

ПЪРВОНАЧАЛЕН БРИФИНГ ЗА РАБОТА С КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Въведение

В изпълнение на Вашите служебни задължения Ви е необходим достъп до класифицирана информация на Европейския съюз.

В този първоначален брифинг по сигурността се посочва задължителния минимум информация, който Вие трябва да знаете, за да работите с класифицирана информация на Европейския съюз във връзка със заеманата от Вас длъжност или изпълняваната задача, които налагат такъв достъп. Необходимо е да познавате Решението на Съвета 2013/488/ЕС от 23 септември 2013 г. относно правилата за сигурност за защита на класифицираната информация на ЕС и Ръководството за защита на класифицираната информация на ЕС, указанията и политиките по тяхното прилагане, които оказват влияние върху вашата ежедневна работа.

Какво е Европейски съюз?

Първата конкретна стъпка към създаването на Европейския съюз е направена на **9 май 1950** г., когато министърът на външните работи на Франция Робер Шуман предлага създаването на Европейската общност за въглища и стомана (ЕОВС). Предложението му влиза в историята като „Декларацията на Шуман“, а датата на предложението – 9 май, се празнува като Ден на Европа. Самата ЕОВС е учредена официално на **18 април 1951** г. с т.нар. Договор от Париж (или Парижки договор), който е подписан от Франция, Федерална република Германия, Италия и трите страни от Бенелюкс – Белгия, Нидерландия и Люксембург; влиза в сила на 23 юли 1952 г. и остава валиден до 23 юли 2002 г. Основната идея е ЕОВС да контролира военната промишленост в Европа, чрез контрол върху добива на двете основни суровини за отрасъла – въглища и стомана. ЕОВС се разглежда като първата международна организация, която се основава на наднационални принципи, и като предшественик на Европейския съюз понастоящем.

На **25 март 1957** г. страните членки на ЕОВС подписват т.нар. Договори от Рим (или Римски договори), с които учредяват две нови организации – Европейската икономическа общност (ЕИО) и Европейската общност за атомна енергия (ЕВРАТОМ).

Европейската икономическа общност се създава, за да гарантира свободното движение на хора, стоки, услуги и капитали, като се премахнат митата, квотите и другите търговски бариери между страните членки. Европейската общност за атомна енергия насърчава използването на атомната енергия за мирни цели.

На **8 април 1965** г. е подписан т.нар. Договор от Брюксел (или Брюкселски договор), с който е въведена обща институционална структура за трите общности –

Европейската общност за въглища и стомана, Европейската икономическа общност и Европейската общност за атомна енергия. Договорът влиза в сила от 1 юли 1967 г. и остава валиден до 1 май 1999 г.

На **7 февруари 1992** г. е подписан Договорът от Маастрихт (или Маастрихтският договор), с който се създава Европейската общност (като обединение от ЕОВС, ЕИО и ЕВРАТОМ). Договорът влиза в сила от 1 ноември 1993 г. По-късно е допълнен и изменен с поредица договори.

На **13 декември 2007** г. е подписан Договорът от Лисабон (или Лисабонски договор), с който се формира Европейският съюз (ЕС) в настоящия му институционален формат. Наред с Римския (1957 г.) и Маастрихтския договор (1992 г.), Договорът от Лисабон (2007 г.) се разглежда като третият договор, който поставя основите на ЕС такъв, какъвто е в момента. Лисабонският договор влиза в сила от 1 септември 2009 г. С него се регулира освен общият пазар, и редица други обществени сфери, вкл. обща политика за сигурност и обща външна политика на държавите членки. Към момента в ЕС членуват общо 28 държави: Австрия, Белгия, България, Великобритания, Германия, Гърция, Дания, Естония, Ирландия, Испания, Италия, Кипър, Латвия, Литва, Люксембург, Малта, Нидерландия, Полша, Португалия, Словакия, Словения, Унгария, Финландия, Франция, Хърватия, Чехия и Швеция.

Символ на Европейския съюз е знаме, което представлява кръг от 12 златни звезди на син фон, то изразява идентичността и единството на държавите членки. Звездите върху него символизират идеалите за единство, солидарност и хармония между народите в Европа.

Съвет на Европейския съюз

Съветът на Европейския съюз (Съвета), заедно с Европейския парламент, Европейския съвет (форумът на лидерите на ЕС), Европейската комисия, е основна институция на ЕС. Той включва министри от всички страни членки, които обсъждат, изменят и приемат закони и координират политики. Министрите имат правомощия да ангажират своите правителства с действията, за които е постигната договореност на срещите. Заедно с Европейския парламент Съветът е основният орган, който взема решения в ЕС. Основните му правомощия са:

- Договаря и приема закони на ЕС заедно с Европейския парламент въз основа на предложения от Европейската комисия;
- Приема годишния бюджет на ЕС съвместно с Европейския парламент;
- Определя външната политика и политиката на сигурност и отбрана на ЕС въз основа на насоките на Европейския съвет;
- Сключва споразумения между ЕС и други държави или международни организации;
- Координира политиките на страните от ЕС;

□ Координира правосъдните системи на страните-членки и по-специално борбата им срещу тероризма.

Съветът на ЕС няма постоянни членове, той заседава в 10 различни конфигурации, като всяка от тях отговаря на областта от политиката, която се обсъжда. В зависимост от конфигурацията всяка страна изпраща министър, който отговаря за съответната област на политиката. Така например, когато се провежда заседание на Съвета по икономически и финансови въпроси (Съвет ECOFIN), на него присъстват финансовите министри на всички страни членки. Всяка страна от ЕС председателства Съвета на ротационен принцип в продължение на 6 месеца.

Национален орган по сигурността

Всяка държава членка на ЕС има Национален орган по сигурността (НОС), отговорен за защитата на класифицираната информация на ЕС. Националният орган по сигурността:

- Отговаря за сигурността на класифицираната информация на ЕС в националните военни или цивилни структури и елементи в страната или чужбина.
- Провежда периодични проверки на мерките за сигурност на класифицираната информация на ЕС във всички национални органи, на всички нива, военни и цивилни, за да установи дали мерките за сигурност са в съответствие с актуалните правила на ЕС за сигурност.
- Гарантира, че е извършена процедура по проучване за надеждност на всички лица, за които се изисква достъп до информация с ниво CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо, в съответствие с Решението на Съвета от 23 септември 2013 г. относно правилата за сигурност за защита на класифицираната информация на ЕС, както и Ръководството за защита на класифицираната информация на ЕС.
- Гарантира, че националните планове за действие при извънредни ситуации са подготвени по начин да предотвратят нерегламентиран достъп до класифицирана информация на ЕС или възможността тя да попадне във враждебни ръце.
- Разрешава откриването или закриването на Централни регистратури TRÈS SECRET UE/EU TOP SECRET, в зависимост от необходимостта и обема от класифицирана информация в организационните единици. За България, Централната регистратура за класифицирана информация на Европейския съюз се намира в Националния орган по сигурността на република България, т. е. в Държавната комисия по сигурността на информацията.

Държавната комисия по сигурността на информацията (ДКСИ) е Национален орган по сигурността на Република България въз основа на международните договорености и притежава изброените по-горе правомощия. Законът за защита на класифицираната информация (ЗЗКИ), приет през 2002 г., ги

конкретизира, като предоставя и други правомощия на ДКСИ за общо ръководство и контрол на мерките по защита както на националната, така и на чуждестранната класифицирана информация, вкл. класифицираната информация на ЕС.

Законът определя ДКСИ като държавен орган, който осъществява политиката на Република България за защита на класифицираната информация, вкл. за защита на класифицираната информация на ЕС (по смисъла на чл. 4, ал. 1 във връзка с чл. 1, ал. 3 от ЗЗКИ).

В качеството си на Национален орган по сигурността (НОС) Комисията организира, осъществява, координира и контролира дейността по защитата на класифицираната информация и осигурява еднаквата ѝ защита (чл. 8 от ЗЗКИ), вкл. организира, осъществява, координира и контролира дейността по защита на класифицираната информация на ЕС и осигурява еднаквата ѝ защита. По-конкретно, ДКСИ:

- организира и осигурява функционирането на регистратурите в областта на международните отношения, респективно Централната регистратура за класифицирана информация на ЕС и регистратури в организационните единици;
- организира, контролира и отговаря за изпълнението на задълженията за защита на класифицираната информация, съдържащи се в международни договори, по които Република България е страна;
- издава сертификати, потвърждаващи пред чуждестранни власти, че български физически или юридически лица притежават разрешение, съответно удостоверение, вкл. по линия на сътрудничеството с ЕС;
- извършва съвместно със службите за сигурност проучване на български граждани, които кандидатстват за заемане на длъжности или за изпълнение на конкретно възложени задачи, налагащи работа с класифицирана информация на друга държава или международна организация, включително ЕС, след постъпване на писмено искане от компетентния орган за сигурност на информацията на съответната държава или международна организация, включително ЕС и комплект от документи, съгласно ЗЗКИ, предоставени от лицето, български гражданин, който има необходимост от достъп до класифицирана информация на ЕС;
- извършва акредитиране на сигурността на национални КИС, предназначени за работа с класифицирана информация на ЕС и точки на присъствие на КИС на ЕС;
- дава разрешения за посещение на лица за извършване на инспекции, провеждани по силата на международни договори за взаимна защита на класифицираната информация, вкл. по линия на ЕС (чл. 9, т. 17 от ЗЗКИ).

Какво е класифицирана информация на ЕС?

Запомнете! Всеки документ или материал, означен с гриф за сигурност на ЕС, представлява класифицирана информация на ЕС, чието неоторизирано

разкриване би могло да увреди в различна степен интересите на Европейския съюз или на една или повече от държавите членки.

Класифицираната информация на ЕС се създава или/и използва при сътрудничеството в рамките на ЕС. Работата с нея е регламентирана в Решението на Съвета 2013/488/ЕС от 23 септември 2013 г. Класифицирането на информацията означава, че достъпът до нея трябва да бъде контролиран, така че да бъде избегнато нерегламентирано разпространение.

Запомнете! Като автор или потребител на класифицирана информация на ЕС, вие също така я съхранявате в ума си. Така че ако имате или сте имали достъп до класифицирана информация на ЕС, трябва да сте особено внимателни относно това кога, къде и с кого обсъждате такава информация.

Въпреки че няма нужда да криете, къде работите, ако ви се налага достъп до класифицирана информация на ЕС, не трябва да я обсъждате:

- с лица, които нямат необходимост да знаят или не притежават необходимото разрешение/сертификат за достъп;
- в заседателни зали, които не са защитени от подслушване;
- в обществени помещения или ситуации, в които може да бъдете чути случайно.

Запомнете! Пазете се от недискретни разговори навсякъде!

Нива на класификация и гриф за сигурност

ЕС има четири нива на класифицирана информация :

- TRÈS SECRET UE/EU TOP SECRET – „Строго секретно на ЕС“;
- SECRET UE/ EU SECRET – „Секретно на ЕС“;
- CONFIDENTIEL UE/ EU CONFIDENTIAL – „Поверително на ЕС“;
- RESTREINT UE/EU RESTRICTED – „За служебно ползване на ЕС“.

TRÈS SECRET UE/EU TOP SECRET. Този гриф за класификация се използва за информация, чието неразрешено разкриване би причинило изключително тежка вреда на съществено важни интереси на ЕС или на една или повече от държавите членки.

SECRET UE/ EU SECRET. Този гриф за класификация се използва за информация, чието неразрешено разкриване би причинило сериозни вреди на ЕС.

CONFIDENTIEL UE/EU CONFIDENTIAL. Този гриф за класификация се използва за информация, чието неразрешено разкриване би нанесло вреда на интересите на ЕС.

RESTREINT UE/EU RESTRICTED. Този гриф за класификация се използва за информация, неразрешеното разкриване на която би било неблагоприятно за интересите на ЕС.

Запомнете! Нивата на класификация на ЕС се изписват едновременно на английски и френски и не се превеждат на друг език.

Документи, които нямат класификация за сигурност, са неклассифицирани.

Правила за работа с информация на ЕС LIMITE

По отношение на разпространението и работата с документи на Съвета, същите се разпределят в 3 категории:

- документи, които нямат маркировка за разпространение или гриф за сигурност, следователно автоматично стават достъпни за обществото;
- документи, които са класифицирани и имат един от четирите грифове за сигурност, съгласно регламентите за сигурност на Съвета, а именно TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL и RESTRIENT UE/EU RESTRICTED;
- документи, които се разпространяват в Съвета, предоставят се на неговите членове, на Европейската комисия и на определени други институции и органи на ЕС. Такива официални документи на Съвета имат поставена маркировка за разпространение LIMITE на заглавната страница и в долната част на листа на последващите страници.

Запомнете! LIMITE не е ниво на класификация или гриф за сигурност, а маркировка за разпространение, ограничаваща вътрешно движението на съответния документ до Съвета и неговите членове, Комисията и някои други институции и организации на ЕС.

Запомнете! Документи с маркировка LIMITE не се публикуват в интернет.

Не е необходимо да се прилагат мерки за техническа защита на документи, маркирани LIMITE при работа или по време на препращането им по информационните системи или мрежи. Когато изпращате по електронна поща документи LIMITE, е необходимо да знаете, че те се адресират, само до потребители, които имат право да ги получат. За документите, маркирани LIMITE не се изискват определени мерки за физическа защита. Такъв вид документи могат

да бъдат унищожени без да се прилагат специални изисквания за физическо унищожаване.

Други маркировки

Класифицираната информация на ЕС може да има и други маркировки в областта на сигурността в допълнение към грифовете за сигурност. Маркировките дават изрични указания как да се обработва или управлява документът или материалът. Тези маркировки сами по себе си не са маркировки за класификация. Например „За предоставяне на трети държави“ е обозначение, определящо условията за предоставяне, знак за идентифициране на създателя на информацията, кодови думи, уточняващи областта, до която се отнася документът, конкретното разпределение на документа в съответствие с принципа „необходимост да се знае“ или ограниченията за ползването му, обозначение на дата или конкретно събитие, след които нивото на класификация може да бъде понижено или премахнато.

Сертификат за достъп до класифицирана информация на ЕС

Служителят по сигурността на информацията ще Ви информира за Вашето ниво на достъп до класифицирана информация на ЕС. Освен това в организационната единица се поддържа поименен списък, в който са посочени нивата на достъп за всяко назначено лице, което има необходимост от сертификат за достъп до класифицирана информация на ЕС.

Запомнете! Достъпът не се определя от заеманата длъжност, ранга или нивото на сертификата за достъп до класифицирана информация на неговия притежател. Достъпът е основан на принципа „необходимост да се знае“ (need-to-know).

Запомнете! Принципът „необходимост да се знае“ се състои в ограничаване на достъпа само до определена класифицирана информация и само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп и които едновременно с това притежават сертификат за достъп със съответното ниво класификация и са преминали инструктаж за достъп до конкретното ниво и вид класифицирана информация на ЕС.

Запомнете! Преди да предоставите достъп на някого, Ваше задължение е да се уверите, че лицето, на което предоставяте достъпа, има сертификат за достъп до конкретен вид или/и ниво на класифицирана информация на ЕС. Това Ваше задължение се отнася до всички форми на предаване на информация, напр. устна, писмена, визуална и електронна. При съмнение, потърсете помощ от вашия ръководител/офицер по сигурността (security officer) или от регистратурата на ЕС.

Запомнете! Само след одобрението на източника на информацията Вие можете да предоставите информация на ЕС на страни и организации, които

не са членки на ЕС. Задължително следва да получите такова предварително одобрение чрез съответния комитет на ЕС.

Преди да им бъде предоставен достъп до класифицирана информация на ЕС, лицата преминават през брифинг относно нейната защита. Ежегодно с тях се провежда и текущ брифинг по теми, свързани с работата с класифицирана информация на ЕС. Брифингите завършват с подписване на декларации, че лицата осъзнават своите отговорности за защита на класифицираната информация на ЕС и последствията, в случай, че тя бъде компрометирана.

За целта, служителят по сигурността на информацията ежегодно изготвя и предоставя за утвърждаване от ръководителя на организационната единица програма и график за първоначално и текущо обучение по защита на класифицираната информация на ЕС на служителите, които имат достъп до такава.

Регистратури за класифицирана информация на ЕС

Във всяка държава членка на Европейския съюз се създава Централна регистратура за осигуряване на контрол и отчетност на класифицираните материали на ЕС при получаването, отчета, обработването, разпространението и унищожаването на такава информация.

Всяка държава членка на ЕС може да създаде Централна регистратура до ниво TRÈS SECRET UE/EU TOP SECRET, действаща като главна точка за приемане и предаване информация на ЕС за съответната държава. Централната регистратура може да изпълнява функции на „обикновена“ регистратура и за друга отчетна информация.

Централната регистратура на ЕС осигурява физическа защита на цялата класифицирана информация на ЕС.

Всички материали с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо се регистрират в определени за целта регистри при постъпването им в Централната регистратура на ЕС и при излизането им от нея.

Централната регистратура на ЕС поддържа регистри на цялата класифицирана информация на ЕС, която се предоставя на Съвета и Генералния секретариат на Съвета на ЕС и на трети държави и международни организации, както и цялата информация, която се получава от тях.

Централната регистратура на ЕС поддържа актуални данни относно цялата класифицирана информация на ЕС, която се съхранява или придвижва в рамките на Централната регистратура на ЕС или преминава към други регистратури на ЕС.

Централната регистратура на ЕС съхранява актуални данни по име за всички лица, на които е предоставен достъп до класифицирана информация на ЕС, съхранявана в централната регистратура на ЕС.

Централна регистратура на ЕС поддържа актуални данни за всички регистратури, с които е оправомощена да обменя класифицирана информация TRÈS SECRET UE/EU TOP SECRET, заедно с имената на назначените завеждащи регистратури TRÈS SECRET UE/EU TOP SECRET.

Централна регистратура на ЕС изпраща класифицирана информация на ЕС TRÈS SECRET UE/EU TOP SECRET само до тези адресати, които имат право на достъп до класифицирана информация TRÈS SECRET UE/EU TOP SECRET.

Запомнете! Регистратурата на Държавната комисия по сигурността на информацията с ниво TRÈS SECRET UE/EU TOP SECRET е Централна регистратура на ЕС за Република България. На територията на Република България организационните единици създават свои регистратури въз основа на своето местонахождение и обема класифицирани материали на ЕС, с които работят.

Създаване на документи с класифицирана информация на ЕС

Когато създавате документ на ЕС, върху всяка страница трябва да отбелязвате ясно нивото на класификация, да номерирате всяка страница, да отбелязвате регистрационния номер на документа и за какво се отнася. Върху документа се поставя дата. На всяка страница на документи с ниво на класификация за сигурност SECRET UE/EU SECRET и по-високо се обозначава номерът на копието, ако документите се разпространяват в няколко екземпляра. Съпроводителните документи следва да бъдат маркирани с класификацията за сигурност на информацията, съдържаща се в тях, когато те са отделно обособени от информацията.

Понижаване нивото на класификация и декласификация

Запомнете! Когато създателят на документа е обозначил, че нивото на класификация на класифицираната информация на ЕС може да бъде понижено или класификацията може да бъде премахната на определена дата, Централната регистратура за класифицирана информация на ЕС е длъжна веднага да изпълни обозначенията, без да уведомява автора.

Централната регистратура на ЕС редовно преразглежда класифицираната информация на ЕС, с която разполага, за да установи дали нивото на класификация продължава да е приложимо.

Централната регистратура за класифицирана информация на ЕС преразглежда нивото на класификация, чийто създател е, не по-рядко от веднъж на пет години. Такъв преглед не се налага, ако от самото начало, създателят е посочил, че нивото на класификация на информацията ще бъде автоматично

понижено или че класификацията ще бъде премахната, и че информацията носи съответното обозначение.

Ако авторът промени класификацията на документа, информира всички адресати. При промяна или премахване нивото на класификация, незабавно се уведомяват всички получатели. Получателите незабавно отбелязват промяната или премахването на грифа за сигурност върху материала и отразяват това обстоятелство в съответните регистри.

Съхранение на материали на ЕС

Общо. Във връзка с изискванията на Решението на Съвета на ЕС относно правилата за сигурност за защита на класифицираната информация на ЕС, всички помещения, сгради, офиси, стаи и други зони, в които се съхраняват и/или обработват класифицирана информация и материали на ЕС, включително зони, в които се помещават комуникационни и информационни системи, трябва да бъдат защитени с подходящи мерки за физическа сигурност.

Материал с гриф RESTREINT UE/EU RESTRICTED може да се съхранява в подходящи заключващи се офис мебели в административна зона или в зона за сигурност. Материалът може да се съхранява временно извън зона за сигурност или административна зона, при условие че притежателят се е ангажирал да спазва мерки, установени в инструкциите за сигурност, издадени от компетентния орган по сигурността, с цел да се гарантира, че класифицираната информация на ЕС е защитена срещу достъп от страна на неоправомощени лица.

Класифицирана информация на ЕС с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се съхранява в зона за сигурност, в сейф или блиндирано помещение.

Класифицирана информация на ЕС с ниво на класификация за сигурност TRÈS SECRET UE/ EU TOP SECRET се обработва в зона за сигурност. Такава информация може да се съхранява в зона за сигурност, когато са приложени допълнителни мерки за контрол:

- постоянна защита или проверки от служители с разрешение за достъп;
- одобрена система против проникване и служители за охрана и реагиране;
- блиндирани помещения, оборудвани със системи против проникване;
- контролиран достъп до стаята или сградата, така че само оторизиран персонал може да получи достъп до информацията.

Всички служители с достъп до каса, която се използва за съхранение на класифицирана информация на ЕС, трябва да бъдат инструктирани и да притежават сертификат за достъп до нивото и вида класифицирана информация на ЕС, която се съхранява в касата.

Комбинации. Управлението на ключовете и шифровите комбинации за офисите, помещенията, блиндираните помещения и сейфовете се променят най-малко на всеки 12 месеца, когато дадена ключалка е преминала през поддръжка

или ремонт, в случай на компрометиране или подозрение за компрометиране на информация, при получаване на нов сейф или когато има смяна на служител, на когото е известна комбинацията.

Важно е да знаете, че шифровите комбинации се запаметяват от възможно най-малък брой лица и в съответствие разбира се с принципа „необходимост да се знае“.

Предаване. За вътрешно или международно предаване на материали с гриф TRÈS SECRET UE/ EU TOP SECRET се използва оторизирана държавна куриерска служба, например: дипломатическа поща или военна куриерска служба. Вътрешното и международното предаване на материали с грифове SECRET UE/EU SECRET и CONFIDENTIEL UE/EU CONFIDENTIAL се извършва от оторизиран куриер или от съответно оторизирани и инструктирани служители, които притежават куриерска идентификация и оторизация или с препоръчана поща. Разписки се изискват за материали SECRET UE/ EU SECRET и CONFIDENTIEL UE/EU CONFIDENTIAL.

Комуникационна и информационна система (КИС)

Комуникационна и информационна система означава всяка система, даваща възможност за работа с класифицирана информация в електронна форма. Една КИС обхваща всички активи, необходими за нейното функциониране, включително инфраструктура, организация, персонал и информационни ресурси. Тези системи следва да гарантират осигуреност на информацията, т. е. защита на информацията, с която се работи в тях. Осигуреността на информацията се основава на процес за управление на риска. Ефективната осигуреност на информацията гарантира необходимите нива на поверителност, достъпност, интегритет, автентичност и невъзможност за отказ.

Поверителност е характеристиката, че информацията не е разкрита на неоправомощени лица, единици или процеси.

Достъпност е характеристиката, че информацията е достъпна и използваема при поискване от оправомощена единица.

Интегритет е характеристиката, че информацията и активите са запазили точността и пълнотата си.

Автентичност е гаранцията, че информацията е истинска и произтича от легитимен източник.

Невъзможност за отказ е 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.

Запомнете! Когато съхранявате, обработвате или пренасяте класифицирана информация в комуникационни и информационни системи, те трябва да притежават валиден сертификат за сигурност до необходимото ниво.

Сертификатът гарантира, че е постигнато необходимото ниво на осигуреност на информацията, с която се работи в нея.

Запомнете! Гарантирането на сигурността е изискване, което важи през целия жизнен цикъл на КИС.

За всяка КИС трябва да има определен Оперативен Орган по Осигуреност на Информацията (ОООИ) и органи по сигурността. Задължение на ОООИ е да изготви документите по сигурността на КИС, включващи Анализ на риска, Специфични изисквания за сигурност и Процедури за сигурност.

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

Запомнете! Всички групи потребители на КИС, преди да получат достъп до необходимите им ресурси на КИС, трябва да бъдат запознати с Процедурите за сигурност на системата и да декларират, че ще спазват описаните в тях задължения.

Унищожаване на класифицирана информация на ЕС

Класифицираната информация, която не е нужна за официални цели, включително излишък, размножена, заместена информация или остатъци от документи и материали, се унищожават по начин, непозволяващ нейното възстановяване.

Унищожаването на документи с ниво на класификация SECRET UE/EU SECRET или TRÈS SECRET UE/EU TOP SECRET се извършва в присъствието на свидетел, който притежава разрешение за достъп до ниво на класификация най-малко на нивото на документа, който се унищожават.

На особен отчет и контрол подлежат материалите с гриф за сигурност TRÈS SECRET UE/EU TOP SECRET. Цялата информация с гриф за сигурност TRÈS SECRET UE/EU TOP SECRET следва да бъде върната в регистратурата, предназначена да я съхранява в готовност за унищожаване. Регистраторът и свидетелят подписват протокол за унищожаване, който се завежда в Централната регистратура на ЕС.

Протоколът за унищожаване на документи с ниво на класификация TRÈS SECRET UE/EU TOP SECRET се съхранява в Централната регистратура на ЕС за срок от най-малко 10 години, а на документи с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET за срок най-малко 5 години.

Класифицирани документи на ЕС, включително документи с ниво на класификация RESTREINT UE/EU RESTRICTED се унищожават така, че да се предотврати цялостното им или частично възстановяване.

Протоколите за унищожаване са задължителни, съгласно националните правила и разпоредби по сигурността.

Запомнете! При извънредна ситуация и наличие на непосредствен риск от нерегламентирано разкриване, класифицираната информация на ЕС се унищожават от нейния притежател по начин, който прави невъзможно цялостното или частичното възстановяване. Авторът на информацията и регистратурата, от която е получена информацията, биват информирани за извънредната ситуация, наложила унищожаването.

Запомнете! Копия от протоколите за унищожаване не се изпращат на автора или на съответната регистратура, освен ако не са специално поискани.

Протоколите трябва да съдържат информация, достатъчна за извършването на оценка на вредите или за осъществяване на разследване по сигурността, за компрометирането или загубата на класифицирана информация на ЕС.

Запомнете! Правилното управление на класифицирана информация на ЕС се разпростира върху целия нейн „жизнен цикъл“, т.е. върху целия процес на нейното съществуване: от създаването, през нейното регистриране, копиране, писмен превод, понижаване на нивото на класификация, декласификация, пренос, унищожаване.

Размножаване, преводи и извлечения. Документите TRÈS SECRET UE/EU TOP SECRET се размножават и превеждат от Централната регистратура, само след писмено разрешение на автора. Централната регистратура докладва за броя на направените копия на автора на документа. Размножаването на информация с ниво SECRET UE/EU SECRET и по-ниско ниво информация може да се извършва от получателя на принципа „необходимост да се знае“ и при условие че източникът на информацията не е ограничил размножаването. Възпроизведените копия се отчитат и съхраняват по същия начин като оригинала.

Мерките за сигурност, приложими към оригиналния документ, се прилагат и за неговите копия и преводи.

Нарушаване на мерките за сигурност и компрометиране на класифицираната информация на ЕС

Нарушение на мерките за сигурност. Нарушението на мерките за сигурност възниква в резултат на действие или бездействие, което е в

противоречие на правилата за сигурност, установени в Решението на Съвета на ЕС, резултатите от които могат да застрашат или изложат на риск класифицираната информацията.

Излагане на риск. Загуба на поверителността, целостта или достъпността на класифицираната информацията, заради нарушение на мерките за сигурност или заради вражески действия като шпионаж, тероризъм, саботаж или кражба. Включва, например, предоставяне или риск от предоставяне на лица без разрешение и физическа загуба или риск от загуба.

Запомнете! Всяко нарушение на сигурността или подозрение за такова нарушение се докладва незабавно на компетентния орган по сигурността.

Когато е известно или когато има достатъчно основания да се приеме, че класифицираната информация на ЕС е компрометирана или изгубена, националният орган по сигурността или друг компетентен орган предприема всички необходими мерки, съгласно съответните закони и подзаконови актове за:

- информиране на създателя на информацията;
- осигуряване на разследване на случая от служители, които нямат непосредствено отношение към нарушението, с оглед установяване на фактите;
- извършване на оценка на потенциалните вреди, причинени на интересите на Съюза или на държавите членки;
- предприемане на необходимите мерки за предотвратяване на повторно нарушение;
- уведомяване на съответните органи за предприетите действия.

Запомнете! На всяко лице, отговорно за нарушение на правилата за сигурност, които са установени в Решението на съвета на ЕС, могат да бъдат наложени дисциплинарни мерки в съответствие с приложимите правила и подзаконови актове. Всяко лице, отговорно за компрометирането или загубата на класифицирана информация на ЕС, подлежи на дисциплинарно и/или съдебно производство в съответствие с приложимите закони, правила и подзаконови актове.

Заплахи за информацията на ЕС

Информация на ЕС е обект на заплахи от шпионаж, саботаж, тероризъм, други злонамерени или престъпни действия, които целят да нанесат вреда на интересите на ЕС или на една или повече от държавите членки.

Информация относно умишлено разкриване на материали на ЕС, опит за шпионаж или действителен шпионаж, насочен срещу информация на ЕС, или действителна или планирана терористична или диверсионна дейност срещу съоръжения или ползватели на класифицирани материали на ЕС трябва да се

докладва веднага на вашия служител по сигурността на информацията или офицера по сигурността. По-долу са представени типичните случаи, които подлежат на докладване:

1. Опити от неоторизирани лица да получат класифицирана информация относно съоръжения, дейности, персонал или материали на ЕС, вкл. чрез задаване на въпроси, извличане на информация (разузнаване), подкупване, заплахи или принуда (насилие) и/или чрез преки или непреки контакти или кореспонденция.

2. Опити от неоторизирани лица да получат класифицирана информация чрез фотографиране, подслушване на телефонни разговори, подслушване, наблюдение или с други средства.

3. Опити от лица с известно, подозирано или възможно чуждестранно разузнавателно минало, връзки или дейности за установяване на приятелски, социални или бизнес отношения или опити да ви задължат чрез специално отношение, услуги, подаръци, пари или други средства.

4. Информация относно терористични планове и дейности, представляващи директна заплаха за съоръжения, персонал или материали на ЕС.

5. Известни или подозирани действия или заговори за увреждане или разрушаване на имущество на ЕС чрез саботаж.

Запомнете! Всеки с достъп до класифицирана информация на ЕС може да бъде потенциална мишена. Ако узнаете за дейности, като описаните по-горе, или някой се обърне към вас директно, за да ви включи в подобни дейности, не забравяйте следното:

1. **Запазете спокойствие!** Не сте виновни, че са Ви избрали за мишена.
2. **Не изразявайте отношение!** Бъдете неопределени дали ще предоставите или няма да предоставите материала или информацията!
3. **Докладвайте за случая веднага!** Дори и да изглежда чисто съвпадение или незначително, малък детайл може да бъде ключът към откриването и парирането на шпионаж, саботаж или терористичен акт. Не обсъждайте инцидента с приятели, семейството, колеги и др., освен ако не е указано от вашия служител по сигурността на информацията/или офицера по сигурността или представител на контраразузнаването!
4. **Никога не е прекалено късно** да докладвате, че сте предоставили материал или информация на неоторизиран получател.
5. **Докладвайте!**

Пътуване в чужбина

Вашите лични пътувания няма да бъдат ограничени само поради факта, че имате достъп до класифицирана информация на ЕС. Ако решите да пътувате до страни с висок риск, Вие трябва да съгласувате с Вашия ръководител, който

разрешава отпуската за пътуване и със служителя по сигурността на информацията и да получите инструктаж за сигурността по време на пътуването.

При завръщане следва да докладвате за всеки случай, който може да е представлявал опит за събиране на информация от особено значение.

Помощ

При проблеми или конкретни въпроси, свързани с класифицираната информация на ЕС, служителят по сигурността на информацията и завеждащият регистратура за класифицирана информация на ЕС, могат да Ви помогнат.