнителен брой документи;

е) копия от документите се раздават само в необходимия брой екземпляри на участниците и устните преводачи в началото на заседанието;

ж) класификацията/маркировката на документите се разяснява от председателстващия заседанието в неговото начало;

з) участниците не могат да изнасят документи от заседателната зала;

и) всички екземпляри на документите се събират и отчитат в края на заседанието от секретариата на парламентарния орган/титуляря на мандатна длъжност; и

й) в заседателната зала, където въпросната поверителна информация се обсъжда или се ползва за справка, не се допускат комуникационни или други електронни устройства.

3. Когато в съответствие с изключенията, предвидени в точка 3.2.2 от приложение II към Рамковото споразумение и в член 6, параграф 5 от Междуинституционалното споразумение, информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“ или с еквивалентно ниво е обсъждана по време на заседание при закрити врата, секретариатът на парламентарния орган/титуляря на мандатна длъжност, отговорен за заседанието, освен че осигурява спазване на разпоредбите на параграф 2, следи определените за участие в заседанието лица да отговарят на изискванията по член 3, параграфи 4 и 7.

4. В случая по параграф 3 ОКИ предоставя на секретариата на парламентарния орган/титуляря на мандатна длъжност, отговорен за заседанието при закрити врата, необходимия брой екземпляри от документите, които подлежат на обсъждане, които след заседанието се връщат на ОКИ.

*Член 12*

**Архивиране на поверителни документи**

1. В обезопасената зона се осигуряват надеждни средства за архивиране. ОКИ е отговорен за управлението на обезопасения архив в съответствие със стандартните критерии за архивиране.

2. Класифицирана информация, която е окончателно депозирана в ОКИ, и информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво, която е депозирана в секретариата на парламентарния орган/титуляря на мандатна длъжност, се предава в обезопасен архив в обезопасената зона шест месеца след извършването на последната справка и най-късно една година след нейното депозиране. „Другата поверителна информация“ се архивира, освен ако е внесена в ОКИ, от секретариатите на съответния парламентарен орган/титуляря на мандатна длъжност в съответствие с общите правила относно управлението на документи.

3. Поверителната информация, съхранявана в обезопасения архив, може да се ползва за справки при спазване на следните условия:

а) единствено лицата, които са идентифицирани по име, функции или чрез длъжността си в придружаващия документ, изготвен при депозирането на поверителната информация, са оправомощени да ползват тази информация за справка;

б) заявлението за ползване на поверителната информация за справка се представя на ОКИ, който прехвърля въпросния документ в обезопасената читалня; и

в) прилагат се процедурите и условията за ползване на поверителната информация за справка, посочени в член 10.

*Член 13*

**Понижаване на нивото на поверителност, премахване на класификацията и сваляне на маркировката на поверителна информация**

1. На поверителна информация може да бъде понижена степента на поверителност, премахната класификацията или свалена маркировката само с предварително разрешение на създателя на информацията, а при необходимост и след обсъждане с други заинтересовани страни.

2. Понижаването или премахването на класификацията се потвърждава в писмена форма. Създателят на информацията носи отговорност за уведомяване на адресатите на информацията за промяната, а те на свой ред са отговорни да уведомят за промяната всички следващи адресати, до които са изпратили документа или копия от него. По възможност създателите на информация посочват върху класифицираните документи дата, срок или обстоятелства, при които може да се понижи или премахне класификацията на съдържанието. В противен случай те извършват преглед на документите най-късно на всеки пет години, за да проверят дали първоначалната класификация е все още необходима.

3. Поверителна информация, съхранявана в обезопасения архив, се разглежда своевременно, но не по-късно от 25-та година след нейното създаване, за да се вземе решение дали нейната класификация да бъде премахната, да бъде понижено нейното ниво на поверителност или да бъде свалена нейната маркировка. Разглеждането и публикуването на такава информация се извършват в съответствие с разпоредбите на Регламент (ЕИО, ЕВРАТОМ) № 354/83 на Съвета от 1 февруари 1983 г. относно отваряне за обществеността на историческите архиви на Европейската икономическа общност и на Европейската общност за атомна енергия ([1]). Премахването на класификацията се извършва от създателя на класифицираната информация или от службата, която носи текуща отговорност съгласно приложение I, част 1, точка 10.

4. След премахване на класификацията, информация, която преди това е била класифицирана и съхранявана в обезопасения архив, се прехвърля в историческия архив на Европейския парламент за постоянно съхранение и последваща обработка съгласно приложимите правила.

5. След сваляне на маркировката информацията, която преди това е била определена като „друга поверителна информация“, е подвластна на правилата на Европейския парламент относно управлението на документи.

*Член 14*

**Нарушаване на сигурността, загуба или компрометиране на класифицираната информация**

1. Нарушение на поверителността като цяло и по-специално на настоящото решение от страна на членове на Европейския парламент ще доведе до прилагане на съответните разпоредби относно санкциите, предвидени в Правилника за дейността на Европейския парламент.

2. Нарушение, извършено от служител на Европейския парламент, се преследва по процедурите и санкциите, предвидени съответно в Правилника за длъжностните лица и Условията за работа на другите служители на Европейския съюз, установени в Регламент (ЕИО, Евратом, ЕОВС) № 259/68 ([2]) („Правилник за длъжностните лица“).

([1]) ОВ L 43, 15.2.1983 г., стр. 1.
([2]) ОВ L 56, 4.3.1968 г., стр. 1.

3. Председателят и/или генералният секретар, според случая, организират всички необходими разследвания в случай на нарушение според определението в насока за сигурност 6.

4. Ако поверителната информация е била съобщена на Европейския парламент от институция на Съюза или от държава членка, председателят и/или генералният секретар, според случая, информират съответната институция на Съюза или държава членка за всяка доказана или предполагаема загуба на класифицирана информация или нейно компрометиране, за резултатите от разследването и за взетите мерки за избягването на повторни случаи.

*Член 15*

**Коригиране на настоящото решение и на правилата за изпълнението му и годишен отчет относно прилагането на настоящото решение**

1. Генералният секретар предлага, ако е необходимо, да се коригират настоящото решение и приложенията за неговото изпълнение и предава тези предложения на Бюрото, което взема решение.

2. Генералният секретар е отговорен за прилагането на настоящото решение от службите на Европейския парламент и издава инструкции за обработката по въпроси, обхванати от СУСИ, в съответствие с посочените в настоящото решение принципи.

3. Генералният секретар представя на Бюрото годишен отчет за прилагането на настоящото решение.

*Член 16*

**Преходни и заключителни разпоредби**

1. Некласифицирана информация, съхранявана в ОКИ или във всеки друг архив на Европейския парламент, която се счита за поверителна и датира отпреди 1 април 2014 г., се счита за целите на настоящото решение за съставляваща „друга поверителна информация“. Създателят на информацията може по всяко време да промени нивото на поверителност.

2. Чрез дерогация от член 5, параграф 1 и от член 8, параграф 1 от настоящото решение за период от дванадесет месеца, считано от 1 април 2014 г., информация, предоставена от Съвета съгласно Междуинституционалното споразумение, която е класифицирана с ниво „RESTREINT UE/EU RESTRICTED“, или с еквивалентно ниво на класификация, се внася в ОКИ и се регистрира и съхранява от него. В тази информация могат да се правят справки в съответствие с член 4, параграф 2, букви а) и в) и с член 5, параграф 4 от Междуинституционалното споразумение.

3. Решението на Бюрото от 6 юни 2011 г. относно Правилника относно обработката на поверителна информация от Европейския парламент се отменя.

*Член 17*

**Влизане в сила**

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

*ПРИЛОЖЕНИЕ I*

**Част 1**

**ОСНОВНИ ПРИНЦИПИ И МИНИМАЛНИ СТАНДАРТИ ЗА СИГУРНОСТ ЗА ЗАЩИТА НА ПОВЕРИТЕЛНАТА ИНФОРМАЦИЯ**

1. **ВЪВЕДЕНИЕ**

Настоящите разпоредби определят основните принципи и минималните стандарти за сигурност за защитата на поверителна информация, които трябва да се съблюдават и/или спазват от Европейския парламент във всички негови места на работа, в т.ч. от всички получатели на класифицирана информация и „друга поверителна информация“ по такъв начин, че да се гарантира сигурността и всички засегнати лица да могат да бъдат сигурни, че е установен общ стандарт за защита. Тези разпоредби се допълват от насоките за сигурност, съдържащи се в приложение II, и от други разпоредби, уреждащи обработката на поверителна информация от парламентарните комисии и други парламентарни органи/титуляри на мандатна длъжност.

2. **ОСНОВНИ ПРИНЦИПИ**

Политиката за сигурност на Европейския парламент съставлява неразделна част от неговата обща политика за вътрешно управление, поради което се основава на принципите, които уреждат общата му политика. Тези принципи включват законосъобразност, прозрачност, отчетност, както и субсидиарност и пропорционалност.

Законосъобразността поражда необходимостта от стриктно придържане към правната рамка при изпълнението на функции във връзка със сигурността, както и необходимостта от спазване на приложимите законови изисквания. Освен това отговорностите в областта на сигурността трябва да се основават на надеждни правни разпоредби. Разпоредбите на Правилника за длъжностните лица, по-специално член 17 от него относно задължението на служителите да се въздържат от всяко неразрешено разкриване на информация, получена във връзка с изпълнението на задълженията им, и дял VI от него относно дисциплинарните мерки се прилагат в тяхната цялост. Този принцип означава също така, че нарушенията на сигурността в рамките на отговорността на Европейския парламент се третират по начин, който съответства на неговия правилник за дейността и политиката му по отношение на дисциплинарните мерки.

Прозрачността поражда необходимостта от яснота относно всички правила и разпоредби за сигурност и от намиране на баланс между различните служби и различните области (физическа сигурност спрямо защита на информацията и т.н.) и необходимостта от последователна и структурирана политика за осведоменост относно сигурността. Освен това ясни писмени насоки са необходими за прилагането на мерки за сигурност.

Отчетността означава, че трябва бъдат ясно определени отговорностите в сферата на сигурността. Освен това тя поражда необходимостта от редовно наблюдение за правилното изпълнение на тези отговорности.

Субсидиарността означава, че сигурността трябва да се организира на най-ниското възможно равнище и във възможно най-тясна връзка с генералните дирекции и службите на Европейския парламент.

Пропорционалността означава, че дейностите във връзка със сигурността трябва да бъдат строго ограничаничени до абсолютно необходимото и че мерките за сигурност трябва да бъдат пропорционални на интересите, които подлежат на защита, и на действителната или потенциалната заплаха за тези интереси, така че да позволи тези интереси да бъдат защитавани по начин, който гарантира възможно най-малко сътресения.

3. **ОСНОВИ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА**

Основите на надеждната сигурност на информацията са:

а) подходящи комуникационни и информационни системи (КИС). Те са в отговорност на органа по сигурността в Европейския парламент (както е определен в насока за сигурност 1);

б) в рамките на Европейския парламент органът за осигуреност на информацията, (както е определен в насока за сигурност 1), който отговаря за работата със съответния орган по сигурността за предоставянето на информация и съвети относно техническите заплахи за сигурността на комуникационните и информационни системи (КИС) и средствата за защита срещу тези заплахи;

в) тясно сътрудничество между компетентните служби на Европейския парламент и службите по сигурността на другите институции на Съюза.

4. **ПРИНЦИПИ ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА**

4.1. ***Цели***

Основните цели на сигурността на информацията са, както следва:

а) защита на поверителна информация срещу шпионаж, излагане на риск или неразрешено разкриване;

б) защита на класифицирана информация, която се обработва в информационни и комуникационни системи и мрежи, срещу заплахи за нейната поверителност, цялостност и наличност;

в) защита на помещенията на Европейския парламент, в които се съхранява класифицирана информация, срещу саботаж и умишлено злонамерено причиняване на вреди;

г) в случай на пропуск в сигурността, оценка на причинените вреди, ограничаване на последиците, провеждане на разследвания в областта на сигурността и предприемане на необходимите мерки за коригиране на пропуска.

4.2. ***Класификация***

4.2.1. Когато става въпрос за поверителност са необходими внимание и опит при подбора на информацията и материала, които ще бъдат защитени, както и при оценката на необходимата степен на защита. От съществено значение е степента на защита да съответства на чувствителния характер по отношение на сигурността на отделните подлежащи на защита информация или материали. За да се гарантира безпрепятственият поток от информация се избягва както прекомерната, така и недостатъчно високата степен на класифициране.

4.2.2. Класификационната система е инструментът за осъществяването на принципите, предвидени в настоящия раздел. Подобна система за класифициране се следва при планирането и организирането на начини за противодействие на шпионаж, саботаж, тероризъм и други заплахи, така че да се осигурява максимална степен на защита на най-важните помещения, в които се съхранява класифицирана информация, и най-чувствителните точки в тези помещения.

4.2.3. Отговорността за класифициране на информация се носи изцяло от създателя на съответната информация.

4.2.4. Степента на класифициране може да се основава единствено на съдържанието на съответната информация.

4.2.5. Когато няколко вида информация са групирани заедно, тяхната класификация трябва да бъде най-малко на нивото но най-високата степен на класифициране, определена за един от тези видове информация. Въпреки това за съвкупност от различни видове информация може да се определи по-висока степен на класификация от тази на нейните съставни части.

4.2.6 Класификация се извършва само в случаите, в които тя е необходима, и единствено за сроковете, в рамките на които тя е необходима.

4.3. ***Цели на мерките за сигурност***

Мерките за сигурност:

а) се отнасят до всички лица, които имат достъп до класифицирана информация, до информационни носители, съдържащи класифицирана информация и „друга поверителна информация“, както и до всички помещения, в които се намира тази информация, и важни съоръжения;

б) са предназначени да идентифицират по такъв начин лица, чиято длъжност (по отношение на достъп, връзки или друг начин) би могла да застраши сигурността на подобна информация и на важни съоръжения, в които се помещава тази информация, и да водят до тяхното отстраняване или преместване на друга длъжност;

в) предотвратяват достъпа на всяко лице без разрешение до такава информация или до съоръженията, в които тя се помещава;

г) гарантират, че тази информация се разпространява единствено на принципа на „необходимост да се знае“, който е основен принцип за всички аспекти на сигурността;

д) гарантират целостта (чрез предотвратяване на повреждане, неразрешена промяна или неразрешено заличаване) и наличността (за лицата, които имат нужда и имат разрешение за достъп до нея) на цялата поверителна информация, независимо дали е класифицирана или некласифицирана, и особено къде се съхранява, обработва или предава в електромагнитен вид.

## 5. **ОБЩИ МИНИМАЛНИ СТАНДАРТИ**

Европейският парламент гарантира, че се спазват общи минимални стандарти за сигурност от всички получатели на класифицирана информация, едновременно вътре в институцията и в рамките на нейната компетентност, а именно от всички негови служби и изпълнители, така че тази информация да може да се предава с увереността, че при работата с нея ще се полагат аналогични грижи. Тези минимални стандарти включват критерии за проверка за надеждност на длъжностните лица на Европейския парламент и другите служители, които работят за политически групи, и процедури за защита на поверителната информация.

Европейският парламент позволява на трети страни достъп до тази информация само при условие че тези трети страни гарантират, че при работата с тази информация се спазват разпоредби, които са най-малкото равностойни на настоящите общи минимални стандарти.

Тези общи минимални стандарти също се прилагат, когато съобразно договор или споразумение за предоставяне на безвъзмездни средства Европейският парламент поверява на стопански или други субекти задачи, които включват поверителна информация.

## 6. **СИГУРНОСТ ВЪВ ВРЪЗКА С ДЛЪЖНОСТНИТЕ ЛИЦА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И ДРУГИТЕ СЛУЖИТЕЛИ НА ПАРЛАМЕНТА, КОИТО РАБОТЯТ ЗА ПОЛИТИЧЕСКИ ГРУПИ**

### 6.1. ***Инструкции за сигурността, адресирани до длъжностните лица на Европейския парламент и другите служители на Парламента, които работят за политически групи***

Длъжностните лица на Европейския парламент и другите служители на Парламента, които работят за политически групи и заемат длъжности, на които биха могли да имат достъп до класифицирана информация, получават подробни инструкции както при встъпването си в длъжност, така и през определени интервали от време след това, относно необходимостта от сигурност и процедурите по обезпечаването ѝ. От тези лица се изисква да потвърдят в писмена форма, че са прочели приложимите разпоредби за сигурност и са напълно запознати с тях.

### 6.2. ***Задължения на ръководството***

Ръководителите са длъжни да знаят кои техни служители боравят в работата си с класифицирана информация или имат достъп до защитени комуникационни или информационни системи, както и да записват и да докладват за всички инциденти или явни слабости в системата, които могат да имат последствия за сигурността.

### 6.3. ***Статус по отношение на сигурността на длъжностните лица на Европейския парламент и другите служители на Парламента, които работят за политическите групи***

Установяват се процедури, с които да се гарантира, че при получаване на неблагоприятна информация за длъжностно лице на Европейския парламент или друг служител на Парламента, работещ за политическа група, се предприемат стъпки за определяне дали работата на това лице го поставя в контакт с класифицирана информация или дали то има достъп до защитени комуникационни или информационни системи и че компетентната служба на Европейския парламент е информирана за това. Ако компетентният национален орган по сигурността посочи, че лицето представлява заплаха за сигурността, то не се допуска или се отстранява от изпълнението на функции, чрез които би могло да застраши сигурността.

## 7. **ФИЗИЧЕСКА СИГУРНОСТ**

„Физическа сигурност“ означава прилагането на мерки за физическа и техническа защита за предотвратяване на неразрешения достъп до класифицирана информация.

7.1. ***Необходимост от защита***

Мерките за физическа сигурност, прилагани за защита на класифицираната информация, са съразмерни със степента на класификация и обема на съхраняваните материали и информация, както и със заплахата, на която те са изложени. Всички, които притежават класифицирана информация, следват единните практики относно класификацията на тази информация и трябва да спазват общите стандарти за защита относно съхраняването, предаването и унищожаването на информация и материали, за които се изисква защита.

7.2. ***Проверка***

Преди да оставят без надзор зони, в които се съдържа класифицирана информация, лицата, които се грижат за тази информация, гарантират, че тя се съхранява сигурно и че са задействани всички устройства за сигурност (ключалки, алармени системи и др.). Допълнително след края на работното време се извършват независими проверки.

7.3. ***Сигурност на сградите***

Сградите, в които се съхранява класифицирана информация или защитени комуникационни и информационни системи, са защитени срещу неразрешен достъп.

Естеството на защитата, с която се ползва класифицираната информация, например решетки за прозорци, ключалки за врати, охрана на входовете, автоматизирани контролни системи за достъп, проверки на сигурността и патрули, алармени системи, системи за откриване на нерегламентирано влизане и охранителни кучета, зависи от:

а) степента на класифициране, обема и местонахождението в сградата на информацията и материалите, които трябва да се защитават;

б) качеството на съоръженията, в които се съхраняват съответните материали и информация, и

в) техническите характеристики и местоположението на сградата.

Естеството на защитата, с която се ползват комуникационните и информационните системи, зависи от оценката на стойността на информацията и материалите, изложени на риск, и на възможните вреди в случай на риск за сигурността, както и от техническите характеристики и местоположението на сградата, в която се намира системата, и от местоположението на системата в сградата.

7.4. ***Планове за непредвидени ситуации***

Предварително се изготвят подробни планове за защита на класифицираната информация при извънредни обстоятелства.

8. **ОБОЗНАЧЕНИЯ ЗА СИГУРНОСТ, МАРКИРОВКА, ПОСТАВЯНЕ И УПРАВЛЕНИЕ НА КЛАСИФИКАЦИЯТА**

8.1. ***Обозначения за сигурност***

Не се разрешават други класификации, различни от определените в член 2, буква г) от настоящото решение.

За определяне на срока на валидност на дадена класификация (за класифицирана информация, обозначаваща автоматично понижаване на нивото на класифициране или премахване на класификацията) може да се използва уговорено обозначение за сигурност.

Обозначенията за сигурност се използват само в съчетание с ниво на класификация.

Обозначенията за сигурност се уреждат допълнително в насока за сигурност 2 и се определят в инструкциите за обработка.

8.2. ***Маркировки***

Маркировка се използва за определяне на предварително определени специални инструкции относно боравенето с поверителна информация. Маркировките може също така да обозначават областта, за която се отнася даден документ, или за указване на особено разпространение въз основа на принципа за „необходимост да се знае“, или за обозначаване на края на ембарго (за некласифицирана информация).

Маркировката не е класификация и не се използва вместо нея.

Маркировките се уреждат допълнително в насока за сигурност 2 и се определят в инструкциите за обработка.

8.3. ***Поставяне на класификация и на обозначения за сигурност***

Поставянето на класификация и на обозначения за сигурност и маркировки се извършва в съответствие с насока за сигурност 2, раздел Д, и с инструкциите за обработка.

8.4. ***Управление на класификацията***

8.4.1 *Общи положения*

Информацията се класифицира само при необходимост. Класификацията се обозначава ясно и правилно и се поддържа само за периода, през който информацията се нуждае от защита.

Отговорността за класифициране на информацията и за всяко евентуално последващо понижаване на нивото на класифициране или премахване на класификацията се носи изцяло от създателя на информацията.

Длъжностни лица на Европейския парламент извършват класификация, понижаване или премахване на класификацията на информацията по указания на генералния секретар или вследствие на делегиране на правомощия от негова страна.

Подробните процедури за работа с класифицирани документи са оформени по начин, който гарантира, че им е предоставена защита, съответна на информацията, която съдържат.

Броят на лицата, оправомощени да създават информация, класифицирана с ниво TRÈS SECRET UE/EU TOP SECRET, се свежда до минимум, а имената им се пазят в списък, изготвен от ОКИ.

8.4.2 *Прилагане на класификация*

Класификацията на документ се определя от степента на чувствителност на неговото съдържание в съответствие с определенията в член 2, буква г). Важно е класификацията да се определя правилно и да се използва умерено.

Класификацията на писмо или записка, включващи приложени документи, съответства най-малко на най-високата степен на класификация, предоставена на едно от техните приложения. Създателят на информация ясно посочва степента на класификация, която писмото или записката трябва да получат след отделянето им от приложенията.

Създателят на подлежащ на класификация документ следва изложените по-горе правила и се въздържа от всякаква склонност към определяне на прекомерно висока или недостатъчно висока степен на класификация.

Отделни страници, параграфи, раздели, приложения, допълнения, прикрепени части и приложения към даден документ могат да изискват различна степен на класификация и това се извършва по съответен начин. Степента на класификация на целия документ съответства на тази част от документа, която има най-висока степен на класификация.

9. **ПРОВЕРКИ НА МЯСТО**

Дирекцията на Европейския парламент, отговаряща за сигурността и оценката на риска, която може да изисква помощ от органите на Съвета или на Комисията, отговарящи за сигурността, извършва периодични вътрешни проверки на мерките за сигурност за защита на класифицираната информация.

Органите по сигурността и компетентните служби на институциите на Съюза могат да извършват, като част от съгласуван процес, иницииран от страните, партньорски проверки на мерките за сигурност за защита на класифицираната информация, които се обменят съгласно съответните междуинституционални споразумения.

10. **ПРОЦЕДУРИ ЗА ПРЕМАХВАНЕ НА КЛАСИФИКАЦИЯТА И ПРЕМАХВАНЕ НА МАРКИРОВКИТЕ**

10.1. ОКИ разглежда класифицираната информация, която се съдържа в неговия регистър, и взема съгласието на създателя на документа за премахване на класификацията или премахване на маркировката на документа не по-късно от 25 години след датата на създаването му. Документите, на които не е премахната класификацията или маркировката при първото разглеждане, се преразглеждат периодично и най-малко на всеки пет години. В допълнение към прилагането ѝ към документите, които понастоящем се намират в обезопасения архив в обезопасената зона и са надлежно класифицирани, процедурата по премахване на маркировката може също да обхване друга поверителна информация, която се съхранява или в служба или орган на Парламента, или в службата, отговаряща за историческите архиви на Парламента.

10.2 Решението за премахването на класификацията или на маркировката на даден документ като общо правило се взема единствено от създателя на документа или, в изключителни случаи, в сътрудничество със службата или органа на Парламента, която съхранява тази информация, преди информацията, съдържаща се в документа, да бъде прехвърлена към службата, отговаряща за историческите архиви на Парламента. Премахването на класификацията или на маркировката на класифицирана информация може да се извършва само след получаване на изричното писмено съгласие на създателя на документа. В случаите на „друга поверителна информация“ секретариатът на службата или органа на Парламента, която съхранява тази информация, в сътрудничество със създателя взема решение дали да бъде премахната маркировката на документа.

10.3. От името на автора ОКИ носи отговорност за информиране на адресатите на документа за промяната в класификацията или маркировката, а те на свой ред са отговорни да информират за промяната всички следващи адресати, до които са изпратили или за които са направили копия от документа.

10.4. Премахването на класификацията не засяга обозначенията за сигурност или маркировката, които могат да бъдат обозначени на документа.

10.5. При премахване на класификацията първоначалната класификация в горната и долната част на всяка страница се зачертава. На първата (заглавната) страница на документа се поставя печат и се попълва референцията на ОКИ. При премахване на маркировката първоначалната маркировка в горната част на всяка страница се зачертава.

10.6. Текстът на документа с премахната класификация или маркировка се прилага към електронния фиш или съответстващата система, където е бил регистриран.

10.7. В случай на документи, които са предмет на изключение във връзка с неприкосновеността на личния живот и личната неприкосновеност или търговски интереси на физическо или юридическо лице и в случай на чувствителни документи, се прилага член 2 от Регламент (ЕИО, Евратом) № 354/83.

10.8. В допълнение към разпоредбите на точки от 10.1 до 10.7 се прилагат следните правила:

а) по отношение на документи от трети страни, ОКИ се консултира със засегнатата трета страна, преди да пристъпи към премахването на класификацията или маркировката;

б) по отношение изключението във връзка с неприкосновеността на личния живот и личната неприкосновеност, процедурата по премахването на класификацията или маркировката взема предвид по-специално съгласието на засегнатото лице или, в зависимост от случая, невъзможността да бъде идентифицирано засегнатото лице;

в) по отношение на изключението във връзка с търговски интереси на физическо или юридическо лице засегнатото лице може да бъде уведомено чрез публикация в *Официален вестник на Европейския съюз* и да му се даде срок от четири седмици от датата на публикацията, в който да представи забележки.

**Част 2**

**ПРОЦЕДУРА ЗА ПРОВЕРКА ЗА НАДЕЖДНОСТ**

11. **ПРОЦЕДУРА ЗА ПРОВЕРКА ЗА НАДЕЖДНОСТ НА ЧЛЕНОВЕ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ**

11.1. За да получат достъп до информация, която е класифицирана с ниво „CONFIDENTIEL UE/EU CONFIDENTIAL“ или с еквивалентно ниво на поверителност, членовете на Европейския парламент трябва да са били оправомощени или в съответствие с процедурата, посочена в подточки точки 11.3 и 11.4 от настоящото приложение, или въз основа на клетвена декларация за неразкриване в съответствие с член 3, параграф 4 от настоящото решение.

11.2 За да получат достъп до информация, която е класифицирана с ниво TRÈS SECRET UE/EU TOP SECRET или SECRET UE/EU SECRET или с еквивалентно ниво на поверителност, членовете на Европейския парламент трябва да са били оправомощени в съответствие с процедурата, посочена в подточки 11.3 и 11,14.

11.3. Разрешение се дава само на членове на Европейския парламент, които са били подложени на проверка за надеждност от компетентните национални органи на държавите членки в съответствие с процедурата, посочена в подточки 11.9—11.14. Отговорен за предоставянето на разрешение за членовете на Европейския парламент е председателят.

11.4 Председателят може да издаде писмено разрешение след получаване на становището на компетентните национални органи на държавите членки въз основа на проверката за надеждност, извършена в съответствие с подточки 11.8—11.13.

11.5. Дирекцията на Европейския парламент, отговаряща за охраната и оценката на риска, поддържа актуален списък на всички членове на Европейския парламент, на които е било предоставено разрешение, включително временно разрешение, по смисъла на подточка 11.15.

11.6. Разрешението е със срок на валидност пет години или за срока на задачите, във връзка с които е издадено, който от двата срока е по-кратък. То може да бъде подновено в съответствие с процедурата, предвидена в подточка 11.4.

11.7. Разрешението се отнема от председателя, ако той счете, че са налице основателни причини за това отнемане. Всяко решение за отнемане на разрешение се съобщава на съответния член на Европейския парламент, който може да поиска да бъде изслушан от председателя, преди отнемането да породи действие, както и на компетентния национален орган.

11.8. Проучването за сигурност се извършва със съдействието на съответния член на Европейския парламент и по искане на председателя. Компетентният национален орган за проучването е органът на държавата членка, чийто гражданин е съответният член.

11.9. Като част от процедурата на проверка от съответния член на Европейския парламент се изисква да попълни формуляр за лични данни.

11.10. Председателят посочва в искането си до компетентните национални органи нивото на класифицираната информация, която ще се предоставя на съответния член на Европейския парламент, така че той да може да извърши проверката.

11.11 Целият процес на проверката за надеждност, извършван от компетентните национални органи, заедно с получените резултати, е в съответствие със съответните действащи правила и разпоредби в съответната държава членка, включително тези, които се отнасят до обжалването.

11.12. Когато компетентният национален орган даде положително становище, председателят може да издаде разрешение на съответния член на Европейския парламент.

11.13. Когато становището, дадено от компетентните национални органи, е отрицателно, се уведомява заинтересованият член на Европейския парламент, който може да поиска да бъде изслушан от председателя. Той има право, ако прецени за необходимо, да се обърне към компетентния национален орган с цел да изиска допълнителни разяснения. При потвърждаване на отрицателното становище не се издава разрешение.

11.14. Всички членове на Европейския парламент, получили разрешение по смисъла на подточка 11.3, получават към момента на издаване на разрешението и на равни интервали от време след това нужните указания относно защитата на класифицираната информация и начина за гарантирането на защитата. Членовете на ЕП подписват декларация в потвърждение на това, че са получили тези указания.

11.15. В изключителни случаи председателят може, след като е уведомил компетентния национален орган и при условие че не е получил отговор от този орган в срок от един месец, да издаде временно разрешение на член на Европейския парламент за срок до шест месеца до получаване на резултата от проверката, посочена в подточка 11.11. Временните разрешения, издадени по този начин, не разрешават достъп до информация със степен на класификация TRÈS SECRET UE/EU TOP SECRET или с еквивалентно ниво на класификация.

## 12. ПРОЦЕДУРА ЗА ПРОВЕРКА ЗА НАДЕЖДНОСТ НА ДЛЪЖНОСТНИ ЛИЦА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА ДРУГИ СЛУЖИТЕЛИ НА ПАРЛАМЕНТА, РАБОТЕЩИ ЗА ПОЛИТИЧЕСКИ ГРУПИ

12.1. Само длъжностни лица на Европейския парламент и други служители на Парламента, които работят за политически групи и които поради естеството на работата си и поради изискванията във връзка със служебните си задължения трябва да са запознати или да използват класифицирана информация, могат да имат достъп до такава.

12.2. За да получат достъп до информация, която е класифицирана с ниво CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или с еквивалентно ниво на класификация, длъжностните лица на Европейския парламент и други служители на Парламента, работещи за политически групи, трябва да са били оправомощени в съответствие с процедурата, предвидена в подточки 12.3 и 12.4.

12.3. Разрешение се дава само на лицата, посочени в подточка 12.1, които са били подложени на проверка за надеждност от компетентните национални органи на държавите членки в съответствие с процедурата, посочена в подточки 12.9—12.14. Генералният секретар е отговорен за издаване на разрешение на длъжностни лица на Европейския парламент и други служители на Парламента, работещи за политически групи.

12.4 Генералният секретар може да издаде писмено разрешение след получаване на становището на компетентните национални органи на държавите членки въз основа на проверката за надеждност, извършена в съответствие с подточки 12.8—12.13.

12.5. Дирекцията на Европейския парламент, отговаряща за охраната и оценката на риска, поддържа и актуализира списък на всички длъжности, за които се изисква проучване за надеждност, предоставен от съответните служби на Европейския парламент, и на всички лица, на които е издадено разрешение, включително временно разрешение по смисъла на подточка 12.15.

12.6. Разрешението е със срок на валидност пет години или за срока на задачите, във връзка с които е издадено, който от двата срока е по-кратък. То може да се подновява в съответствие с процедурата, посочена в подточка 12.4.

12.7. Разрешението се отнема от генералния секретар, ако той счете, че са налице основателни причини за това отнемане. Всяко решение за отнемане на разрешение се съобщава на съответното длъжностно лице на Европейския парламент или друг служител на Парламента, който работи за политически групи, който може да поиска да бъде изслушан от генералния секретар, преди отнемането да породи действие, както и на компетентния национален орган.

12.8. Проверката за надеждност се извършва със съдействието на съответното длъжностно лице на Европейския парламент или друг служител на Парламента, който работи за политически групи, и по искане на генералния секретар. Компетентният национален орган за проверката е органът на държавата членка, чийто гражданин е съответното лице. Когато това се допуска от националните законови и подзаконови актове, компетентните национални органи могат да проведат разследвания по отношение на граждани на други държави, които искат достъп до информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или TRÈS SECRET UE/EU TOP SECRET.

12.9. Като част от процедурата за проверка от съответното длъжностно лице на Европейския парламент или от служителя на Парламента, работещ за политическа група, се изисква да попълни формуляр с лични данни.

12.10. Генералният секретар уточнява в своето искане до компетентния национален орган нивото на класифицираната информация, до която заинтересованото длъжностно лице на Европейския парламент или друг служител на Парламента, който работи за политически групи, следва да има достъп, за да може той да извърша проверката и да даде становището си относно степента на разрешение, която би било най-подходящо да се издаде на лицето.

12.11. Целият процес на проверката за надеждност, извършвана от компетентния национален орган, заедно с получените резултати, е в съответствие със съответните действащи правила и разпоредби в съответната държава членка, включително тези, които се отнасят до обжалването.

12.12. Когато становището, дадено от компетентния национален орган е положително, генералният секретар може да издаде разрешение на съответното длъжностно лице на Европейския парламент или друг служител на Парламента, който работи за политически групи.

12.13. Всяко отрицателно становище на компетентните национални органи се съобщава на съответното длъжностно лице на Европейския парламент или на служителя на Парламента, работещ за политическа група, който може да поиска да бъде изслушан от генералния секретар. Ако прецени за необходимо, генералният секретар може да се обърне към компетентния национален орган с цел да изиска допълнителни разяснения. При потвърждаване на отрицателното становище не се издава разрешение.

12.14. Всички длъжностни лица на Европейския парламент и други служители на Парламента, работещи за политически групи, на които е издадено разрешение по смисъла на подточки 12.4 и 12.5, при издаване на разрешението, а след това на равни интервали от време, получават всички необходими инструкции относно защитата на класифицирана информация и за средствата, които осигуряват тази защита. Тези длъжностните лица и служители подписват декларация, с която се удостоверява, че са получили тези инструкции и че се задължават да ги съблюдават.

12.15. В изключителни случаи генералният секретар може, след като е уведомил компетентните национални органи и при условие че не е получил оттовор от този орган в срок от един месец, да издаде временно разрешение на длъжностно лице на Европейския парламент или на служител, работещ за политическа група, за срок до шест месеца до получаване на резултата от проверката, предвидена в подточка 12.11 от настоящия раздел. Временните разрешения, издадени по този начин, не разрешават достъп до информация с ниво на класификация TRÈS SECRET UE/EU TOP SECRET или с еквивалентно ниво на класификация.

*ПРИЛОЖЕНИЕ II*

**УВОД**

Настоящите разпоредби определят насоките за сигурност, с които се урежда и гарантира сигурното третиране и управление на поверителната информация от Европейския парламент. Тези насоки за сигурност, в съчетание с инструкциите за обработка, съставят система на Европейския парламент за управление на сигурността на информацията (СУСИ), посочена в член 3, параграф 2 от настоящото решение.

**НАСОКА ЗА СИГУРНОСТ 1**

**Организацията на сигурността в Европейския парламент за защита на поверителната информация**

**НАСОКА ЗА СИГУРНОСТ 2**

**Управление на поверителна информация**

**НАСОКА ЗА СИГУРНОСТ 3**

**Обработката на поверителна информация посредством автоматизирани комуникационни и информационни системи (КИС)**

**НАСОКА ЗА СИГУРНОСТ 4**

**Физическа сигурност**

**НАСОКА ЗА СИГУРНОСТ 5**

**Индустриална сигурност**

**НАСОКА ЗА СИГУРНОСТ 6**

**Нарушаване на сигурността, загуба или компрометиране на поверителна информация**

**НАСОКА ЗА СИГУРНОСТ 1**

ОРГАНИЗАЦИЯТА НА СИГУРНОСТТА В ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ ЗА ЗАЩИТА НА ПОВЕРИТЕЛНАТА ИНФОРМАЦИЯ

1. Генералният секретар е отговорен за цялостното и последователно прилагане на настоящото решение.

Генералният секретар предприема всички необходими мерки, за да се гарантира, че за целите на обработката и съхраняването на поверителна информация настоящото решение се прилага в помещенията на Европейския парламент от членове на Европейския парламент, от длъжностни лица на Европейския парламент и от други служители на Парламента, които работят за политически групи, както и от изпълнители.

2. Генералният секретар е органът по сигурността. В това си качество генералният секретар е отговорен за:

2.1. координацията на всички въпроси на сигурността, свързани с дейностите на Парламента, и във връзка със защитата на поверителната информация;

2.2. одобряване на изграждането на обезопасена зона, обезопасени читални и обезопасено оборудване;

2.3. прилагане на решения за разрешаване, в съответствие с член 6 от настоящото решение, на предаване на класифицирана информация от Парламент на трети лица;

2.4. разследване или възлагане на разследване във връзка с изтичане на поверителна информация, което е било извършено prima facie в Парламента, в сътрудничество с председателя, когато това засяга член на Европейския парламент;

2.5. поддържане на тесни връзки с органите по сигурността на другите институции на Съюза и с националните органи по сигурността в държавите членки с цел гарантиране на оптимална координация на политиката по сигурността във връзка с поверителната информация;

2.6. извършване на непрестанен преглед на политиката и процедурите на Парламента по отношение на сигурността и представяне на съответни препоръки, произтичащи от този преглед;

2.7. докладване до националния орган по сигурността (НОС), който е извършил процедурата за проверка за надеждност, в съответствие с приложение I, част 2, подточка 11.3, ако става въпрос за неблагоприятна информация, която може да окаже въздействие върху този орган;

3. Ако са засегнати членове на Европейския парламент, генералният секретар изпълнява своите отговорности в тясно сътрудничество с председателя на Европейския парламент.

4. При изпълнението на своите отговорности в съответствие с параграфи 2 и 3 генералният секретар се подпомага от заместник генералния секретар, Дирекцията по охраната и оценка на риска, Дирекцията за информационни технологии (ДИТ) и Отдела за класифицирана информация (ОКИ),

4.1. Дирекцията по охраната и оценка на риска отговаря за личните мерки за защита, по-конкретно за процедурата за разрешение за достъп, както това е определено в приложение I, част 2. Дирекцията по охраната и оценка на риска също така:

а) е звеното за контакт за органите по сигурността на другите институции на Съюза и за НОС по въпроси, свързани с процедурите за проверка за надеждност на членовете на Европейския парламент, длъжностните лица на Европейския парламент и другите служители на парламента, които работят за политически групи;

б) предоставя необходимата обща информация, свързана със сигурността, относно задълженията за защита на класифицираната информация и относно последствията от всяко неизпълнение на тези задължения;

в) наблюдава функционирането на обезопасената зона и обезопасените читални в помещенията на Парламента в сътрудничество, когато това е уместно, със службите по сигурността на други институции на Съюза и на НОС;

г) извършва одит в сътрудничество с органите по сигурността на други институции на Съюза и с НОС, на процедурите за управление и съхранение на класифицирана информация, обезопасената зона и обезопасените читални в помещенията на Парламента, в които се извършва обработка на класифицирана информация;

д) предлага на генералния секретар подходящи инструкции за обработка;

4.2. ДИТ отговаря за обезопасените информационно-технологични системи за обработка на поверителна информация от Европейския парламент чрез сигурни системи за информационни технологии.

4.3. ОКИ отговаря за:

а) установяване на свързаните със сигурността потребности за ефективна защита на поверителната информация в тясно сътрудничество сс Дирекцията за сигурност и оценка на риска и ДИТ, както и със службите по сигурността на другите институции на Съюза;

б) определяне на всички аспекти на управлението и съхранението на поверителна информация в помещенията на Парламента, както това е изложено в инструкциите за обработка;

в) функционирането на обезопасената зона;

г) управлението или проучването на поверителна информация в обезопасената зона или в обезопасената читалня на ОКИ) в съответствие с член 7, параграфи 2 и 3 от настоящото решение;

д) управлението на регистъра на ОКИ;

е) докладване до органа по сигурността на всяко доказано или предполагаемо нарушаване на сигурността, загуба или компрометиране на поверителна информация, депозирана в ОКИ и съхранявана в обезопасената зона или в обезопасената читалня на ОКИ.

5. Освен това в качеството си на орган по сигурността генералният секретар назначава следните органи:

а) орган по акредитиране на сигурността (ОАС);

б) оперативен орган за осигуреност на информацията;

в) орган за разпределение на криптографски материали;

г) орган по Tempest (ОТ);

д) орган за осигуреност на информацията;

За тези функции не са необходими самостоятелни организационни единици. Единиците имат самостоятелни мандати. Функциите обаче и съпътстващите ги отговорности могат да бъдат комбинирани или интегрирани в една и съща организационна единица или разделени в различни организационни единици, при условие че се избягват конфликти на интереси или дублиране на задачи.

6. Органът по акредитиране на сигурността предоставя експертни съвети по всички въпроси на сигурността, свързани с акредитацията на всяка информационна и технологична система и мрежа на територията на Парламента чрез:

6.1. гарантиране, че комуникационните и информационните системи (КИС) спазват съответните политики за сигурност и насоки за сигурност, предоставяне на декларация за одобрение на КИС за работа с класифицирана информация до определено ниво на класификация в съответната оперативна среда, като се посочват редът и условията за акредитация, както и критериите, според които се изисква повторно одобрение;

6.2. установяване на процес за акредитация на сигурността в съответствие с разработените политики, като ясно посочва условията за одобрение на подчинената му КИС;

6.3. изготвяне на стратегия за акредитация на сигурността, която да определя степента на задълбоченост при процеса на акредитация, която да съответства на необходимото равнище на осигуреност;

6.4. преглед и одобряване на документация, свързана със сигурността, включително декларации за управление на риска и за остатъчен риск, документация за удостоверяване на изпълнението на мерките за сигурност и оперативните процедури за сигурност, както и гарантиране на съответствието на тази документация с правилата и политиките на Парламента в областта на сигурността;

6.5. проверка на прилагането на мерките за сигурност по отношение на КИС чрез предприемане или спонсориране на оценки, проверки или прегледи по сигурността;

6.6. определяне на изискванията за сигурност (например нива на разрешение за достъп на персонала) за чувствителни от гледна точка на КИС длъжности;

6.7. одобряване или, когато е уместно — участие в съвместно одобряване на взаимната свързаност на дадена КИС с други КИС;

6.8. одобряване на стандартите за сигурност на техническото оборудване, предназначено за обезопасена обработка и защита на класифицирана информация;

6.9. гарантиране, че криптографските продукти, използвани в Парламента, са включени в списъка на одобрени от ЕС продукти; както и

6.10. даване на консултации на доставчика на системата, участниците в областта на сигурността и представители на ползвателите относно управлението на риска за сигурността, по-конкретно на остатъчния риск, както и относно реда и условията на декларацията за одобрение.

7. Оперативният орган по осигуреност на информацията отговаря за:

7.1. разработване на документация по сигурността в съответствие с политиките и насоките за сигурност, по-конкретно включително декларацията за остатъчен риск, оперативните процедури за сигурност и криптографския план в рамките на процеса на акредитация на КИС;

7.2. участие в избора и изпитването на специфичните за системата мерки, уреди и софтуер за техническа сигурност, с цел контрол на прилагането им и гарантиране, че те са инсталирани, конфигурирани и поддържани съгласно съответната документация по сигурността;

7.3. наблюдение на изпълнението и прилагането на оперативните процедури за сигурност и, когато е уместно, делегиране на отговорности, свързани с оперативната сигурност, на собственика на системата, а именно на ОКИ;

7.4. управление и работа с криптографски продукти, осигуряване на грижливото съхранение на криптографски и контролирани елементи, като при необходимост осигурява генерирането на криптографски променливи;

7.5. провеждане на аналитични прегледи и изпитвания на сигурността, по-специално за съставяне на съответните доклади за риска съгласно изискванията на ОАС;

7.6. предоставяне на специфично за КИС обучение за целите на осигуреността на информацията;

7.7. въвеждане и прилагане на специфични за КИС мерки за сигурност.

8. Органът за разпределение на криптографски материали (ОРКМ) отговаря за:

8.1. управление и отчитане на криптографски материали на ЕС;

8.2. гарантиране, в тясно сътрудничество с ОАС, че се прилагат подходящи процедури и че са създадени планове за отчитане, защитена работа, съхранение и разпределение на всички криптографски материали на ЕС; както и

8.3. осигуряване предаването на криптографски материали на ЕС на или от лицата или службите, които ги използват.

9. Органът по Tempest отговаря за осигуряване на съответствие на КИС с политиките и инструкциите за обработка по Tempest. Той одобрява контрамерки по Tempest за инсталации и продукти за защита на класифицирана информация до определено ниво на класификация за сигурност в съответната оперативна среда.

10. Органът за осигуреност на информацията е отговорен за всички аспекти на управлението и работата с поверителна информация в помещенията на Парламента и по-конкретно за:

10.1 разработване на сигурност за осигуреността на информацията и насоки за сигурност и наблюдение на тяхната ефективност и целесъобразност;

10.2. опазване и администриране на техническата информация, свързана с криптографските продукти;

10.3. гарантиране, че избраните за защита на класифицирана информация мерки за осигуреността на информацията съответстват на политиките, уреждащи тяхната пригодност и избор;

10.4. гарантиране, че криптографските продукти се подбират в съответствие с политиките, уреждащи тяхната пригодност и избор;

10.5. консултиране с доставчика на системата, участниците в областта на сигурността и представители на потребителите по отношение на сигурността на осигуреността на информацията.

**НАСОКА ЗА СИГУРНОСТ 2**

УПРАВЛЕНИЕ НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ

А. **УВОД**

1. Настоящата насока за сигурност определя разпоредбите да управлението от Парламента на поверителна информация.

2. Когато създава поверителна информация, създателят оценява равнището на поверителност и взема решение въз основа на принципите, определени в настоящата насока, относно класификацията или маркирането на тази информация.

Б. **КЛАСИФИКАЦИЯ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС**

3. Решението за класификация на документ се взема преди създаването на документа. За тази цел класифицирането на информация като класифицирана информация на ЕС включва предварителна оценка на нивото на нейната поверителност и решение от страна на създателя, че неразрешеното оповестяване на тази информация би могло да се отрази в определена степен неблагоприятно на интересите на Съюза или на една или повече от държавите членки или на отделни лица.

4. След вземането на решение за класификация на информацията следва втора предварителна оценка, за да се определи подходящото ниво на класификация. Класификацията на документа се определя от нивото на чувствителност на неговото съдържание.

5. Отговорността за класифициране на информация се носи изцяло от създателя на съответната информация. Длъжностни лица на Парламента извършват класификация по указания на генералния секретар или вследствие на делегиране на правомощия от негова страна.

6. Класификацията се използва правилно и умерено. Създателят на подлежащ на класификация документ се въздържа от всякаква склонност към определяне на прекомерно висока или недостатъчно висока степен на класификация.

7. С нивото на класификация, което се дава на информацията, се определя нивото на защита, което ще ѝ бъде осигурено по отношение на изискванията за сигурност на персонала, физическа и процедурна сигурност и осигуреност на информацията.

8. Информацията, за която има основания да бъде класифицирана, се маркира и обработва като такава, независимо от формата, под която е представена. Получателите на тази информация са ясно информирани за нейното класифициране или чрез маркиране с маркировка за сигурност (ако тя се предоставя в писмена форма — на хартиен носител или чрез КИС), или чрез обявяване (ако тя се предоставя в устна форма — в разговор или заседание при закрити врата). Класифицираните материали се обозначават със знак, така че това да позволи лесното идентифициране на класификацията за сигурност.

9. Класифицирана информация на ЕС (КИЕС) в електронна форма може да бъде създавана само в акредитирани КИС. Самата класифицирана информация, както и наименованието на файла и устройството за съхранение (ако е външно, например компакт диск или устройство с външна памет (USB)), носят съответната маркировка за сигурност.

10. Информацията се класифицира веднага след като бъде създадена под определена форма. Например личните бележки, проекти или електронни съобщения, съдържащи информация, за която има основания да бъде класифицирана, следва да бъдат маркирани като КИЕС от самото начало и се изготвят и обработват в съответствие с настоящото решение и неговите инструкции за обработка по отношение на физическата и техническата сигурност. След това тази информация може да се превърне в официален документ, който на свой ред да бъде маркиран и обработван по подходящ начин. По време на процеса на съставяне може да е необходимо даден официален документ да бъде преоценен и да му се определи по-високо или по-ниско ниво на класификация в процеса на развитието му.

11. Създателят може да реши да определи стандартно ниво на класификация за категориите информация, които редовно създава. Въпреки това той трябва да се увери, че с това не дава систематично по-високо или по-ниско ниво на класификация от необходимото на отделни части от информацията.

12. КИЕС винаги е обозначена с маркировка за сигурност, която съответства на нивото на класификация за сигурност.

Б.1. ***Нива на класификация***

13. Всяка КИЕС се класифицира на някое от следните нива:

— „TRÈS SECRET UE/EU TOP SECRET“, съгласно определението в член 2, буква г) от настоящото решение, когато нейното компрометиране би могло:

а) да застраши пряко вътрешната стабилност на Съюза или на една или повече държави членки или трети държави или международни организации,

б) да причини изключително сериозна вреда на отношенията с трети държави или международни организации,

в) да доведе пряко до мащабни загуби на човешки живот,

г) да причини изключително сериозна вреда на оперативната ефективност или сигурността на развърнатия личен състав на държавите членки или на други участници, или на непрекъснатата ефективност на изключително важни операции за сигурност или разузнавателни операции,

д) да причини тежка и дълготрайна вреда на икономиката на Съюза или на държава членка;

— „SECRET UE/EU SECRET“, съгласно определението в член 2, буква г) от настоящото решение, когато нейното компрометиране би могло:

а) да доведе до значително повишаване на международното напрежение,

б) да причини сериозна вреда на отношенията с трети държави и международни организации,

в) да застраши пряко човешки живот или да навреди сериозно на обществения ред или на индивидуалната сигурност или свобода,

г) да причини вреда на важни търговски или политически преговори, като създаде значителни оперативни проблеми за Съюза или държавите членки,

д) да причини сериозна вреда на оперативната сигурност на държавите членки или на ефективността на много важни операции за сигурност или разузнавателни операции,

е) да причини съществена материална вреда на финансовите, паричните, икономическите и търговските интереси на Съюза или на държава членка,

ж) да наруши съществено финансовата жизнеспособност на големи организации или оператори,

з) да попречи сериозно на развитието или провеждането на политики на ЕС със значителни икономически, търговски или финансови последици;

— „CONFIDENTIEL UE/EU CONFIDENTIAL“, съгласно определението в член 2, буква г) от настоящото решение, когато нейното компрометиране би могло:

а) да причини значителна вреда на дипломатическите отношения, например да доведе до официален протест или други санкции,

б) да застраши индивидуалната сигурност или свобода,

в) да изложи на сериозен риск резултатите от търговските или политическите преговори; да създаде оперативни проблеми за Съюза или на една или повече негови държави членки,

г) да причини вреда на оперативната сигурност на една или повече държави членки или на ефективността на операции за сигурност или разузнавателни операции,

д) да наруши съществено финансовата жизнеспособност на големи организации или оператори,

е) да попречи на разследването или да улесни извършването на престъпна или терористична дейност,

ж) да навреди съществено на финансовите, паричните, икономическите и търговските интереси на Съюза или на държави членки,

з) да попречи сериозно на развитието или провеждането на политики на Съюза със значителни икономически, търговски или финансови последици;

— „RESTREINT UE/EU RESTRICTED“, съгласно определението в член 2, буква г) от настоящото решение, когато нейното компрометиране би могло:

а) да се отрази неблагоприятно на общите интереси на Съюза,

б) да повлияе неблагоприятно на дипломатическите отношения,

в) да причини съществена вреда на отделни лица или дружества,

г) да постави Съюза или държави членки в неизгодно положение при провеждането на търговски или политически преговори,

д) да затрудни поддържането на ефективна сигурност в рамките на Съюза или държави членки,

е) да попречи на ефективното разработване или провеждане на политиките на Съюза,

ж) да наруши правилното управление на Съюза и на неговите операции,

з) да наруши ангажиментите, поети от Парламента за запазване на класифицирания статут на информацията, предоставена от трети страни,

и) да наруши законово установени ограничения относно разкриването на информация,

й) да причини финансови загуби или да улесни неправомерното получаване на печалби или преимущества от отделни лица или дружества,

к) да навреди на разследването на престъпления или да улесни извършването на такива.

Б.2. ***Класификация на сборници, заглавни страници и извадки***

14. Класификацията на писмо или записка, включващи приложени документи, съответства на най-високото ниво на класификация, определено на едно от техните приложения. Създателят на информация ясно посочва нивото на класификация, което писмото или записката трябва да получат след отделянето им от приложенията. Когато не е необходима класификация на придружаващата бележка/писмо, тя/то включва следната заключителна формулировка: „След отделянето от приложенията настоящата бележка/писмо се декласифицира“.

15. Доколкото е възможно, документите или файловете, съдържащи части с различни нива на класификация, се структурират по начин, който да позволява лесното идентифициране и отделяне, ако това е необходимо, на частите с различни нива на класификация. Нивото, на което се класифицира даден документ или файл, е не по-ниско от най-високото ниво на класификация за сигурност на негов елемент.

16 Отделни страници, параграфи, раздели, приложения, допълнения, прикрепени части и приложения към даден документ могат да изискват различно ниво на класификация и това се извършва по съответен начин. В документи, съдържащи КИЕС, за обозначаване на нивото на класификация на раздели или части от текст, по-малки от една страница, могат да се използват стандартни съкращения.

17. Когато се обединява информация от различни източници, се прави преглед на окончателния продукт, за да се определи цялостното ниво на класификация за сигурност, тъй като може да е необходимо той да бъде с по-високо ниво на класификация от това на съставните му части.

В. **ДРУГА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ**

18. „Другата поверителна информация“ се обозначава в съответствие с раздел Д от настоящата насока за сигурност и инструкциите за обработка.

Г. **СЪЗДАВАНЕ НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ**

19. Единствено лицата, надлежно оправомощени с настоящото решение или получили разрешение от органа по сигурността, могат да създават поверителна информация.

20. Поверителната информация не се добавя в интернет или интранет системи за управление на документите.

Г.1. ***Създаване на КИЕС***

21. За да се създаде КИЕС с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET, съответното лице се оправомощава с настоящото решение или първо получава разрешение в съответствие с член 4, параграф 1 от настоящото решение.

22. КИЕС с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET се създава единствено в рамките на обезопасената зона.

23. За създаването на КИЕС се прилагат следните правила:

а) върху всяка страница се отбелязва ясно приложимото ниво на класификация;

б) всяка страница се номерира и се посочва общият брой на страниците;

в) документът има регистрационен номер на първата страница и предмет, които сами по себе си не представляват класифицирана информация, освен ако не са обозначени като такава;

г) документът има дата на първата страница;

д) първата страница на всеки документ с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET съдържа списък на всички приложения и притурки;

е) на всяка страница на документите с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET се обозначава номерът на копието, ако документите се разпространяват в няколко екземпляра; на първата страница на всяко копие се посочва общият брой на копията и страниците; и

ж) ако документът се позовава на други документи, съдържащи класифицирана информация, която е получена от други институции на Съюза, или ако съдържа класифицирана информация, произтичаща от тези документи, той има същото ниво на класификация като тези документи и не може, без предварителното писмено съгласие на създателя си, да бъде разпространяван на лица, различни от упоменатите в списъка за разпространение във връзка с оригиналния документ или документите, съдържащи класифицирана информация.

24. Създателят на информация запазва контрол върху КИЕС, която е създал. От него се иска съгласие в писмена форма, преди КИЕС да:

а) бъде декласифицирана или да претърпи понижаване на нивото на класификация;

б) се използва за цели, различни от установените от създателя;

в) бъде разкрита на трети държави или международни организации;

г) бъде разкрита на лица, институции, държави или международни организации, различни от адресатите, които са първоначално оправомощени от създателя да правят справки с въпросната информация;

д) бъде разкрита на изпълнител или потенциален изпълнител, установен в трета държава;

е) бъде копирана или преведена, ако информацията е с ниво на класификация TRES SECRET UE/EU TOP SECRET;

ж) бъде унищожена.

Г.2. ***Създаване на друга поверителна информация***

25. Генералният секретар, който действа в качеството на орган по сигурността (SA), може да реши дали да разреши или не създаването на „друга поверителна информация“ от дадена функция, служба и/или лице.

26. „Друга поверителна информация“ се обозначава с една от маркировките, определени в инструкциите за обработка.

27. За създаването на „друга поверителна информация“ се прилагат следните правила:

а) обозначението ѝ се посочва в горната част на първата страница на документа;

б) всяка страница се номерира и се посочва общият брой на страниците;

в) документът има регистрационен номер на първата страница и предмет;

г) документът има дата на първата страница и;

д) последната страница на документа съдържа списък на всички приложения и притурки.

28. Създаването на „друга поверителна информация“ подлежи на специфични правила и процедури, установени в инструкциите за обработка.

Д. **ОБОЗНАЧЕНИЯ И МАРКИРОВКИ ЗА СИГУРНОСТ**

29. Обозначенията и маркировките за сигурност върху документите целят да контролират потока на информацията и да ограничат достъпа до поверителна информация въз основа на принципа „необходимост да се знае“.

30. Когато се използват или се поставят обозначения и/или маркировки за сигурност, се полагат грижи да се избегне объркването с класификациите за сигурност за КИЕС: „RESTREINT UE/EU RESTRICTED“, „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“, „TRES SECRET UE/EU TOP SECRET“.

31. В инструкциите за обработка се установяват специфични правила относно използването на обозначения и маркировки за сигурност, заедно със списъка на одобрените от Европейския парламент маркировки за сигурност.

Д.1. ***Обозначения за сигурност***

32. Обозначенията за сигурност могат да се използват само в съчетание с ниво на класификация за сигурност и не се прилагат отделно за документите. За КИЕС може да се прилага обозначение за сигурност с цел:

а) определяне на срока на валидност на дадена класификация (за класифицирана информация, обозначаваща автоматично понижаване на нивото на класификацията или премахване на класификацията);

б) ограничаване на въпросното разпространение на КИЕС;

в) установяване на специални условия за обработка, в допълнение към тези, които съответстват на нивото на класификация за сигурност.

33. Допълнителните проверки, приложими за обработката и съхранението на документи, съдържащи КИЕС, налагат допълнителна тежест на всички участници. За да се сведе до минимум работата, която е необходима в тази връзка, добра практика е при създаването на подобен документ да се установи срок или събитие, след което класификацията се прекратява автоматично и се понижава или премахва класификацията на съдържащата се в документа информация.

34. Когато даден документ касае специфична област на работа и разпространението му трябва да бъде ограничено и/или да подлежи на специални условия за обработка, към класификацията му може да се добави декларация в този смисъл с цел да се спомогне за идентифицирането на целевата му аудитория.

Д.2. ***Маркировки***

35. Маркировките не представляват класификация за сигурност. Те са предназначени да служат единствено за предоставянето на конкретни инструкции за обработката на даден документ и не се използват за описание на съдържанието на този документ.

36. Маркировките могат да се прилагат отделно за документите или да се използват в съчетание с ниво на класификация за сигурност.

37. Като общо правило, маркировките се прилагат за информация, обхваната от професионалната тайна, посочена в член 339 от ДФЕС и в член 17 от Правилника за длъжностните лица), или за информация, която трябва да бъде защитена от Парламента по правни съображения, но не е необходимо или не може да бъде класифицирана.

Д.3. ***Използване на маркировки в КИС***

38. Правилата относно използването на маркировки се прилагат и в акредитираната КИС.

39. ОАС определя специфични правила относно използването на маркировки в акредитираната КИС.

Е. **ПОЛУЧАВАНЕ НА ИНФОРМАЦИЯ**

40. Единствено ОКИ има право в рамките на Парламента да получава от трети лица информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво на класификация.

41. При информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво на класификация и „друга поверителна информация“ ОКИ или компетентният парламентарен орган/титуляр на мандатна длъжност може да отговаря за получаването ѝ от трети страни и за прилагането на принципите, определени в настоящата насока за сигурност.

Ж. **РЕГИСТРАЦИЯ**

42. Регистрация означава прилагането на процедури за отбелязване на жизнения цикъл на поверителната информация, включително нейното разпространение, извършване на справки и унищожаване.

43. За целите на настоящата насока за сигурност, „регистър“ означава регистър, в който по-специално се отбелязват датите и часовете, в които поверителната информация:

а) постъпва или напуска съответния секретариат на парламентарния орган/титуляря на мандатна длъжност, или ОКИ, според случая;

б) е достъпна или е предадена на лице, проучено за надеждност; и

в) е унищожена.

44. Създателят на класифицираната информация отговаря за маркирането на първоначалната декларация при създаването на документ, съдържащ подобна информация. Тази декларация се предава на ОКИ, когато документът бъде създаден.

45. Информацията с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво може да се регистрира единствено от ОКИ за целите на сигурността. Информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и „друга поверителна информация“, получена от трети страни, се регистрира от службата, която отговаря за официалното получаване на документа, т.е. или ОКИ или секретариата на парламентарния орган/титуляря на мандатна длъжност, за административни цели. „Другата поверителна информация“, изготвена в рамките на Парламента, се регистрира от създателя, за административни цели.

46. Информацията с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво се регистрира, по-специално:

а) при изготвянето ѝ;

б) при постъпването ѝ в ОКИ и при излизането ѝ от него; както и

в) при постъпването ѝ в КИС и при излизането ѝ от нея.

47. Информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво се регистрира, по-специално:

а) при изготвянето ѝ;

б) при постъпването ѝ в съответния секретариат на парламентарния орган/титуляря на мандатна длъжност, или ОКИ, и при излизането ѝ от него; както и

в) при постъпването ѝ в дадена КИС и при напускането ѝ,

48. Регистрацията на поверителна информация може да се извършва на хартия или в електронни регистри/КИС.

49. За информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и „друга поверителна информация“ се вписва най-малко следното:

а) датата и часът на постъпването и излизането ѝ от съответния секретариат на парламентарния орган/титуляря на мандатна длъжност, или ОКИ, според случая;

б) наименованието на документа, нивото на класификация или маркировка, датата на изтичане на класификацията/маркировката, както и всеки референтен номер, зачислен на документа;

50. За информацията с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво се вписва най-малко следното:

а) датата и часът на постъпването и излизането ѝ от ОКИ;

б) наименованието на документа, нивото на класификация или маркировка, всеки референтен номер, зачислен на документа, както и датата на изтичане на класификацията/маркировката;

в) данните на създателя;

г) справка за самоличността на лицето, получило достъп до документа, и кога е осъществен достъпът от това лице;

д) справка за евентуални копия или преводи на документа;

е) датата и часът, когато евентуални копия или преводи на документа напускат ОКИ или се връщат в него, и подробности за мястото им на изпращане и за лицето, което ги е върнало;

ж) датата и часът на унищожаването на документа и лицето, което го е унищожило, в съответствие с правилата за сигурност на Парламента относно унищожаването; както и

з) премахването и понижаването на класификацията на документа.

51. Регистрите могат да бъдат класифицирани или маркирани по целесъобразност. Регистрите за информацията с ниво на класификация „TRES SECRET UE/EU TOP SECRET“ или с еквивалентно ниво се регистрират на същото ниво.

52. Класифицираната информация може да бъде регистрирана:

а) в един единствен регистър; или

б) в различни регистри в зависимост от нивото на класификация за сигурност, статута на информацията като постъпваща или напускаща и от нейния произход или местоназначение.

53. При електронна обработка в рамките на КИС процедурите по регистрация могат да бъдат извършени посредством инструментите в рамките на самата система, отговарящи на същите като посочените по-горе изисквания. Винаги когато КИЕС напуска периметъра на КИС се прилага описаната по-горе процедура по регистрация.

54. ОКИ поддържа регистри за цялата класифицирана информация, която се предоставя от Парламента на трети страни, както и за цялата класифицирана информация, която се получава в Парламента от трети лица.

55. Когато регистрацията на информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво приключи, ОКИ проверява дали адресатът има валидно разрешение, свързано със сигурността. Когато случаят е такъв, адресатът се уведомява от ОКИ. Справки в класифицирана информация могат да се извършват единствено след регистрацията на документа, който я съдържа.

3. **РАЗПРОСТРАНЕНИЕ**

56. Създателят изготвя първоначалния списък за разпространение за създадената от него КИЕС.

57. Информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и друга поверителна информация, изготвена от Парламента, се разпространява в рамките на Парламента от създателя, в съответствие с приложимите инструкции за обработка и въз основа на принципа „необходимост да се знае“. За информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET, създадена от Парламента в обезопасената зона, списъкът за разпространение (и всички допълнителни указания за разпространението) се предава на ОКИ, който отговаря за неговото управление.

58. Изготвената от Парламента КИЕС може да се разпространява на трети страни единствено от ОКИ, въз основа на принципа „необходимост да се знае“.

59. Поверителната информация, получена от ОКИ или всеки парламентарен орган/титуляр на мандатна длъжност, внесъл искането за това, се разпространява в съответствие с инструкциите, получени от създателя.

И. **ОБРАБОТКА, СЪХРАНЕНИЕ И ИЗВЪРШВАНЕ НА СПРАВКИ**

60. Обработката, съхранението и справките в поверителна информация се извършват в съответствие с насока за сигурност 4 и инструкциите за обработка.

Й. **КОПИРАНЕ/ПИСМЕН ПРЕВОД/УСТЕН ПРЕВОД НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ**

61. Информацията с ниво на класификация „TRES SECRET UE/EU TOP SECRET“ или с еквивалентно ниво не се копира или превежда без предварително писмено съгласие на създателя. Документите, съдържащи информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“ или с еквивалентно ниво или с ниво на класификация „SECRET UE/EU SECRET“ или с еквивалентно ниво, могат да се копират или превеждат по указание на притежателя им, при условие че създателят не е наложил забрана.

62. Всяко копие на документ, съдържащ информация с ниво на класификация „TRES SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET“ или „CONFIDENTIEL UE/EU CONFIDENTIAL“ или с еквивалентно ниво, се регистрира за целите на сигурността.

63. Мерките за сигурност, приложими към оригиналния документ, съдържащ класифицирана информация, се прилагат и за неговите копия и преводи.

64. Документите от Съвета следва да бъдат получавани на всички официални езици.

65. Искания за копия и/или преводи на документи, съдържащи класифицирана информация, могат да бъдат отправяни от създателя или притежателя на копието. Копията на документи, съдържащи информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво, могат да бъдат правени единствено в обезопасената зона и на копирни машини, които са част от акредитирана КИС. Копията на документи, съдържащи информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или еквивалентно ниво и друга поверителна информация, се правят с акредитиран уред за възпроизвеждане в помещенията на Парламента.

66. Всички копия и преводи на всеки документ или части от копия на документи, съдържащи поверителна информация, са подходящо обозначени, номерирани и регистрирани.

67. Не се правят повече от действително необходимия брой копия. Всички копия се унищожават в съответствие с инструкциите за обработка в края на срока за извършване на справки.

68. Достъп до класифицирана информация се предоставя само на устни и писмени преводачи, които са длъжностни лица на Парламента.

69. Устните и писмените преводачи с достъп до документи, съдържащи информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL EU“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво, имат съответното разрешение за достъп до секретни материали.

70. Когато работят по документи, съдържащи информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL EU“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво, устните и писмените преводачи работят в обезопасената зона.

## К. ПОНИЖАВАНЕ НА КЛАСИФИКАЦИЯТА, ДЕКЛАСИФИКАЦИЯ И ПРЕМАХВАНЕ НА МАРКИРОВКАТА НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ

### К.1. *Общи принципи*

71. Поверителна информация се декласифицира, намалява се нивото ѝ на класификация или се премахва маркировката ѝ, когато вече не е необходима защита или тази защита вече не е необходима на първоначалното ниво.

72. Решения за понижаване на нивото на класификация, декласификация или премахване на маркировката на информацията, съдържаща се в документите, изготвени в рамките на Парламента, може също така да се наложи да се вземат по конкретен повод, например, в отговор на искане за достъп от обществеността или друга институция на Съюза, или по инициатива на ОКИ или парламентарния орган/титуляря на мандатна длъжност.

73. При създаване на информацията създателят на КИЕС посочва, когато е възможно, дали нивото на класификация за сигурност на въпросната КИЕС може да бъде понижено или КИЕС може да бъде декласифицирана на определена дата или след конкретно събитие. Когато предоставянето на такава информация не е осъществимо, създателят, ОКИ или парламентарният орган/титулярят на мандатна длъжност, притежаващ информацията, преразглежда нивото на класификация за сигурност на КИЕС най-малко веднъж на всеки пет години. Във всички случаи класификацията на КИЕС може да бъде понижена или премахната само с предварителното писмено съгласие на създателя.

74. В случай че създателят на КИЕС не може да бъде установен или проследен във връзка с документите, изготвени в рамките на Парламента, органът по сигурността преразглежда нивото на класификация за сигурност на съответната КИЕС въз основа на предложение от парламентарния орган/титуляря на мандатна длъжност, притежаващ информацията, който може да се консултира с ОКИ.

75. ОКИ или парламентарният орган/титулярят на мандатна длъжност, притежаващ информацията, носи отговорност за информиране на адресатите на документа за премахването или понижаването на нивото на класификация на информацията, а те на свой ред са отговорни да информират за промяната всички следващи адресати, до които са изпратили или за които са направили копия от документа.

76. Декласификацията, понижаването на класификацията или премахването на маркировката на информацията, съдържаща се в даден документ, се регистрира.

### К.2. *Декласификация*

77. КИЕС може да бъде напълно или частично декласифицирана. Тя може да бъде частично декласифицирана, когато защитата вече не се счита за необходима за конкретна част от документа, който я съдържа, но продължава да бъде оправдана за останалата част от документа.

78. Когато в резултат на преразглеждането на КИЕС, съдържаща се в документ, изготвен в рамките на Парламента, се вземе решение за нейната декласификация, трябва да се разгледа въпросът дали до документа може да бъде предоставен публичен достъп или той да носи обозначение относно разпространението (т.е. да не се предоставя публичен достъп).

79. При декласификация на КИЕС това се вписва в регистъра със следните данни: датата на декласификацията, имената на лицата, поискали и разрешили декласификацията, референтният номер на декласифицирания документ и крайното му местоназначение.

80. Старите маркировки за сигурност в декласифицирания документ и във всички негови копия се зачертават. Документът и всички негови копия се съхраняват по съответния начин.

81. При частична декласификация на класифицирана информация декласифицираната част от него се възпроизвежда и се съхранява по подходящ начин. Компетентната служба регистрира:

а) датата на частичната декласификация;

б) имената на лицата, поискали и разрешили декласификацията; както и

в) референтния номер на декласифицираната част от документа.

К.3. ***Понижаване на нивото на класификация***

82. След понижаване на нивото на класифицираната информация документът, който я съдържа, се вписва в регистрите, отговарящи както на старото, така и на новото ниво на класификация. Вписва се датата на понижаване на нивото на класификация, както и името на лицето, което го е разрешило.

83. Документът, съдържащ информацията с понижено ниво на класификация, и всички негови копия се класифицират с новото ниво на класификация и се съхраняват по подходящ начин.

Л. **УНИЩОЖАВАНЕ НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ**

84. Поверителна информация (както на хартиен носител, така и в електронна форма), която вече не е необходима, се унищожава или заличава, в съответствие с инструкциите за обработка и съответните правила за архивиране.

85. Информацията с ниво на класификация „TRES SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET“ или с еквивалентно ниво на класификация, се унищожава от ОКИ. Това става в присъствието на лице, притежател на разрешение за достъп, отговарящо най-малко на степента на класификация на унищожаваната информация.

86. Информацията с ниво на класификация „TRES SECRET UE/EU TOP SECRET“ или с еквивалентно ниво на класификация се унищожава само с предварително писмено съгласие на създателя на информацията.

87. Информацията с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или с еквивалентно ниво на класификация се унищожава от ОКИ по инструкции на създателя на информацията или от компетентния орган. Регистрационните дневници и другите регистри се актуализират съответно. Информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво на класификация се унищожава и заличава от ОКИ или от съответния парламентарен орган/титуляр на мандатна длъжност.

88. Длъжностното лице, отговарящо за унищожаването, и съответният свидетел, който присъства на унищожаването, подписват удостоверение за унищожаване, което се депозира и архивира в ОКИ. ОКИ съхранява, заедно с формулярите за разпространение, сертификатите за унищожаване на информация с ниво на класификация „TRES SECRET UE/EU TOP SECRET“ или с еквивалентно ниво на класификация за срок от най-малко десет години, а информацията с ниво на класификация „SECRET UE/EU SECRET“ или с еквивалентно ниво и с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“ или с еквивалентно ниво на класификация за срок от най-малко пет години.

89. Документ, съдържащ класифицирана информация, се унищожава чрез методи, отговарящи на съответните стандарти на ЕС или еквивалентни стандарти, така че да не може да бъде възстановен, изцяло или частично.

90. Унищожаването на компютърните средства за съхранение, използвани за класифицирана информация, се извършва съгласно приложимите инструкции за обработка.

91. Унищожаването на регистрираната класифицирана информация се вписва в съответния регистрационен дневник със следните данни:

а) дата и час на унищожаване;

б) име на длъжностното лице, отговарящо за унищожаването;

в) идентифициране на унищожения документ или копия;

г) оригинален физически формат на унищожената класифицирана информация на ЕС;

д) средства за унищожаване; както и

е) място на унищожаване.

M. **АРХИВИРАНЕ**

92. Класифицираната информация, включително придружаващата бележка/писмо, приложенията, разписката за депозиране и другите части от досието, се прехвърлят към обезопасения архив в обезопасената зона шест месеца след извършването на последната справка и най-късно една година след нейното депозиране. Подробни правила за архивирането на класифицирана информация се посочват в инструкциите за обработка.

93. За „другата поверителна информация“ се прилагат общите правила за управление на документи, без да се засягат евентуални други специфични разпоредби относно обработката ѝ.

**НАСОКА ЗА СИГУРНОСТ 3**

ОБРАБОТКАТА НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ ПОСРЕДСТВОМ АВТОМАТИЗИРАНИ КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ СИСТЕМИ (КИС)

A. **ОСИГУРЕНОСТ НА ИНФОРМАЦИЯТА НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ, ОБРАБОТВАНА В ИНФОРМАЦИОННИ СИСТЕМИ**

1. „Осигуреност на информацията“ (ОИ) в областта на информационните системи е увереността, че тези системи ще осигурят защита на класифицираната информация, с която се работи в тях, и че ще функционират както и когато е необходимо, под контрола на легитимни ползватели. Ефективната ОИ гарантира необходимите нива на поверителност, интегритет, наличност, невъзможност за отказ и автентичност. ОИ се основава на процес за управление на риска.

2. „Комуникационна и информационна система“ (КИС) за работа с класифицирана информация означава система, позволяваща работата с информация в електронна форма. Такава информационна система обхваща всички активи, необходими за нейното функциониране, включително инфраструктура, организация, персонал и информационни ресурси.

3. КИС работят с класифицирана информация в съответствие с концепцията за ОИ.

4. КИС преминават процедура за акредитация. Целта на акредитацията е да се гарантира, че са изпълнени всички необходими мерки за сигурност и е постигнато достатъчно ниво на защита на класифицираната информация и на КИС в съответствие с настоящата насока за сигурност. В декларацията за акредитация се определя най-високото ниво на класификация за сигурност на информацията, с което може да се работи в дадена КИС, както и съответните изисквания и условия за това.

5. Следните понятия и характеристики на ОИ имат основно значение за сигурността и правилното протичане на операциите в КИС:

а) Автентичност: гаранцията, че информацията е истинска и произтича от bona fide източници.

б) Достъпност: характеристиката на информацията да е достъпна и използваема при поискване от оправомощена единица.

в) Поверителност: характеристиката, че информацията не се разкрива на неоправомощени лица, единици или процеси.

г) Интегритет: характеристиката, че информацията и активите са запазили точността и пълнотата си.

д) Невъзможност за отказ: способността да се докаже, че дадено действие или събитие действително е настъпило, така че това действие или събитие да не може впоследствие да бъде отречено.

## Б. **ПРИНЦИПИ НА ОСИГУРЕНОСТТА НА ИНФОРМАЦИЯТА**

6. Установените по-долу разпоредби съставляват основните параметри за сигурността на всяка КИС, в която се работи с класифицирана информация. Подробните изисквания за изпълнение на тези разпоредби се определят в политиките и насоките за сигурност.

### Б.1. ***Управление на риска за сигурността***

7. Управлението на риска за сигурността е неразделна част от определянето, разработването, функционирането и поддръжката на КИС. Управлението на риска (оценка, третиране, приемане и съобщаване) се осъществява съвместно, като повтарящ се процес, от представители на собствениците на системата, органите по проекта, оперативните органи и органите за одобрение на сигурността, в съответствие с насока за сигурност 1, чрез използване на доказан, прозрачен и разбираем процес на оценка на риска. Обхватът на КИС и нейните активи се определят ясно в началото на процеса на оценка на риска.

8. Компетентните органи, в съответствие с насока за сигурност 1, правят преглед на потенциалните заплахи за КИС и поддържат актуализирани и точни оценки на заплахите, които отразяват състоянието на оперативната среда към дадения момент. Те постоянно актуализират своите познания по въпросите, свързани с уязвимите места, и периодично правят преглед на оценката на уязвимостта в отговор на променящата се информационно-технологична среда.

9. Целта на третирането на риска за сигурността е да се приложи съвкупност от мерки за сигурност, които да доведат до задоволителен баланс между изискванията на ползвателите, разходите и остатъчния риск за сигурността.

10. Акредитацията на КИС включва формална декларация за остатъчен риск и приемане на остатъчния риск от отговорния орган. Специфичните изисквания, мащаб и степен на задълбоченост, определени от съответния ОАС за акредитация на КИС, съответстват на оценката на риска, като се вземат предвид всички релевантни фактори, включително нивото на класификация на класифицираната информация, с която се работи в КИС.

### Б.2. ***Сигурност през жизнения цикъл на КИС***

11. Гарантирането на сигурността е изискване, което важи през целия жизнен цикъл на КИС, от решението за нейното създаване до извеждането ѝ от експлоатация.

12. Ролята на участниците в КИС и взаимодействието между тях по отношение на сигурността на системата се определят за всеки етап от жизнения цикъл.

13. КИС, включително техническите и нетехническите мерки за нейната сигурност, се подлага на изпитване за сигурност по време на процеса на акредитация, за да се гарантира, че е постигнато необходимото ниво на осигуреност и да се удостовери, че КИС, включително техническите и нетехническите мерки за нейната сигурност, са правилно приложени, интегрирани и конфигурирани.

14. Оценки на сигурността, проверки и прегледи се извършват периодично по време на функционирането и поддръжката на КИС, както и при възникване на извънредни обстоятелства.

15. Документацията по сигурността на КИС се развива по време на жизнения цикъл на системата като неразделна част от процеса за управление на промените.

16. При необходимост изпълняваните от КИС процедури за регистрация се проверяват в рамките на процеса на акредитация.

Б.3. ***Най-добри практики***

17. Органът по осигуреността на информацията (ООИ) развива най-добри практики за защита на класифицирана информация, с която се работи в КИС. Насоките за най-добри практики съдържат технически, физически, организационни и процедурни мерки за сигурност на КИС с доказана ефективност за противодействие на определени заплахи и уязвими места.

18. Защитата на класифицирана информация, с която се работи в КИС, се усъвършенства въз основа на изводите, направени от структурите, ангажирани с осигуреността на информацията.

19. Разпространението и последващото прилагане на най-добри практики допринася за постигане на равностойно ниво на осигуреност на използваните от Секретариата на Парламента КИС, които работят с класифицирана информация.

Б.4. ***Защита в дълбочина***

20. С оглед намаляване на риска за КИС се прилага съвкупност от технически и нетехнически мерки за сигурност, организирани под формата на многослойна защита. Те включват:

а) възпиране: мерки за сигурност, имащи за цел възпиране на евентуален противник, който планира атака срещу КИС;

б) превенция: мерки за сигурност, имащи за цел възпрепятстване или блокиране на атаки срещу КИС;

в) разкриване: мерки за сигурност, имащи за цел откриване на извършена атака срещу КИС;

г) устойчивост: мерки за сигурност, имащи за цел ограничаване на въздействието на извършена атака в рамките на минимално количество информация или активи на КИС и предотвратяване на по-нататъшни вреди; както и

д) възстановяване: мерки за сигурност, имащи за цел възстановяване на сигурната среда за работа на КИС.

Степента на стриктност на тези мерки за сигурност се определя въз основа на оценка на риска.

21. Компетентните органи, установени в насока за сигурност 1, гарантират, че могат да реагират на инциденти, които е възможно да надхвърлят организационните и националните граници по начин, че координират ответните реакции и обменят информация за тези инциденти и свързаните с тях рискове (компютърни способности за реагиране при извънредни обстоятелства).

Б.5. ***Принцип на минималност и най-малко привилегии***

22. С цел да се избегне ненужно излагане на риск, в отговор на оперативните изисквания се прилагат само основни функционални възможности, съоръжения и услуги.

23. На ползвателите и автоматизираните процеси на КИС се дава само такъв достъп, привилегии или разрешения, които са необходими за изпълнение на задачите им, с оглед ограничаване на вредите в резултат от инциденти, грешки или неразрешено използване на ресурси на КИС.

Б.6. ***Повишаване на осведомеността по въпросите на осигуреността на информацията***

24. Познаването на риска и на наличните мерки за сигурност представлява първата линия на защита на сигурността на КИС. По-конкретно всички служители, които имат отношение към жизнения цикъл на КИС, включително ползвателите, разбират:

а) че пропуските в сигурността могат да нанесат значителни вреди на КИС, работещи с класифицирана информация;

б) потенциалната вреда за други системи, която може да бъде предизвикана от взаимната свързаност и взаимната зависимост; както и

в) индивидуалната си отговорност за сигурността на КИС в зависимост от конкретната си роля в рамките на системите и процесите.

25. Обучението и повишаването на осведомеността по въпросите на ОИ са задължителни за всички участващи служители, включително висшето ръководство, членовете на Европейския парламент и ползвателите на КИС, с цел да се гарантира, че те осъзнават своите отговорности по отношение на сигурността.

Б.7. ***Оценка и одобрение на информационно-технологични продукти за сигурност***

26. КИС за работа с информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво са защитени по начин, който да не допуска информацията да бъде компрометирана от неумишлени електромагнитни излъчвания („мерки за сигурност по Tempest“).

27. Когато защитата на класифицираната информация се осигурява от криптографски продукти, такива продукти се удостоверяват от ОАС като одобрени от ЕС криптографски продукти.

28. При предаване на класифицирана информация с електронни средства се използват одобрени криптографски продукти. Въпреки това изискване, при извънредни обстоятелства могат да се прилагат специфични процедури или специфични технически конфигурации, както е посочено в точки 41 — 44.

29. Необходимата степен на доверие в мерките за сигурност, определена като степен на осигуреност, се определя в съответствие с резултатите от процеса на управление на риска, съобразно съответните политики и насоки за сигурност.

30. Степента на осигуреност се удостоверява чрез международно признати или национално одобрени процеси и методологии. Тук се включват преди всичко оценката, контролът и одитът.

31. ОАС одобрява насоките за сигурност при квалифицирането и одобряването на некриптографски информационно-технологични продукти за сигурност.

Б.8. ***Предаване в рамките на обезопасената зона***

32. Когато предаването на класифицирана информация е ограничено в рамките на обезопасената зона, може да се прибегне до некриптирано разпространение или криптиране на по-ниско ниво, в зависимост от резултатите от процеса на управление на риска и с одобрението на ОАС.

Б.9. ***Сигурност на взаимната свързаност на КИС***

33. Взаимна свързаност означава пряка връзка между две или повече информационно-технологични системи за целите на обмен на данни и други информационни ресурси в еднопосочен или многопосочен план.

34. КИС третира всички взаимосвързани информационно-технологични системи като ненадеждни и прилага защитни мерки за контрол на обмена на класифицирана информация с всички останали КИС.

35. По отношение на всички взаимни връзки на КИС с друга информационно-технологична система се спазват следните основни изисквания:

а) изискванията на дейността или оперативните изисквания за такива взаимни връзки се декларират и одобряват от компетентните органи;

б) въпросната взаимна връзка преминава през процес на управление на риска и акредитация и се нуждае от одобрението на компетентната ОАС;

в) по периметъра на КИС се създават системи за защита.

36. Не се допуска взаимна свързаност между акредитирана КИС и незащитена или обществена мрежа, освен в случаите, когато КИС разполага с одобрени системи за защита, инсталирани за тази цел между КИС и незащитената или обществената мрежа. Мерките за сигурност при такива взаимни връзки се разглеждат от компетентния по въпросите на осигуреността на информацията орган и се одобряват от компетентния ОАС.

37. Когато незащитената или обществената мрежа се използва единствено като преносител и данните са криптирани чрез криптографски продукт на ЕС, удостоверен в съответствие с член 27, такава връзка не се счита за взаимна свързаност.

38. Забранява се пряка или каскадна взаимна връзка с незащитена или обществена мрежа на КИС, акредитирана да работи с информация с ниво на класификация „TRES SECRET UE/EU TOP SECRET“ или с еквивалентно ниво или с ниво на класификация „SECRET UE/EU SECRET“ или с еквивалентно ниво. и.

Б.10. ***Компютърни средства за съхранение***

39. Компютърните средства за съхранение се унищожават в съответствие с процедури, одобрени от компетентния орган по сигурността.

40. Компютърните средства за съхранение се използват повторно, понижава се нивото им на класификация или се декласифицират в съответствие с инструкциите за обработка.

Б.11. ***Извънредни обстоятелства***

41. Описаните по-долу специални процедури могат да се прилагат в извънредна ситуация, например в ситуация на предстояща или настояща криза, конфликт, състояние на война или при извънредни оперативни обстоятелства.

42. Класифицираната информация може да се предава, като се използват криптографски продукти, одобрени за по-ниско ниво на класификация за сигурност, или без да се криптира, със съгласието на компетентния орган, в случай че евентуално забавяне би причинило очевидно по-голяма вреда от тази, произтичаща от разкриване на класифицирания материал, и ако:

а) изпращачът и получателят не притежават необходимите уреди за криптиране или не притежават никакви уреди за криптиране; както и

б) класифицираният материал не може да бъде изпратен своевременно с други средства.

43. Класифицираната информация, предавана при описаните в точка 41 обстоятелства, няма маркировки за сигурност или обозначения, които да я отличават от некласифицирана информация или от информация, която може да бъде защитена с наличен криптографски продукт. Получателите се уведомяват незабавно за нивото на класификация с други средства.

44. При прилагане на параграф 41 и 42 се изготвя доклад до компетентния орган.

**НАСОКА ЗА СИГУРНОСТ 4**

ФИЗИЧЕСКА СИГУРНОСТ:

А. **ВЪВЕДЕНИЕ**

Настоящата насока за сигурност определя принципите за сигурност за създаването на сигурна среда за правилно обработване на поверителната информация в Европейския парламент. Тези принципи, включително тези, отнасящи се до техническата сигурност, се допълват от инструкциите за обработка.

Б. **УПРАВЛЕНИЕ НА РИСКА ЗА СИГУРНОСТТА**

1. Рискът по отношение на класифицираната информация се управлява като процес. Този процес има за цел да се установят познатите рискове за сигурността, да се набележат мерки за сигурност с оглед свеждане на такива рискове до приемливо ниво, съгласно изложените в настоящата насока за сигурност основни принципи и минимални стандарти, и да се прилагат тези мерки в съответствие с концепцията за дълбочинна защита, определена в насока за сигурност 3. Ефективността на тези мерки подлежи на постоянна оценка.

2. Мерките за сигурност за защита на класифицираната информация за целия ѝ жизнен цикъл съответстват по-конкретно на нивото на класификацията ѝ за сигурност, формата и обема на съответната информация или материалите, местоположението и конструкцията на структурите, в които се намира класифицираната информация, както и оценката на местно ниво на риска от злонамерени и/или престъпни действия, включително шпионаж, саботаж и тероризъм.

3. Плановете за действие при извънредни ситуации отчитат необходимостта от защита на класифицираната информация в извънредни ситуации, за да се предотврати неразрешен достъп, разкриване или загуба на интегритета или наличността.

4. В плановете за непрекъснатост на дейността се включват мерки за предотвратяване и възстановяване с оглед да се намали въздействието на сериозни системни грешки или инциденти при работа с класифицираната информация и нейното съхранение.

В. **ОБЩИ ПРИНЦИПИ**

5. С нивото на класификация или маркиране, което се дава на информацията, се определя нивото на защита, което ще ѝ бъде осигурено по отношение на физическата сигурност.

6. Информацията, за която има основания да бъде класифицирана, се маркира и обработва като такава, независимо от формата, под която е представена. Получателите на тази информация са ясно информирани за нейното класифициране или чрез маркиране с маркировка за сигурност (ако тя се предоставя в писмена форма — на хартиен носител или чрез КИС), или чрез обявяване (ако тя се предоставя в устна форма — в разговор или презентация). Класифицираните материали се маркират физически, така че това да позволи лесното идентифициране на класификацията за сигурност.

7. При никакви обстоятелства поверителната информация не се чете на публични места, когато би могло да бъде видяна от лице, което не е необходимо да е запознато с нея, напр. влакове, самолети, кафенета, питейни заведения и т.н. Тя не се оставя в хотелски сейфове или стаи, нито без надзор на публични места.

Г. **ОТГОВОРНОСТИ**

8. ОКИ отговаря за гарантиране на физическата сигурност при управлението на поверителната информация, депозирана в неговите обезопасени съоръжения. ОКИ отговаря също така за управлението на обезопасените си съоръжения..

9. Физическата сигурност при управлението на информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и на „другата поверителна информация“ е отговорност на съответния парламентарен орган/титуляр на мандатна длъжност.

10. Дирекцията по охраната и оценка на риска осигурява личната сигурност и разрешенията за достъп, необходими за обезопасената работа с поверителна информация в Европейския парламент.

11. ДИТ предоставя експертни съвети и гарантира, че всички създадени или използвани КИС са в пълно съответствие с насока за сигурност 3 и съответните инструкции за обработване.

Д. **ОБЕЗОПАСЕНИ СЪОРЪЖЕНИЯ**

12. Може да се инсталират обезопасени съоръжения в съответствие с техническите стандарти за сигурност и в съответствие с нивото, дадено на поверителната информация съгласно член 7.

13. Обезопасените съоръжения се удостоверяват от ОАС и валидират от органа по сигурността.

Е. **СПРАВКИ В ПОВЕРИТЕЛНА ИНФОРМАЦИЯ**

14. Когато информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и „друга поверителна информация“ е депозирана в ОКИ и в нея трябва да се направи справка извън обезопасената зона, ОКИ предава копие на надлежно оправомощената служба, която гарантира, че справките и работата с въпросната информация е в съответствие с член 8, параграф 2 и член 10 от настоящото решение и надлежните инструкции за обработка.

15. Когато информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или еквивалентно ниво и „друга поверителна информация“ е депозирана в парламентарен орган/ титуляр на мандатна длъжност, различен от ОКИ, секретариатът на този парламентарен орган/титуляр на мандатна длъжност гарантира, че справките и работата с въпросната информация е в съответствие с член 7, параграф 3, член 8, параграфи 1, 2 и 4, член 9, параграфи 3, 4 и 5, член 10, параграфи 2 до 6 и член 11 от настоящото решение и надлежните инструкции за обработка.

16. Когато трябва да се извърши справка с информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или с еквивалентно ниво в обезопасената зона, ОКИ гарантира, че справките и работата с въпросната информация е в съответствие с членове 9 и 10 от настоящото решение и надлежните инструкции за обработка.

Ж. **ТЕХНИЧЕСКА СИГУРНОСТ**

17. Техническите мерки за сигурност са отговорност на ОАС, който определя в надлежните инструкции за обработка специфичните технически мерки за сигурност, които се прилагат.

18. Обезопасените читални за справки с информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и с „друга поверителна информация“ изпълняват специфичните технически мерки за сигурност, предвидени в инструкциите за обработка.

19. Обезопасената зона включва следните структури:

а) зала за контролиране на достъпа, която се инсталира в съответствие с техническите мерки за сигурност, предвидени в инструкциите за обработка. Достъпът до тази структура се вписва в регистър. Залата за контролиране на достъпа отговаря на високи стандарти по отношение на идентификацията на лицата, които имат достъп, извършването на видеозаписи, предоставянето на безопасно място за съхранение на лични вещи, които не се допускат в обезопасените зали (телефони, химикалки и др.);

б) комуникационна зала за предаване или получаване на класифицирана информация, включително криптирана класифицирана информация, в съответствие с насоката за сигурност 3 и съответните инструкции за обработването на информацията;

в) обезопасен архив, в който се използват отделни одобрени и сертифицирани контейнери за информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“, „CONFIDENTIEL UE/EU CONFIDENTIAL“ и „SECRET EU/EU SECRET“ или с еквивалентно ниво. Информацията с ниво на класификация „TRES SECRET UE/EU TOP SECRET“ или с еквивалентно ниво се поставя в отделна зала в специален сертифициран контейнер. Единственото друго оборудване, което се намира в тази отделена зала, е бюрото, което се използва от ОКИ за работа с архива;

г) регистрационна зала, в която се предоставят необходимите средства, за да се гарантира, че регистрацията може да се извърши на хартиен носител или по електронен път, и която следователно разполага с необходимото обезопасено оборудване за инсталиране на подходящите комуникационни и информационни системи. Единствено регистрационната зала може да съдържа одобрени и акредитирани уреди за възпроизвеждане (за снемане на копия на хартиен носител или в електронен вид). В инструкциите за обработка се уточнява кои уреди за възпроизвеждане са одобрени и акредитирани. В регистрационната зала се предоставя същопространство, необходимо за съхраняване и обработване на акредитирани материали, които да позволяват маркирането, копирането и изпращането на класифицирана информация във физически вид според нивото на класификация. Всички акредитирани материали се определят от ОКИ и се акредитират от ОАС в съответствие с препоръката, получена от оперативния орган по осигуреността на информацията. Регистрационната зала е оборудвана също с акредитиран уред за унищожаване на информация, одобрен за най-високото ниво на класификация, съгласно описанието в инструкциите за обработка. Преводът на информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL EU“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или еквивалентно ниво се извършва в регистрационната зала в целесъобразната и акредитирана система. Регистрационната зала предоставя условия за едновременна работа на максимално двама преводачи по един и същи документ. В залата присъства и служител от ОКИ;

д) читалня за индивидуални справки във връзка с класифицирана информация от надлежно оправомощени лица. В читалнята има достатъчно пространство за две лица, включително за служител от ОКИ, който присъства през цялото време на справката. Нивото на сигурност за тази зала е адекватно за целите на справки в информацията с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или с еквивалентно ниво на класификация. Читалнята може да бъде оборудвана със системата „TEMPEST“, което при необходимост да позволява справка по електронен път, в съответствие с нивото на класификация на съответната информация;

е) заседателна зала, в която могат да се поберат максимално 25 души за целите на обсъждането на информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET EU/EU SECRET“ или с еквивалентно ниво. Заседателната зала предоставя необходимите технически обезопасени и сертифицирани съоръжения за устен превод на и от максимално два езика. Когато не се използва за заседания, заседателната зала може да се използва и като допълнителна читалня за индивидуални справки. В извънредни случаи ОКИ може да разреши на две или повече оправомощени лица да извършат справка, свързана с класифицирана информация, доколкото нивото на разрешението и необходимостта от знаене на информацията са еднакви за всички лица в залата. Не повече от четири лица могат да бъдат допуснати да извършат справка, свързана с класифицирана информация, по едно и също време. Присъствието на служители от ОКИ се засилва;

ж) технически обезопасени зали, в които се помещават цялото техническо оборудване, свързано със сигурността на цялата обезопасена зона, и обезопасените сървъри.

20. Обезопасената зона отговаря на действащите международни стандарти за сигурност и се сертифицира от Дирекцията по охраната и оценка на риска. Обезопасената зона разполага със следното минимално необходимо техническо оборудване в областта на сигурността:

а) алармени системи и системи за контрол на сигурността;

б) оборудване за безопасност и аварийни системи (двупосочна предупредителна система);

в) система за видео наблюдение (CCTV);

г) алармена система против проникване;

д) контрол върху достъпа (включително система за сигурност, използваща биометрични данни);

е) контейнери;

ж) метални каси;

з) електромагнитна защита.

21. Когато са необходими допълнителни технически мерки за сигурност, ОАС може да добави такива, като действа в тясно сътрудничество с ОКИ и след като е взел одобрението на органа по сигурността.

22. Инфраструктурното оборудване може да бъде свързано с общите системи за управление на сградата, в която се намира обезопасената зона. При все това оборудването за сигурност, предназначено за контрол върху достъпа и за целите на ОКИ, е независимо от всички други съществуващи системи в Европейския парламент.

З. **ИНСПЕКЦИИ В ОБЕЗОПАСЕНАТА ЗОНА**

23. Инспекциите в обезопасената зона се извършват редовно от ОАС по искане от страна на ОКИ.

24. ОАС изготвя и актуализира контролен списък с въпроси, които трябва да се проверят по време на инспекцията в съответствие с инструкциите за обработка.

И. **ПРЕНОС НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ**

25. Поверителната информация се пренася, скрита от погледа, и не съдържа признаци за поверителния характер на съдържанието ѝ в съответствие с инструкциите за обработка.

26. Единствено куриери или служители със съответното ниво на разрешение, свързано със сигурността, могат да пренасят информация с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или с еквивалентно ниво.

27. Поверителна информация може да се пренася само от външна поща или на ръка извън сградата единствено в съответствие с условията, предвидени в инструкциите за обработка.

28. Информацията с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или с еквивалентно ниво не се изпраща никога чрез електронна поща или факс, дори чрез „обезопасена“ система за електронна поща или факс машина със система за криптиране. Информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и друга поверителна информация може да се изпраща чрез електронна поща, като се използва акредитирана система за криптиране.

Й. **СЪХРАНЯВАНЕ НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ**

29. Нивото на класификация или маркировка на поверителна информация определя нивото на защита, с която тя се ползва с оглед на нейното съхраняване. Тя се съхранява в сертифицираното за тази цел оборудване в съответствие с инструкциите за обработка.

30. Информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и „другата поверителна информация“:

а) се съхранява в стандартен стоманен шкаф, който се заключва, или в офис или работно помещение, когато тя не се използва на практика;

б) не се оставя без надзор, освен ако тя е надлежно заключена и съхранявана;

в) не се оставя върху бюро, маса и др. по начин, при който неоправомощени лица, напр. посетители, чистачи, служители по поддръжката и др., могат да я прочетат или вземат;

г) не се показва на неоправомощени лица и не се обсъжда с такива лица.

31. Информацията с ниво на класификация „RESTREINT UE/EU RESTRICTED“ или с еквивалентно ниво и „друга поверителна информация“ се съхранява единствено в секретариата на парламентарния орган/титуляря на мандатна длъжност или в ОКИ в съответствие с инструкциите за обработка.

32. Информацията с ниво на класификация „CONFIDENTIEL UE/EU CONFIDENTIAL“, SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET или с по-високо или еквивалентно ниво:

а) се съхранява в обезопасената зона в сейф или в блиндирано помещение. По изключение, например ако ОКИ е затворен, тя може да се съхранява в одобрен и сертифициран сейф на службите по охрана;

б) не се оставя без надзор в рамките на обезопасената зона по което и да време, без първо да е била заключена в одобрен сейф (дори и при най-кратко отсъствие);

в) не се оставя върху бюро, маса и др. по начин, при който неоправомощено лице може да я прочете или вземе, дори ако отговорният служител на Отдела за класифицирана информация присъства в залата.

Когато документ, съдържащ класифицирана информация, се изготвя в електронен вид в рамките на обезопасената зона, компютърът се заключва и не се разрешава достъп до екрана, ако създателят на документа или отговорният служител на ОКИ напусне залата (дори при съвсем кратко отсъствие). Автоматичното блокиране на компютъра след изтичането на няколко минути не се счита за достатъчна мярка.

**НАСОКА ЗА СИГУРНОСТ 5**

ИНДУСТРИАЛНА СИГУРНОСТ

А. **ВЪВЕДЕНИЕ**

1. Настоящата насока за сигурност се отнася единствено до класифицираната информация.

2. В нея се определят разпоредбите за прилагане на общите минимални стандарти по приложение I, част 1 от настоящото решение.

3. „Индустриална сигурност“ е прилагането на мерки за гарантиране на защитата на класифицирана информация от изпълнители или подизпълнители по време на преговори за сключване на договор и през целия жизнен цикъл на класифицираните договори. При такива договори не се допуска достъп до информация с ниво на класификация „TRÉS SECRET UE/EU TOP SECRET“.

4. В качеството си на възложител Европейският парламент гарантира, че при възлагане на класифицирани договори на индустриални или други образувания се спазват минималните стандарти за индустриална сигурност, установени в настоящото решение и посочени в договора.

Б. **ЕЛЕМЕНТИ, СВЪРЗАНИ СЪС СИГУРНОСТТА, В КЛАСИФИЦИРАНИТЕ ДОГОВОРИ**

Б.1. ***Ръководство за класифициране за целите на сигурността***

5. Преди да обяви търг за възлагане на класифициран договор или да възложи такъв договор, Европейският парламент, в качеството си на възложител, определя класификацията за сигурност на информацията, която се предоставя на участниците в търга и на изпълнителите, както и класификацията за сигурност на информацията, която се създава от изпълнителя. За тази цел Европейският парламент изготвя ръководство за класифициране за целите на сигурността, което да се ползва при изпълнението на договора.

6. При определяне на нивото на класификация за сигурност на различните елементи на класифицирания договор се прилагат следните принципи:

а) при изготвяне на ръководството за класифициране за целите на сигурността Европейският парламент взема предвид всички съответни аспекти на сигурността, включително нивото на класификация за сигурност, определено за информацията, която е предоставена и одобрена от създателя на информацията за ползване при изпълнението на договора;

б) общото ниво на класификация за сигурност на договора не може да бъде по-ниско от най-високото ниво на класификация на който и да е от неговите елементи.

Б.2. ***Писмо относно аспектите на сигурността***

7. Свързаните с договора изисквания за сигурност се описват в писмо относно аспектите на сигурността. Когато това е уместно, писмото относно аспектите на сигурността включва ръководството за класифициране за целите на сигурността и представлява неразделна част от класифицирания договор за изпълнение или подизпълнение.

8. В писмото относно аспектите на сигурността се съдържат разпоредби, изискващи от изпълнителя и/или подизпълнителя да спазва минималните стандарти, установени в настоящото решение. Неспазването на тези минимални стандарти може да представлява достатъчно основание за прекратяване на договора.

В.3. ***Инструкции за сигурност на програмата/проекта***

9. В зависимост от обхвата на програмите или проектите, включващи достъп до класифицирана информация на ЕС или обработване или съхранение на тази информация, определеният за управление на програмата или проекта възложител може да изготви специфични инструкции за сигурност на съответната програма или проект.

В. **УДОСТОВЕРЯВАНЕ НА СИГУРНОСТТА НА СТРУКТУРИТЕ**

10. Удостоверението за сигурност на дадена структура се издава от НОС или друг компетентен орган по сигурността на държавата членка, за да се удостовери в съответствие с националните законови и подзаконови актове, че дадена индустриална или друга структура е в състояние да осигури в рамките на структурите си защита на класифицираната информация на ЕС на ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET или негов еквивалент. Това удостоверение се представя на Европейския парламент, в качеството му на възложител, преди на изпълнителя/подизпълнителя или на потенциалния изпълнител или подизпълнител да бъде предоставен или даден достъп до класифицирана информация на ЕС.

11. При удостоверяването на сигурността на дадена структура:

а) се извършва оценка на индустриалната или друга структура като цяло;

б) се извършва оценка на собствеността, контрола и/или потенциала за странично влияние, които могат да се считат за риск за сигурността;

в) се проверява дали индустриалната или друга единица е инсталирала система за сигурност в рамките на структурата, която обхваща всички подходящи мерки за сигурност, необходими за защитата на информация или материал с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, в съответствие с изискванията, установени в настоящото решение;

г) се проверява дали статусът, от гледна точка на сигурността, на ръководството, собствениците и служителите, от които се изисква да имат достъп до информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, е установен съгласно изискванията на настоящото решение;

д) се проверява дали индустриалната или друга структура е назначила служител по сигурността на структурата, който отговаря пред ръководството за прилагане на задълженията в областта на сигурността в рамките на съответната структура.

12. Когато е уместно, Европейският парламент, в качеството си на възложител, уведомява съответния национален орган по сигурността или друг компетентен орган по сигурността, че на предварителния етап или за изпълнението на договора се изисква да се удостовери сигурността на структурата. В рамките на предварителния етап се изисква удостоверение за сигурността на структура или разрешение за достъп на персонала, ако в процеса на представяне на оферта трябва да се предостави класифицирана информация на ЕС с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

13. Възложителят не възлага класифициран договор на предпочитан участник в търга, преди да е получил потвърждение от НОС или друг компетентен орган по сигурността на държавата членка, в която е регистриран съответният изпълнител или подизпълнител, че е издадено съответното удостоверение за сигурност на дадена структура, ако такова удостоверение е необходимо.

14. Всеки компетентен орган по сигурността, издал удостоверението за сигурност на дадена структура, уведомява Европейския парламент, в качеството му на възложител, за всички промени, засягащи удостоверението за сигурност на структурата. При договори за подизпълнение се информира съответно компетентният орган по сигурността.

15. Отнемането на удостоверението за сигурност на дадена структура от съответния национален орган по сигурността или друг компетентен орган по сигурността представлява достатъчно основание за Европейския парламент, в качеството му на възложител, да прекрати класифициран договор или да изключи участник от търга.

## Г. **КЛАСИФИЦИРАНИ ДОГОВОРИ ЗА ИЗПЪЛНЕНИЕ И ПОДИЗПЪЛНЕНИЕ**

16. Когато на участник в търга се предоставя класифицирана информация на ЕС на предварителния етап, поканата за представяне на оферта съдържа разпоредба, задължаваща участниците в търга, които не са представили оферта и/или не са избрани, да върнат всички класифицирани документи в определен срок.

17. След възлагането на класифициран договор за изпълнение или подизпълнение Европейският парламент, в качеството си на възложител, уведомява НОС на изпълнителя и/или подизпълнителя или друг компетентен орган по сигурността за разпоредбите за сигурност на класифицирания договор.

18. При прекратяване на такъв договор Европейският парламент, в качеството си на възложител (и/или по целесъобразност компетентният орган по сигурността при договори за подизпълнение), уведомява своевременно НОС или съответно друг компетентен орган по сигурността на държавата членка, в която е регистриран изпълнителят или подизпълнителят.

19. Като общо правило при прекратяване на класифицирания договор за изпълнение или за подизпълнение изпълнителят или подизпълнителят е длъжен да върне на възложителя цялата класифицирана информация, която му е била предоставена.

20. Конкретните разпоредби за разпореждане с класифицирана информация по време на изпълнението на договора или при неговото прекратяване се посочват в писмото относно аспектите на сигурността.

21. В случаите, в които на изпълнител или подизпълнител е разрешено да задържи класифицирана информация след прекратяване на договора, той продължава да спазва установените в настоящото решение минимални стандарти и да осигурява защита на поверителността на класифицираната информация на ЕС.

22. Условията, при които изпълнителят може да възлага договора за подизпълнение, се определят в условията за търга и в договора.

23. За да предостави за подизпълнение части от класифициран договор, изпълнителят получава разрешение от Европейския парламент в качеството му на възложител. Договор за подизпълнение не може да бъде възлаган на индустриални или други единици, регистрирани в трета държава, която не е сключила споразумение за сигурност на информацията със Съюза.

24. Изпълнителят носи отговорност за осигуряване на спазването на установените в настоящото решение минимални стандарти за сигурност по време на извършването на всички подизпълнителски дейности и не предоставя класифицирана информация на ЕС на подизпълнителя без предварителното писмено съгласие на възложителя.

25. По отношение на класифицираната информация, която е създадена от изпълнител или подизпълнител или с която те работят, правата на създател се упражняват от възложителя.

## Д. **ПОСЕЩЕНИЯ ВЪВ ВРЪЗКА С КЛАСИФИЦИРАНИ ДОГОВОРИ**

26. Когато за целите на изпълнение на класифициран договор е необходимо Европейският парламент, изпълнители или подизпълнители да получат на взаимна основа достъп до информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET в помещенията си, се уреждат посещения, като се поддържа връзка с НОС или друг съответен компетентен орган по сигурността. В контекста на конкретни проекти обаче НОС могат да постигнат също така съгласие по процедура, при която такива посещения да могат да се организират пряко.

27. Всички посетители разполагат със съответното разрешение за достъп и отговарят на изискването за „необходимост да се знае“ за получаване на достъп до класифицирана информация, свързана с договора с Европейския парламент.

28. На посетителите се предоставя достъп единствено до класифицирана информация, свързана с целите на посещението.

## Е. **ПРЕДАВАНЕ И ПРЕНОС НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ**

29. По отношение на предаването на класифицирана информация чрез електронни средства се прилагат съответните разпоредби от насока за сигурност 3.

30. По отношение на преноса на класифицирана информация се прилагат съответните разпоредби от насока за сигурност 4 и съответните инструкции за обработка.

31. При определяне на мерките за сигурност при транспортиране на класифицирани материали като товар се прилагат следните принципи:

а) сигурността се осигурява на всеки етап по време на транспорта от пункта на произход до крайното местоназначение;

б) степента на защита, предоставена за дадена пратка, се определя от най-високото ниво на класификация за сигурност на материала, който се съдържа в нея;

в) за предоставящите транспорта компании се получава удостоверение за сигурността на структурите на съответното ниво. В такива случаи персоналът, обработващ пратката, е бил подложен на проучване за надеждност в съответствие с приложение I;

г) преди трансграничен пренос на материали, класифицирани с ниво CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET или друго равностойно обозначение, изпращачът изготвя план за пренос, който се одобрява от генералния секретар;

д) пътуванията, доколкото това е възможно, се извършват от определена точка на тръгване до определена точка на пристигане и толкова бързо, колкото позволяват обстоятелствата;

е) по възможност маршрутите преминават през територията на държави членки.

Ж. **ПРЕДАВАНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ИЗПЪЛНИТЕЛИ, УСТАНОВЕНИ В ТРЕТИ ДЪРЖАВИ**

32. Класифицирана информация се предава на изпълнители и подизпълнители, установени в трети държави, в съответствие с мерките за сигурност, договорени между Европейския парламент в качеството му на възложител и съответната трета държава, в която е регистриран изпълнителят.

З. **ОБРАБОТКА И СЪХРАНЕНИЕ НА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ „RESTREINT UE/EU RESTRICTED“**

33. Като по целесъобразност поддържа връзка с НОС на съответната държава членка, Европейският парламент в качеството си на възложител има право да извършва посещения на структурите на изпълнителя/подизпълнителя на основание на договорните разпоредби с цел да се увери, че са осъществени съответните мерки за сигурност за защита на класифицирана информация на ЕС с ниво на класификация за сигурност „RESTREINT UE/EU RESTRICTED“, както се изисква съгласно сключения договор.

34. В необходимата съобразно националните законови и подзаконови актове степен НОС или други компетентни органи по сигурността биват уведомявани от Европейския парламент в качеството му на възложител относно договори за изпълнение или подизпълнение, съдържащи информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“.

35. Не се изисква удостоверение за сигурност на структура, нито разрешение за достъп за изпълнители или подизпълнители и техния персонал при договори, възлагани от Европейския парламент, които съдържат информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“.

36. В качеството си на възложител Европейският парламент разглежда оттоворите на поканите за представяне на оферти за договори, изискващи достъп до информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“, независимо от евентуалните изисквания за удостоверяване на сигурността на структурите или разрешаване на достъпа на персонала съгласно националните законови и подзаконови актове.

37. Условията, при които изпълнителят може да възлага договора за подизпълнение, се определят в условията за търга и в договора.

38. Когато един договор включва обработване на информация с ниво на класификация „RESTREINT UE/EU RESTRICTED“ в рамките на комуникационни и информационни системи, с които оперира изпълнител, Европейският парламент в качеството си на възложител гарантира включването в договора за изпълнение или подизпълнение на необходимите технически и административни изисквания за акредитация на комуникационните и информационните системи, съизмерими с оценката на риска, като се вземат предвид всички съответни фактори. Обхватът на акредитацията на тези комуникационни и информационни системи се съгласува между възложителя и съответния НОС.

**НАСОКА ЗА СИГУРНОСТ 6**

НАРУШАВАНЕ НА СИГУРНОСТТА, ЗАГУБА ИЛИ КОМПРОМЕТИРАНЕ НА ПОВЕРИТЕЛНА ИНФОРМАЦИЯ

1. До нарушение на сигурността се стига в резултат на действие или бездействие в разрез с настоящото решение, което може да застраши или компрометира поверителна информация.

2. Компрометиране на класифицирана информация настъпва, когато тя изцяло или отчасти е попаднала у лица, които нямат разрешение за това, т.е. лица, които нито имат съответното разрешение за достъп до секретни материали, нито е „необходимо да знаят“, или когато съществува вероятност това вече да се е случило.

3. Поверителна информация може да бъде компрометирана вследствие на невнимание, небрежност или недискретност, както и вследствие на дейността на служби, чийто обект е Съюзът, или на подривни организации.

4. Когато генералният секретар открие или получи информация за доказано или предполагаемо нарушение на сигурността, загуба или компрометиране във връзка с поверителна информация, той/тя:

а) установява фактите;

б) извършва оценка и свежда до минимум нанесената вреда;

в) предприема мерки за предотвратяване на повторно нарушение;

г) уведомява компетентния орган на третото лице или държавата членка, която е създала или предала поверителната информация.

Ако е засегнат член на Европейския парламент, генералният секретар действа в сътрудничество с председателя на Европейския парламент.

Ако информацията е получена от друга институция на Съюза, генералният секретар действа в съответствие с подходящите за случая мерки за сигурност за класифицирана информация и установените условия, определени съгласно Рамковото споразумение с Комисията или Междуинституционалното споразумение със Съвета.

5. Всички лица, от които се изисква да обработват поверителна информация, биват информирани подробно за процедурите за сигурност, опасностите, свързани с недискретните разговори, и техните отношения със средствата за масово осведомяване и по целесъобразност те подписват декларация, в която заявяват, че няма да разкриват съдържанието на поверителна информация пред трети лица, че ще съблюдават задълженията за защита на класифицираната информация и че съзнават последиците от неспазването на тези изисквания. Достъпът или използването на класифицирана информация от лице, което не е било информирано и което не е подписало съответната декларация, се счита за нарушение на сигурността.

6. Членовете на Европейския парламент, длъжностните лица на Европейския парламент и другите служители на Парламента, работещи за политическите групи, или изпълнителите докладват незабавно на генералния секретар за всяко забелязано от тях нарушение на сигурността, загуба или компрометиране на поверителна информация.

7. Лице, което е отговорно за компрометирането на поверителна информация на ЕС, подлежи на дисциплинарно наказание в съответствие с правилата и разпоредбите в тази област. Тези мерки не засягат предприемането на правни мерки, които може да бъдат предприети в съответствие с приложимото право.

8. Без да се засяга предприемането на други правни мерки, нарушенията, извършени от длъжностни лица на Европейския парламент или от други служители на Парламента, работещи за политическите групи, водят до прилагане на процедурите и санкциите, предвидени в дял IV от Правилника за длъжностните лица на Европейския съюз и Условия за работа на другите служители на Съюза.

9. Без да се засяга предприемането на други правни мерки, нарушенията, извършени от членове на Европейския парламент, се разглеждат в съответствие с член 9, параграф 2 и членове 152, 153 и 154 от Правилника за дейността на Европейския парламент.