РЕШЕНИЕ НА КОМИСИЯТА

от 4 май 2010 година

относно плана за сигурност за централната ШИС II и комуникационната инфраструктура

(2010/261/ЕС)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. за създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) ([1]), и по-специално член 16 от него,

като взе предвид Решение 2007/533/ПВР на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) ([2]), и по-специално член 16 от него,

като има предвид, че:

(1) Член 16 от Регламент (ЕО) № 1987/2006 и член 16 от Решение 2007/533/ПВР предвиждат, че управителният орган, по отношение на централната ШИС II, и Комисията, по отношение на комуникационната инфраструктура, следва да предприемат необходимите мерки, включително план за сигурност.

(2) Член 15, параграф 4 от Регламент (ЕО) № 1987/2006 и член 15, параграф 4 от Решение 2007/533/ПВР предвиждат, че през преходния период преди управителният орган да поеме своите задължения, Комисията следва да е отговорна за оперативното управление на централната ШИС II.

(3) Тъй като управителният орган все още не е създаден, планът за сигурност, който трябва да бъде приет от Комисията, следва в преходния период да е приложим също и към централната ШИС II.

(4) Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета ([3]) се прилага към обработването на лични данни от Комисията, когато тя изпълнява задълженията си по оперативното управление на ШИС II.

(5) Член 15, параграф 7 от Регламент (ЕО) № 1987/2006 и член 15, параграф 7 от Решение 2007/533/ПВР предвиждат, че когато Комисията делегира своите задължения по време на преходния период преди управителният орган да поеме своите задължения, тя гарантира, че това делегиране не влияе неблагоприятно върху ефективните контролни механизми съгласно правото на Съюза, независимо дали са на Съда, на Сметната палата или на Европейския надзорен орган по защита на данните.

(6) Управителният орган следва да приеме свой собствен план за сигурност по отношение на централната ШИС II, веднага щом поеме своите задължения. Поради това настоящият план за сигурност следва да изтече, доколкото е свързан с централната ШИС II, когато управителният орган поеме своите задължения.

(7) Член 4, параграф 3 от Регламент (ЕО) № 1987/2006 и член 4, параграф 3 от Решение 2007/533/ПВР предвиждат, че ЦС-ШИС, която изпълнява технически надзор и административни функции, е разположена в Страсбург (Франция), а резервната ЦС-ШИС, която в случай на повреда на основната ЦС-ШИС е способна да осигури всички нейни функционалности, е разположена в Санкт Йохан им Понгау (Австрия).

(8) Планът за сигурност следва да предвиди един служител по сигурността на системата, който да изпълнява задачи, свързани със сигурността, както за централната ШИС II, така и за комуникационната инфраструктура и двама местни служители по сигурността, които да изпълняват задачи, свързани със сигурността, съответно за централната ШИС II и за комуникационната инфраструктура. Ролите на служителите по сигурността следва да са определени така, че да осигуряват ефективна и навременна реакция на инциденти по сигурността, както и тяхното докладване.

(9) Следва да бъде определена политика за сигурност, която да описва всички технически и организационни детайли в съответствие с разпоредбите на настоящото решение.

(10) Следва да бъдат дефинирани мерки, които да осигурят необходимото ниво на сигурност на работата на централната ШИС II и на комуникационната инфраструктура,

([1]) ОВ L 381, 28.12.2006 г., стр. 4.
([2]) ОВ L 205, 7.8.2007 г., стр. 63.
([3]) ОВ L 8, 12.1.2001 г., стр. 1.

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

1. Настоящото решение установява организацията и мерките за сигурност (план за сигурност) за защитата на централната ШИС II и на данните, обработвани в нея, срещу заплахи за тяхната наличност, цялост и поверителност по смисъла на член 16, параграф 1 от Регламент (ЕО) № 1987/2006 и член 16, параграф 1 от Решение 2007/533/ПВР относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) през преходния период, докато управителният орган поеме своите задължения.

2. Настоящото решение установява организацията и мерките за сигурност (план за сигурност) за защитата на комуникационната инфраструктура срещу заплахи за нейната наличност, цялост и поверителност по смисъла на член 16 от Регламент (ЕО) № 1987/2006 и член 16 от Решение 2007/533/ПВР относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II).

ГЛАВА II

ОРГАНИЗАЦИЯ, ЗАДЪЛЖЕНИЯ И УПРАВЛЕНИЕ НА ИНЦИДЕНТИ

Член 2

Задачи на Комисията

1. Комисията прилага и наблюдава ефективността на мерките за сигурност за централната ШИС II, посочени в настоящото решение.

2. Комисията прилага и наблюдава ефективността на мерките за сигурност за комуникационната инфраструктура, посочени в настоящото решение.

3. Комисията определя служител по сигурност на системата от длъжностните си лица. Служителят по сигурността на системата се назначава от генералния директор на Генерална дирекция „Правосъдие, свобода и сигурност“ на Комисията. Задачите на служителя по сигурността на системата по-специално включват:

а) изготвяне на политиката за сигурност, както е описано в член 7 от настоящото решение;

б) наблюдаване на ефективността при изпълнението на процедурите за сигурност на централната ШИС II;

в) наблюдаване на ефективността при изпълнението на процедурите за сигурност на комуникационната инфраструктура;

г) принос в подготовката на докладването във връзка със сигурността, както е посочено в член 50 от Регламент (ЕО) № 1987/2006 и в член 66 от Решение 2007/533/ПВР;

д) изпълнение на задачи по координиране и подпомагане при проверките и одитите, извършвани от Европейския надзорен орган по защита на данните, посочени в член 45 от Регламент (ЕО) № 1987/2006 и в член 61 от Решение 2007/533/ПВР, както и уведомяване на служителя на Комисията по защита на данните за инциденти по смисъла на член 5, параграф 2;

е) наблюдение дали настоящото решение и политиката за сигурност се прилагат правилно и изцяло от всички изпълнители или подизпълнители на договори, които участват по някакъв начин в управлението на централната ШИС II;

ж) наблюдение дали настоящото решение и политиката за сигурност се прилагат правилно и изцяло от всички изпълнители или подизпълнители на договори, които участват по някакъв начин в управлението на комуникационната инфраструктура;

з) поддържане на списък от единични национални контактни точки за сигурността на ШИС II и предоставянето му на местния служител по сигурността за комуникационната инфраструктура;

и) предоставяне на списъка, посочен в буква з), на местния служител по сигурността за централната ШИС II.

Член 3

Местен служител по сигурността за централната ШИС II

1. Без да се засяга член 8, Комисията определя местен служител по сигурността за централната ШИС II от длъжностните си лица. Конфликтите на интереси между задълженията на местния служител по сигурността и всяко друго официално задължение се предотвратяват. Местният служител по сигурността за централната ШИС II се назначава от генералния директор на Генерална дирекция „Правосъдие, свобода и сигурност“ на Комисията.

2. Местният служител по сигурността за централната ШИС II осигурява мерките по сигурността, посочени в настоящото решение, да бъдат изпълнявани и процедурите по сигурността да бъдат следвани в основната ЦС-ШИС. По отношение на резервната ЦС-ШИС местният служител по сигурността за централната ШИС II осигурява още мерките по сигурността, посочени в настоящото решение, с изключение на тези, посочени в член 9, да бъдат прилагани и процедурите по сигурността, свързани с нея, да бъдат изпълнявани.

3. Местният служител по сигурността за централната ШИС II може да прехвърли всяка от своите задачи на подчинени служители. Конфликтите на интереси между задължението за изпълнение на тези задачи и всяко друго официално задължение се предотвратяват. Единичен телефонен номер и адрес за връзка позволяват свързването с местния служител по сигурността или неговия или нейния подчинен на служба по всяко време.

4. Местният служител по сигурността за централната ШИС II изпълнява задачите, произтичащи от мерките за сигурност, които трябва да бъдат взети в помещенията, в които са разположени основната ЦС-ШИС и резервната ЦС-ШИС, в рамките на параграф 1, които по-специално включват:

а) задачи по местната оперативна сигурност, включващи одит на „защитната стена“, редовни изпитвания на сигурността, одитиране и докладване;

б) наблюдение на ефективността на плана за непрекъснатост на работата и осигуряване на редовното провеждане на учения;

в) събиране на доказателства и докладване на служителя по сигурността на системата за всеки инцидент в централната ШИС II, който може да повлияе на сигурността на централната ШИС II или на комуникационната инфраструктура;

г) информиране на служителя по сигурността на системата, ако политиката за сигурност се нуждае от изменение;

д) наблюдение дали настоящото решение и политиката за сигурност се прилагат от всички изпълнители или подизпълнители на договори, които участват по някакъв начин в оперативното управление на централната ШИС II;

е) осигуряване на това, че персоналът осъзнава своите задължения и наблюдаване на прилагането на политиката за сигурност;

ж) наблюдаване на развитието в сферата на сигурността на ИТ и осигуряване на това, че персоналът е съответно обучен;

з) подготвяне на необходимата информация и варианти за създаването, актуализирането и прегледа на политиката за сигурност в съответствие с член 7.

Член 4

Местен служител по сигурността за комуникационната инфраструктура

1. Без да се засяга член 8, Комисията определя местен служител по сигурността за комуникационната инфраструктура от своите длъжностни лица. Конфликтите на интереси между задълженията на местния служител по сигурността и всяко друго официално задължение се предотвратяват. Местният служител по сигурността за комуникационната инфраструктура се назначава от генералния директор на Генерална дирекция „Правосъдие, свобода и сигурност“ на Комисията.

2. Местният служител по сигурността за комуникационната инфраструктура наблюдава функционирането на комуникационната инфраструктура и осигурява това, че мерките по сигурността се прилагат, както и това, че процедурите по сигурността се изпълняват.

3. Местният служител по сигурността за комуникационната инфраструктура може да прехвърли всяка от своите задачи на подчинени служители. Конфликтите на интереси между задължението за изпълнение на тези задачи и всяко друго официално задължение се предотвратяват. Единичен телефонен номер и адрес за връзка позволяват свързването с местния служител по сигурността или неговия или нейния подчинен на служба по всяко време.

4. Местният служител по сигурността за комуникационната инфраструктура изпълнява задачите, произтичащи от мерките за сигурност, които трябва да бъдат взети по комуникационната инфраструктура и които по-специално включват:

а) всички задачи по оперативната сигурност, свързани с комуникационната инфраструктура, включващи одит на „защитната стена“, редовни изпитвания на сигурността, одитиране и докладване;

б) наблюдение на ефективността на плана за непрекъснатост на работата и осигуряване на редовното провеждане на учения;

в) събиране на доказателства и докладване на служителя по сигурността на системата за всеки инцидент, настъпил в комуникационната инфраструктура, който може да повлияе на сигурността на централната ШИС II или на комуникационната инфраструктура;

г) информиране на служителя по сигурността на системата, ако политиката за сигурност се нуждае от изменение;

д) наблюдение дали настоящото решение и политиката за сигурност се прилагат от всички изпълнители или подизпълнители на договори, които участват по някакъв начин в управлението на комуникационната инфраструктура;

е) осигуряване на това, че персоналът осъзнава своите задължения, както и наблюдаване на прилагането на политиката за сигурност;

ж) наблюдаване на развитието в сферата на сигурността на ИТ и осигуряване на това, че персоналът е съответно обучен;

з) подготвяне на необходимата информация и варианти за създаването, актуализирането и прегледа на политиката за сигурност в съответствие с член 7.

Член 5

Инциденти по сигурността

1. Всяко събитие, което има или може да има въздействие върху сигурността на ШИС II и може да предизвика щети или загуба на ШИС II, се разглежда като инцидент по сигурността, особено когато може да е бил осъществен достъп до данни или когато наличността, целостта и поверителността на данните са били или е могло да бъдат компрометирани.

2. Инцидентите по сигурността се управляват така, че да се осигури бърза, ефективна и правилна реакция в съответствие с политиката за сигурност. Създават се процедури за възстановяване след инцидент.

3. На засегнатата държава-членка се предоставя информация по отношение на инцидент по сигурността, който има или може да има въздействие върху работата на ШИС II в държавата-членка или върху наличността, целостта и поверителността на данните, въведени или изпратени от държавата-членка. Служителят по защита на данните на Комисията се уведомява за инцидентите по сигурността.

Член 6

Управление на инциденти

1. От всички служители и изпълнители на договори в разработването, управлението или експлоатацията на ШИС II се изисква да отбелязват и докладват на служителя по сигурността на системата или на местния служител по сигурността за комуникационната инфраструктура всички наблюдавани или подозирани слабости в сигурността на комуникационната инфраструктура.

2. В случай на установяване на инцидент, който има или може да има въздействие върху сигурността на ШИС II, местният служител по сигурността за комуникационната инфраструктура информира възможно най-бързо служителя по сигурността на системата и когато е необходимо, единичната национална контактна точка за сигурността на ШИС II, ако във въпросната държава-членка съществува такава контактна точка, писмено, или в случай на изключителна спешност, посредством други комуникационни канали. Докладът съдържа описанието на инцидента по сигурността, степента на риск, възможните последици и мерките, които са били или следва да бъдат предприети, за да се смекчи рискът.

3. Всички доказателства във връзка с инцидент по сигурността се запазват незабавно от местния служител по сигурността за комуникационната инфраструктура. В степента, в която позволяват приложимите разпоредби за защита на данните, такива доказателства се предоставят на служителя по сигурността на системата при поискване от негова страна.

4. В политиката за сигурност се дефинират процеси за обратна връзка, за да се гарантира, че информацията за типа, третирането и резултата от инцидент по сигурността се съобщава на служителя по сигурността на системата и на местния служител по сигурността за комуникационната инфраструктура, веднага след като инцидентът е отработен и повече не е в развитие.

5. Параграфи от 1 до 4 се прилагат *mutatis mutandis* към инциденти в централната ШИС II. В този смисъл всяко позоваване на местния служител по сигурността за комуникационната инфраструктура в параграфи от 1 до 4 се чете като позоваване на местния служител по сигурността за централната ШИС II.

ГЛАВА III

МЕРКИ ЗА СИГУРНОСТ

Член 7

Политика за сигурност

1. Генералният директор на Генерална дирекция „Правосъдие, свобода и сигурност“ установява, актуализира и редовно преглежда обвързваща политика за сигурност в съответствие с настоящото решение. Политиката за сигурност предоставя подробните процедури и мерки за защита срещу заплахи за наличността, целостта и поверителността на комуникационната инфраструктура, включително планиране за извънредни ситуации с цел да се осигури необходимото ниво на сигурност, както е предписано от настоящото решение. Политиката за сигурност е в съответствие с настоящото решение.

2. Политиката за сигурност се базира на оценка на риска. Мерките, описани от политиката за сигурност, са пропорционални на идентифицираните рискове.

3. Оценката на риска и политиката за сигурност се актуализират, ако технологичните промени, идентифицирането на нови заплахи или някакви други обстоятелства правят това необходимо. Във всички случаи на политиката за сигурност се прави преглед ежегодно, за да се гарантира, че все още осигурява подходящ отговор на последната оценка на риска или на всяка друга новоидентифицирана технологична промяна, заплаха или друго подобно обстоятелство.

4. Политиката за сигурност се изготвя от служителя по сигурността на системата при координиране с местния служител по сигурността за централната ШИС II и местния служител по сигурността за комуникационната инфраструктура.

5. Параграфи от 1 до 4 се прилагат *mutatis mutandis* към инциденти в централната ШИС II. В този смисъл всяко позоваване на местния служител по сигурността за комуникационната инфраструктура в параграфи от 1 до 4 се чете като позоваване на местния служител по сигурността за централната ШИС II.

Член 8

Изпълнение на мерките за сигурност

1. Изпълнението на задачите и изискванията, установени в настоящото решение и в политиката за сигурност, включително задачата за определяне на местен служител по сигурността, може да бъде възложено с договор или поверено на частни или публични образувания.

2. В този случай Комисията осигурява посредством правнообвързващо споразумение, че изискванията, установени в настоящото решение и в политиката за сигурност, са спазени напълно. В случай на делегиране или възлагане с договор на задачата за определяне на местен служител по сигурността Комисията осигурява посредством правнообвързващо споразумение, че ще бъде потърсено становището ѝ относно лицето, което ще бъде определено за местен служител по сигурността.

Член 9

Контрол на достъпа до съоръженията

1. За защита на районите, в които са разположени съоръжения за обработка на данни, се използват периметри за сигурност с подходящите бариери и контрол на входовете.

2. В периметрите за сигурност се дефинират обезопасени зони за защита на физически компоненти (активи), включващи хардуер, носители и конзоли за данни, планове и други документи за ШИС II, както и офиси и други работни места за персонала, участващ в експлоатацията на ШИС II. Тези обезопасени зони се защитават с подходящ контрол на входовете, за да се гарантира, че достъп се позволява само на персонал, който е упълномощен. Работата в обезопасените зони е предмет на подробни правила за сигурност, определени в политиката за сигурност.

3. Предвижда се и се монтира физическа сигурност за офиси, стаи и съоръжения. Точките за достъп, като зоните за доставка и товаро-разтоварни дейности, и други точки, през които неупълномощени лица могат да влязат в помещенията, се контролират и ако е възможно, се изолират от съоръженията за обработка на данни, за да се избегне неразрешеният достъп.

4. Проектира се и се прилага пропорционално на риска физическа защита на периметрите за сигурност срещу повреда от природни или предизвикани от човека бедствия.

5. Оборудването се защитава от физически и екологични заплахи и от възможности за неразрешен достъп.

6. Ако Комисията притежава такава информация, тя добавя към списъка, посочен в член 2, параграф 3, буква з), единична контактна точка за наблюдението и изпълнението на разпоредбите на настоящия член в помещенията, в които е разположена резервната ЦС-ШИС.

Член 10

Контрол на носителите на данни и на активите

1. Сменяем носител, който съдържа данни, се защитава срещу неразрешен достъп, неправилна употреба или повреда, а разчитането му се осигурява за целия живот на данните.

2. Освобождаването от носителите, когато повече не са необходими, се извършва по сигурен и безопасен начин в съответствие с подробните процедури, които ще бъдат определени в политиката за сигурност.

3. Инвентарни списъци осигуряват наличието на информация за мястото на съхранение, приложимия срок на запазване и разрешенията за достъп.

4. Определят се всички важни активи на комуникационната инфраструктура, така че да могат да бъдат защитени в съответствие с важността им. Води се актуален регистър на съответното ИТ оборудване.

5. Осигурява се актуална документация на комуникационната инфраструктура. Такава документация трябва да е защитена срещу неразрешен достъп.

6. Параграфи от 1 до 5 се прилагат *mutatis mutandis* към инциденти в централната ШИС II. В този смисъл всяко позоваване на комуникационната инфраструктура се чете като позоваване на централната ШИС II.

Член 11

Контрол върху съхранението

1. Вземат се подходящи мерки за осигуряване на правилно съхранение на данните и предотвратяване на неразрешения достъп до тях.

2. Всички елементи на оборудването, съдържащи носители за съхранение на данни, се проверяват, за да се гарантира, че чувствителните данни са били премахнати или напълно заличени преди освобождаването от тях, или се унищожават по сигурен начин.

Член 12

Контрол на пароли

1. Всички пароли се пазят в безопасност и се третират с поверителност. В случай на подозрение, че дадена парола е била разкрита, паролата се сменя незабавно или съответният потребителски достъп се прекратява. Използват се уникални и индивидуални идентификации за потребителите.

2. В политиката за сигурност се дефинират процедури за вход и изход, за да се предотврати неразрешен достъп.

Член 13

Контрол на достъпа

1. За целите на оперативното управление политиката за сигурност установява официална процедура за регистриране и прекратяване на регистрацията на персонала за даване и отнемане на достъп до хардуера и софтуера на ШИС II. Определянето и използването на подходящи атрибути за достъп (пароли или други подходящи средства) се контролира посредством официален управленски процес, както е определен в политиката за сигурност.

2. Достъпът до хардуера и софтуера на ШИС II в ЦС-ШИС:

i) се ограничава до упълномощените лица;

ii) се ограничава до случаите, в които е налице легитимна цел в съответствие с член 45 от Регламент (ЕО) № 1987/2006 и член 61 от Решение 2007/533/ПВР или с член 50, параграф 2 от Регламент (ЕО) № 1987/2006 и член 66, параграф 2 от Решение 2007/533/ПВР;

iii) се ограничава до продължителността и обхвата, необходими за целта на достъпа; и

iv) се осъществява само в съответствие с политика за контрол на достъпа, която се определя в политиката за сигурност.

3. В ЦС-ШИС се използват само конзолите и софтуерът, разрешени от местния служител по сигурността за централната ШИС II. Използването на системни възможности, които може да са способни да заобиколят контролите на системата и на приложенията, се ограничава и контролира. Въвеждат се процедури за контрол на инсталирането на софтуер.

Член 14

Контрол на комуникациите

Комуникационната инфраструктура се наблюдава с цел осигуряване на наличност, цялост и поверителност на обмена на информация. Използват се средства за криптиране, за да се защитят данните, предавани по комуникационната инфраструктура.

Член 15

Контрол на въвеждането

Правата на достъп на лица, упълномощени за достъп до софтуера на ШИС II от ЦС-ШИС II, се наблюдават от местния служител по сигурността за централната ШИС II. Регистрира се използването на тези права на достъп, което включва времето и самоличността на потребителя.

Член 16

Контрол на транспорта

1. В политиката за сигурност се определят подходящи мерки за предотвратяване на неразрешено четене, копиране, промяна или заличаване на лични данни по време на предаване към или от ШИС II или по време на транспортирането на носители на данни. В политиката за сигурност се установяват разпоредби по отношение на допустимите типове изпращане или транспорт, както и по отношение на процедурите за отчетност за транспортирането на предмети и пристигането им в тяхното местоназначение. Носителят на данни не съдържа никакви други данни, освен данните, които трябва да бъдат изпратени.

2. Услугите, предоставени от трети страни, които включват оценка, обработване, комуникации или управление на съоръжения за обработка на данни или добавянето на продукти или услуги към съоръженията за обработка на данни, имат подходящи интегрирани контроли за сигурност.

Член 17

Сигурност на комуникационната инфраструктура

1. Комуникационната инфраструктура се управлява и контролира по подходящ начин с цел да бъде защитена от заплахи и да се осигури сигурността както на самата комуникационна инфраструктура, така и на централната ШИС II, включително на данните, обменяни през нея.

2. Характеристиките на сигурността, нивата на обслужване и управленските изисквания на всички мрежови услуги се идентифицират в мрежово споразумение за обслужване с доставчика на услуги.

3. Освен защитата на точките на достъп на ШИС II се защитават и всички допълнителни услуги, използвани от комуникационната инфраструктура. В политиката за сигурност се дефинират подходящите мерки.

Член 18

Наблюдение

1. Регистрите, записващи информацията, посочена в член 18, параграф 1 от Регламент (ЕО) № 1987/2006 и член 18, параграф 1 от Решение 2007/533/ПВР по отношение на всеки достъп и всеки обмен на лични данни с ЦС-ШИС II, се съхраняват по сигурен начин и са достъпни от помещенията, в които са разположени основната ЦС-ШИС и резервната ЦС-ШИС за максималния срок, посочен в член 18, параграф 3 от Регламент (ЕО) № 1987/2006 и член 18, параграф 3 от Решение 2007/533/ПВР.

2. В политиката за сигурност се създават процедури за наблюдение на използването или на грешки в съоръженията за обработка на данни и резултатите от дейностите по наблюдение се преглеждат редовно. Ако е необходимо, се предприемат подходящи действия.

3. Устройствата за водене на регистри и регистрите се защитават срещу злонамерена намеса и неразрешен достъп с цел да се изпълнят изискванията за събиране и запазване на доказателства за срока на запазване.

Член 19

Мерки за криптиране

За защитата на информацията, когато е необходимо, се прилагат мерки за криптиране. Тяхното използване, заедно с целите и условията, трябва да бъде одобрено предварително от служителя по сигурността на системата.

ГЛАВА IV

СИГУРНОСТ НА ЧОВЕШКИТЕ РЕСУРСИ

Член 20

Профили на персонала

1. Политиката за сигурност дефинира функциите и отговорностите на лицата, които имат разрешен достъп до централната ШИС II.

2. Политиката за сигурност дефинира функциите и отговорностите на лицата, които имат разрешен достъп до комуникационната инфраструктура.

3. Свързаните със сигурността роли и отговорности на персонала на Комисията, изпълнителите на договори и персонала, участващ в оперативното управление, се дефинират, документират и съобщават на засегнатите лица. В описанието на длъжността и в целите се посочват ролите и отговорностите на персонала на Комисията; в договорите или в споразуменията за нивото на обслужване се посочват тези за изпълнителните на договори.

4. Споразуменията за поверителност и служебна тайна се сключват с всички лица, към които не се прилага служебен правилник на Европейския съюз или на публична служба на държава-членка. Персоналът, който трябва да работи с ШИС II, преминава през необходимата проверка за сигурност или процедура на сертифициране в съответствие с подробните процедури, определени в политиката за сигурност.

Член 21

Информиране на персонала

1. Целият персонал и всички изпълнители на договори получават подходящо обучение за рисковете за сигурността, правните изисквания, политиките и процедурите в степента, изисквана от техните задължения.

2. При приключване на трудовите взаимоотношения или договора отговорностите на персонала и изпълнителите на договори, свързани с промяна на работата или приключване на трудовите взаимоотношения, се определят в политиката за сигурност и се създават процедури в политиката за сигурност за връщане на активите и за прекратяване на правата за достъп.

ГЛАВА V

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 22

Приложимост

1. Настоящото решение влиза в сила на датата, определена от Съвета в съответствие с член 55, параграф 2 от Регламент (ЕО) № 1987/2006 и член 71, параграф 2 от Решение 2007/533/ПВР.

2. Член 1, параграф 1, член 2, параграф 1, член 2, параграф 3, букви б), г), е) и и), член 3, член 6, параграф 5, член 7, параграф 5, член 9, параграф 6, член 10, параграф 6, член 13, параграфи 2 и 3, член 15, член 18 и член 20, параграф 1 изтичат, когато управителният орган поеме своите задължения.

Съставено в Брюксел на 4 май 2010 година.

За Комисията

Председател

José Manuel BARROSO