ПРИЛОЖЕНИЕ № 2

КЪМ ИНСТРУКЦИЯ ЗА ПРАКТИЧЕСКОТО ОСЪЩЕСТВЯВАНЕ НА НАДЗОРНАТА ДЕЙНОСТ НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

БЕЛЕЖКА: Въпросниците, които задължително се изпращат на АЛД при всяка една проверка, съдържат: **I. „Обща част. Базови въпроси“** и **II. „Технически и организационни мерки за защита на личните данни“**.

III. „Въпроси при извършване на проверки с предмет видеонаблюдение“ се изпраща на АЛД когато проверката касае видеонаблюдение.

IV. „Допълнителни въпроси при извършване на проверки след постъпило уведомление по чл. 33 от Регламент2016/679“ се изпраща на АЛД при проверка след постъпило уведомление.

V. „Допълнителни въпроси относно предприетите от АЛД мерки за мрежова и информационна сигурност“ се ползват от експертите по проверката когато са относими към съответната проверка. На АЛД се изпращат само тези от тях, които имат връзка с проверката.

Въпросниците **VI. „Допълнителни въпроси при извършване на проверки на Шенгенската информационна система (ШИС)“, VII. „Допълнителни въпроси при извършване на проверки на Визовата информационна система (ВИС)“, VIII „Допълнителни въпроси при извършване на проверки на информационната система на Европол“** и **IX. „Допълнителни въпроси при извършване на проверки на информационната система на Евродак“** се изпращат на АЛД само при извършване на съответната специализирана проверка.

ВЪПРОСНИК ЗА ИЗВЪРШВАНЕ НА ПРОВЕРКИ ПРИ ОСЪЩЕСТВЯВАНЕ НА НАДЗОРНАТА ДЕЙНОСТ НА КЗЛД

(……име на АЛД……)

I. ОБЩА ЧАСТ. БАЗОВИ ВЪПРОСИ

1. Какви регулативни документи на ЕС прилага в дейността си АЛД?
2. Каква национална правна рамка се прилага при осъществяваната от АЛД дейност?
3. Каква е организационната структура на АЛД?
4. Кои са основните направления на дейност на АЛД?

5. Какви са поддържаните от АЛД регистри съгласно чл. 30 от Регламент 2016/679?

6. Какво е нормативното основание за водене на поддържаните регистри с лични данни?

7. Какви категории лични данни се обработват в поддържаните от АЛД регистри?

8. Съществуват ли Политики (Правила, Процедури, Инструкции) за защита на личните данни в съответствие с изискванията на чл. 24, параграф 2 от Регламент 2016/679?

9. Обработва ли АЛД данни по чл. 9 от Регламент 2016/679 – специални категории лични данни и какви?

10. На какви носители се обработват личните данни?

11. Съществува ли съгласие на физическите лица за обработване на личните им данни от АЛД, съгласно чл. 6, § 1, б. „а" от Регламент 2016/679?

12. Възлага ли АЛД действия по обработване на лични данни, съгласно чл. 28 и чл. 29 от Регламент 2016/679? На кои организации и/или физически лица?

13. Как АЛД информира физическите лица, чийто лични данни обработва за:

13.1. целите на обработването на личните данни;

13.2. получателите или категориите получатели, на които могат да бъдат разкрити личните данните;

13.3. задължителния или доброволния характер на предоставяне на личните данни и последиците от отказ за предоставянето им;

13.4. правото им на достъп и правото им на коригиране на събраните лични данни, съгласно членове 13 – 20 от Регламент 2016/679?

14. Какви действия предприема АЛД след постигане на целите на обработване на личните данни в съответствие с изискванията на Регламент 2016/679 и ЗЗЛД?

15. От кои други администратори АЛД получава данни и на кои АЛД предоставя данни (други АЛД, международни организации)? На какво правно основание и какви категории лични данни? Посочете механизма за взаимодействие и обмен на лични данни.

16. Имат ли други АЛД директен достъп до обработваните от АЛД регистри с лични данни – посочете кои са АЛД и категориите лични данни, които достъпват?

17. Осъществява ли се предоставяне на лични данни в трети страни (чл. 4, параграф 10 от Регламент 2016/679)? Ако Да – на кои страни и какви категории са предоставяните лични данни?

18. Осъществява ли се предаване на лични данни в трети държави (държави извън ЕС) или международни организации?

19. Какви мерки са предприети за защита на носители с лични данни при пренасяне

(включително предотвратяване на неоправомощено четене, копиране, модифициране или унищожаване)?

II. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

А. ФИЗИЧЕСКА ЗАЩИТА

1. Посочете местоположението на обектите, в които се обработват личните данни.

2. Описание на организацията на физическия достъп и използваните средства за техническа защита.

3. Посочете спомагателните системи (сигнално-охранителна, видеонаблюдение, резервно електрозахранване, пожароизвестителна и противопожарна система, климатизация на помещенията) за обезпечаване на сигурността на личните данни.

4. Определен ли е екип за реагиране при нарушения на сигурността на личните данни? Ако Да – какви са съставът и функциите му?

5. Описание на обособените зони с контролиран достъп.

6. Оборудвани ли са помещенията по отношение на ключалки, шкафове и метални каси?

7. Използват ли се системи/устройства за контрол на физическия достъп и какви са те?

8. Има ли изготвени процедури по съхраняването на резервни ключове, кодове за каси, пароли за достъп до специфично оборудване, карти за достъп и др.? Какви са те?

9. Изградена ли е система за охрана и/или система за сигурност? Какво представлява тя?

10. Съществува ли система/средства за защита на периметъра? Какво представлява?

11. Използват ли се детектори за субстанции (метали, взривни вещества и др.)?

Б. ПЕРСОНАЛНА ЗАЩИТА

1. Преминали ли са служителите на администратора обучение по защита на личните данни и кога?

2. Какви мерки се извършват за проверка на външни лица от организации, наети за изпълнение на специфични задачи в помещенията (ремонти, доставки и др.)?

3. Спазва ли се принципът "Необходимост да се знае"? Как е регламентирано спазването му?

4. Как се запознават служителите с политиките и ръководствата за защита на

личните данни?

5. Съществува ли система от знания за опасностите за личните данни, обработвани от администратора? Как са запознати служителите?

6. Предприети ли са мерки за недопускане споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.)? Какви са те?

7. Служителите/контрагентите подписват ли декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си?

8. АЛД поддържа ли информация за проведеното обучение, тренировки на персонала, съгласие и декларации и вътрешна регламентация?

В. ДОКУМЕНТАЛНА ЗАЩИТА

1. Осъществява ли се контрол на достъпа до регистрите с лични данни? Как?

2. Посочете срокове за съхранение на регистрите с лични данни.

3. Посочете кои са регистрите, които ще се поддържат на хартиен носител?

4. Съществуват ли правила за размножаване и разпространение на документи? Какви са те и как се прилагат и контролират?

5. Съществуват ли процедури за проверка и контрол на обработването на документи, съдържащи лични данни? Какви са те и как се прилагат и контролират?

6. Съществуват ли процедури за унищожаване на документи? Какви са те и как се прилагат и контролират?

Г. ЗАЩИТА НА АВТОМАТИЗИРАНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ И/ИЛИ МРЕЖИ И КРИПТОГРАФСКА ЗАЩИТА

1. Описание на изградената компютърна мрежа и използваните информационни системи за обработка на лични данни.

2. Сертифицирана ли е мрежата на АЛД по отношение на информационната сигурност и до какво ниво?

3. Какви мерки са предприети за ограничаване на достъпа до данните (достъп до операционната система, достъп до специализиран софтуер)?

4. Осъществява ли се регистриране на достъпа до регистрите с лични данни, включително и регистриране на извършените действия (въвеждане, модифициране, изтриване на данни от регистрите)?

5. Какви мерки се прилагат за осигуряване на възможност за възстановяване на данните в случай на отказ на системата?

6. Какви мерки са предприети за осигуряване надеждност и интегритет на системата (резервно захранване за сървърите, изолиране на сървъра с базата данни от интернет, отделяне на всички сървъри в специално помещение, разделяне на мрежата на сегменти за осигуряване на по-висока надеждност и др.)?

7. Има ли изработени правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.?

8. Съществува ли политика за защита на информационните системи? Какво представлява и как се прилага?

9. Съществуват ли ръководства за защита на информационните системи? Какво представляват и как се прилагат?

10. Какви операционни процедури за защита на личните данни се използват в това число и какви средства за криптиране на информацията?

11. Определени ли са ролите и отговорностите в информационните системи?

12. Какви механизми за идентификация и автентификация се използват?

13. Какви контроли на сесията се използват?

14. Съществуват ли външни връзки/свързване? Как са защитени?

15. Съществува ли възможност за отдалечен достъп до информационните системи? Как е защитен?

16. Как е реализирана системата за защита от вируси?

17. Съществува ли план за случайни събития/непредвидени случаи? Какво представлява и как се прилага?

18. Съществуват ли правила/ръководства за поддържане/експлоатация на информационните системи? Какво представляват и как се прилагат?

19. Как се управлява конфигурацията на системата?

20. Съществува ли политика за копия/резервни копия за възстановяване? Какво представлява и как се прилага?

21. Съществуват ли ръководства/правила за работа с копията/резервни копия за възстановяване? Какво представляват и как се прилагат?

22. Как са осъществява контролът върху носителите на информация?

23. Съществуват ли процедури за унищожаване/заличаване/изтриване на технически носители? Какво представляват и как се прилагат?

24. Как се контролират унищожаването/заличаването/изтриването на технически носители?

25. Криптира ли се информацията при осъществяване на външни връзки и отдалечен достъп?

26. Какви мерки са предприети за защита на личните данни, свързани с разпространението им по телекомуникационни мрежи (защита на данните при предаването, предотвратяване неоправомощено четене, копиране, модификация и заличаване на лични данни)?

III. ВЪПРОСИ ПРИ ИЗВЪРШВАНЕ НА ПРОВЕРКИ С ПРЕДМЕТ ВИДЕОНАБЛЮДЕНИЕ

1. Наименование на АЛД?

2. Булстат/ ЕИК за юридическо лице/ ЕГН за физическо лице?

3. Седалище и адрес на управление за юридическо лице/ постоянен и настоящ адрес за физическо лице, данни за контакт с АЛД, в т.ч. телефон и електронна поща?

4. Описание и адрес на проверявания обект, предмет на видеонаблюдение?

5. Категории физически лица, за които се обработват лични данни посредством изградената система за видеонаблюдение?

6. Основание за извършваното видеонаблюдение?

7. Кога е изградена системата за видеонаблюдение?

8. От кого е изградена и от кого се поддържа системата за видеонаблюдение?

9. Извършва ли се охрана на обекта от друго физическо/юридическо лице по реда на Закона за частната охранителна дейност, същото има ли права на достъп до системата за видеонаблюдение, на какво основание и как се осъществява той?

10. Техническо описание на системата за видеонаблюдение?

11. Пространствено разположение на видеокамерите и обхват на заснемане?

12. Позволява ли системата за видеонаблюдение извършване на запис на видеокадри?

13. На какъв носител и за какъв период се съхраняват записите с видеокадри?

14. Позволява ли системата за видеонаблюдение предаване и запис на моментни снимки и видеокадри от образа на отдалечено устройство – *FTP/Cloud* сървър или друго място за съхранение на данни?

15. По какъв начин и от кого се осъществява достъпа до изходящия образ в реално време, видеокадрите и записите, в т.ч. и отдалечения такъв?

16. Налице ли са информационни табели за осъществяваното видоенаблюдение, какво е тяхното местоположение и каква информация се съдържа в тях?

17. Позволява ли системата за видеонаблюдение идентификация на физически лица?

18. Позволява ли системата за видеонаблюдение лицево разпознаване на физически лица?

19. Какви са предприетите технически и организационни мерки за защита на данните?

20. Налице ли са документи (правила, процедура, инструкция или други), регламентиращи обработването на лични данни чрез изградената система за видеонаблюдение?

IV. ДОПЪЛНИТЕЛНИ ВЪПРОСИ ПРИ ИЗВЪРШВАНЕ НА ПРОВЕРКИ СЛЕД ПОСТЪПИЛО УВЕДОМЛЕНИЕ ПО ЧЛ. 33 ОТ РЕГЛАМЕНТ 2016/679

1. Категории физически лица, до чиито лични данни е осъществен неоторизиран достъп?

2. Списък на физически лица, до чиито лични данни е осъществен неоторизиран достъп?

3. Категории лични данни и видове информация, станали достъпни при неоторизирания достъп?

4. Предприети мерки в 72 часовия срок от узнаване за нарушението на сигурността?

5. Уведомяване на засегнатите субекти?

6. Предприети мерки за минимализиране на вредите?

7. Постъпили сигнали и жалби до АЛД за конкретното нарушение?

8. Документация от извършената вътрешна проверка на АЛД по казуса?

9. Документация относно одита на информационните системи на АЛД след осъществения нерегламентиран достъп?

10. Извършван ли е предишен одит на информационните системи и електронните услугите, предоставяни от АЛД?

11. Информация за извършената оценка на риска, през какъв период се извършва и по каква методика?

12. Колко и какви електронни услуги предлага АЛД?

13. Вътрешни правила и процедури по отношение на техническите характеристики и мерките за защита на личните данни на услугата, чрез която е осъществен неоторизираният достъп?

14. Извършена ли е оценка на въздействието на предоставените електронни услуги?

15. Какви подходящи технически и организационни мерки са предприети в етапа на проектиране на предоставяне на електронните услуги?

16. Наличие на одити по отношение спазването на Наредбата за минимални изисквания за мрежова и информационна сигурност и ISO 27701 (ако е приложимо)?

17. Проверка на сигурността и сертифициране на информационните системи, обработващи лични данни?

18. Наличие на сертификати за информационна сигурност и за защита на личните данни?

19. Присъединил ли се е АЛД към одобрен Кодекс за поведение?

20. Приложете доказателства за всеки факт – документи на хартиен и/или електронен носител (в т.ч. направения анализ на риска и определяне на нивото на въздействие, правила, процедури, становища, екранни разпечатки и др.), като задължително да се предоставят заверени копия на сключени договори с физически или юридически лица, касаещи обработването на лични данни.

V. ДОПЪЛНИТЕЛНИ ВЪПРОСИ ОТНОСНО ПРЕДПРИЕТИТЕ ОТ АЛД МЕРКИ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ – КОГАТО Е ОТНОСИМО КЪМ СЪОТВЕТНАТА ПРОВЕРКА

1. Проведен ли е преглед на мрежовата и информационната сигурност и на адекватността на предприетите мерки за период от една година назад от датата на извършване на настоящата оценка?

2. Има ли заповед за определяне на служител или административно звено, отговарящо за мрежовата и информационната сигурност?

3. Има ли заповед за определяне на служители или административно звено, отговарящо за мрежовата и информационна сигурност?

4. Има ли заповед за определяне на служители или административно звено, отговарящо за мрежовата и информационна сигурност за териториалните структури?

5. Има ли политика за мрежова и информационна сигурност?

6. Политиката за мрежова и информационна сигурност преразгледана ли е за период от една година назад от датата на текущото оценяване?

7. Има ли опис на информационните активи?

8. Има ли документация по отношение на физическата схема на свързаност?

9. Има ли документация по отношение на логическата схема на информационните потоци?

10. Има ли документация на структурната кабелна система?

11. Налична ли е техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти?

12. Има ли инструкции/вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер?

13. Има ли вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, обработващи лични данни, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи, принтиране, факс, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.?

14. Документацията преразглеждана (обновена) ли е за период от една година назад от датата на текущото оценяване?

15. Документацията одобрена/утвърдена ли е от ръководителя?

16. Документацията достъпна ли е само до тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения?

17. Има ли приети вътрешни правила за класификация на информацията, свързана с лични данни на физически лица, които указват как да се маркира, използва, обработва, обменя, съхранява и унищожава информацията с която разполага организацията?

18. Приложена ли е класификацията върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването на информацията?

19. Нанесено ли е нивото на класификацията по подходящ начин върху документираната информация?

20. Нивата на класификация различни ли са от тези по ЗЗКИ?

21. Има ли извършен анализ и оценка на риска във връзка с дейностите по обработване на лични данни за период от една година назад от датата на проверката?

22. Има ли одобрена/утвърдена от ръководителя методика за извършване на анализ и оценка на риска?

23. Има ли план за намаляване на неприемливите рискове, който да включва подходящи и пропорционални мерки за смекчаване на неприемливите рискове, необходими ресурси за изпълнение на тези мерки, срок за прилагане на мерките и отговорни лица?

24. Има ли приети вътрешни правила, регламентиращи процеса на управление на жизнения цикъл на информационните и комуникационните системи и техните компоненти и в тях указани ли са условията, начина и реда за придобиване, въвеждане в експлоатация, поддръжка, преместване/изнасяне, извеждане от експлоатация и унищожаване на информационни и комуникационни системи и техните компоненти?

25. Има ли опис на информационните активи, който да съдържа информация като еднозначна идентификация (като инвентарен, сериен номер или др.); основни характеристики; услуги, процеси и дейности, в които участва; местоположение; година на производство, където е приложимо; дата на въвеждане в експлоатация, където е приложимо; версия, където е приложимо; 8. местонахождение на свързаната с него документация (техническа, експлоатационна, потребителска и др.); отговорно лице?

26. Има ли вътрешни правила и инструкции за служителите имащи отношение към процесите и дейностите по обработка на лични данни, имат ли подходящата квалификация, знания и умения за изпълнение на отговорностите им?

27. Вътрешните правила от предходния въпрос регламентират ли процеса за наемане на работа в съответствие с приложимите закони и подзаконови нормативни актове, професионалната етика и съобразно изискванията, свързани с дейността им – класификацията на информацията, до която имат достъп, и предполагаемите рискове?

28. Вътрешните правила по предходния въпрос регламентират ли отговорностите и задълженията по отношение на сигурността на информацията при прекратяване или промяна на служебните/договорните отношения?

29. Вътрешните правила по предходния въпрос регламентират ли дисциплинарен процес за лицата, които са извършили нарушение по отношение на политиката и вътрешните правила за мрежова и информационна сигурност?

30. Документирани ли са отговорностите на служителите имащи отношение към процесите и дейностите по отношение на сигурността на информацията с ясно определени срокове и задължения?

31. Проведено ли е подходящо професионално обучение за повишаване на квалификацията на служителите в съответствие с използваната техника и технологии?

32. Проведен ли е инструктаж на служителите за повишаване на вниманието им по отношение на мрежовата и информационната сигурност за период от една година назад от датата на проверката?

33. В договорите с трети страни има ли договорени изисквания за сигурност на информацията, свързани с достъпа на представители на трети страни до информация и активи?

34. В договорите с трети страни има ли договорени изисквания за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити?

35. В договорите с трети страни има ли договорени изисквания за последици при неспазване на изискванията за сигурност на информацията?

36. В договорите с трети страни има ли договорени изисквания за отговорност при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност?

37. В договорите с трети страни има ли договорени изисквания за взаимодействие в случай на възникване на инцидент, който най-малко включва: контактни точки, начин за докладване, време за реакция, време за възстановяване на работата, условия за затваряне на инцидент?

38. Има ли определен служител/служители, отговарящ/отговарящи за спазване на изискванията по договорите с трети страни и параметрите на нивото на обслужване?

39. Има ли изготвен план за действие в случай на неспазване на уговорените дейности и клаузи с тратата страна?

40. Има ли приети вътрешни правила за управление на измененията във важните информационни активи?

41. Прави ли се анализ и оценка на риска преди извършване на изменението?

42. Планират ли се измененията?

43. Измененията съгласуват ли се предварително с всички страни, имащи отговорности към процесите и дейностите?

44. Одобрява ли се от ръководителя извършването на измененията?

45. Оповестява ли се предварително за извършване на дадено изменение?

46. Проверяват ли се измененията в тестова среда преди да се извършат?

47. Има ли план за връщане на системите в предишното им състояние?

48. Разделени и изолирани помежду им ли са информационните и комуникационните системи, изпълняващи различни функции?

49. Има ли разписани и одобрени правила за филтриране на трафика?

50. Забранени ли са ненужните портове по протоколи TCP и User Datagram Protocol (UDP)?

51. Има ли политика относно използването на лични технически средства и преносими записващи устройства?

52. Политиката отразена ли е във вътрешни правила?

53. Има ли политики и вътрешни правила за прилагане на криптографски механизми?

54. Сменени ли са идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационните активи?

55. Персонални ли са администраторските профили?

56. Използват ли се администраторските профили само за административни цели?

57. Създадени ли са администраторски профили само на служители, които извършват административни операции?

58. Ограничени ли са правата на всеки администраторски акаунт?

59. Различни ли са данните за автентикация на администраторските акаунти за всяка система?

60. Данните за автентикация с възможно най-голяма сложност ли са?

61. Данните за автентикация съхраняват ли се подходящо физически и логически защитени?

62. Поддържа ли се списък на администраторските профили за информационните и комуникационните системи и техните компоненти?

63. Правата на административните акаунти на администраторите спират ли се за съответния период при невъзможност на администратор да изпълнява пълноценно функциите си поради обективни причини?

64. Правен ли е преглед на администраторските профили за период от една година назад от датата на настоящото оценяване?

65. Паролите за автентикация на администраторските профили сменяни ли са за период от една година назад от датата на настоящото оценяване?

66. Документират ли се всички операции, процеси и дейности в информационните и комуникационните системи и техните компоненти, извършени с администраторски права?

67. Въвеждат и съхраняват ли се в документацията пароли на административен профил под формата на явен текст или хеш?

68. Използва ли се отделна подходящо защитена среда за целите на администриране на информационните и комуникационните системи и техните компоненти?

69. Ако не се използва отделна подходящо защитена среда за целите на администриране на информационните и комуникационните системи и техните компоненти, защитават ли се потоците информация чрез механизми за удостоверяване и криптиране?

70. Във вътрешните правила определени ли са правата на достъп до конкретни информационни активи на служителите според длъжността им?

71. Във вътрешните правила определен ли е реда за заявяване, промяна и прекратяване на достъп?

72. Прилагат ли се мерки за автентикация, оторизация и одит на компютърните мрежи и системи?

73. Минималната дължина на използваните пароли 8 символа за потребителските и 12 символа за администраторските профили ли е?

74. Паролите на потребителските акаунти сменят ли се регулярно на период не по-голям от шест месеца?

75. Потребителските профили индивидуални ли са?

76. За периода от една година назад от датата на настоящото оценяване правен ли е преглед на достъпите?

77. Достъпът до споделени файлове и принтери разрешен ли е само от мрежата, контролирана от субекта?

78. При използване на достъп до информационни активи извън мрежата използва ли се двуфакторна автентикация?

79. При използване на достъп до информационни активи извън мрежата използват само канали с висока степен на защита?

80. При използване на достъп до информационни активи извън мрежата забранено ли е използването на File Transfer Protocol (FTP) и Remote Desktop Connection?

81. При хардуерните устройства има ли осигурени климатико-механичните условия, указани от производителя?

82. Осъществява ли се наблюдение на параметрите климатико-механичните условия?

83. Провежда ли се планирана регулярна техническа профилактика на устройствата в съответствие с политиката му за жизнения им цикъл?

84. Устройствата разположени ли са в зони, които са физически и логически защитени в съответствие с информацията, с която работят?

85. Инсталирани ли са версии на използвания в системите софтуер и фърмуер, който се поддържат от техните доставчици или производители и са актуални от гледна точка на сигурността?

86. Има ли списък с одобрения софтуер, който се използва в информационните и комуникационните системи?

87. Има ли библиотека с дистрибутиви на използвания софтуер и фърмуер?

88. Взети ли са мерки за недопускане на инсталирането и използването на неодобрен софтуер и фърмуер?

89. Контролира ли се използвания софтуер и фърмуер, включително неговата актуалност?

90. Има ли вътрешни правила и инструкции за регламентиране на действията по поддържане на библиотеката с дистрибутиви на използвания софтуер и фърмуер в актуално състояние?

91. Има ли вътрешни правила и инструкции за регламентиране на действията по управление на достъпа до нея?

92. Има ли вътрешни правила и инструкции за регламентиране на действията по проследяване за новооткрити уязвимости в сигурността на използваните в системите софтуери и фърмуер и за техни актуализации (нови версии, ъпдейти и пачове), които отстраняват тези уязвимости, или мерки за смекчаването им, публикувани от производителите или доставчиците?

93. Има ли вътрешни правила и инструкции за регламентиране на действията по придобиване и проверка на произхода и цялостта на актуализацията преди инсталирането й?

94. Има ли вътрешни правила и инструкции за регламентиране на действията по прилагането на актуализациите и препоръчаните мерки?

95. Забранени ли са macros в office пакетите?

96. Забранени ли са pop-up в браузерите?

97. Auto play функцията конфигурирана ли е винаги да иска потвърждение на потребителя?

98. User Account Control конфигуриран ли е до на-високо ниво, така че винаги да издава предупреждения?

99. При споделянето на файлове и принтери използва ли се настройка Everyone?

100. Забранен ли е TRACE/TRACK методът?

101. Забранена ли е anonymous authentication?

102. Използва ли се Unicast Reverse-Path Forwarding (uRPF) и rate-limiting?

103. Забранен ли е TLS renegotiation в системи, използващи TLS, или да се конфигурира rate-limiter за ограничаване на броя на предоговаряне на сесия?

104. В съобщенията за грешки в системите скрита ли е излишната информация?

105. Забранен ли е AutoComplete?

106. Използват ли се приложения (add-ons) към браузърите за блокиране на рекламно съдържание?

107. Съхранява ли се off-line копие от актуалните конфигурационни файлове и/или описание на настройките?

108. Копията проверяват ли се регулярно относно качество и годност?

109. Направена ли е проверка на конфигурационните файлове и/или описание на настройките?

110. Има ли инсталиран антивирусен софтуер?

111. Антивирусният софтуер на всички устройства ли е инсталиран?

112. Антивирусния софтуер актуализиран ли е?

113. Инсталираният антивирусен софтуер позволява ли извършване на пълна проверка за наличие на зловреден софтуер поне веднъж в седмицата?

114. Инсталираният антивирусен софтуер позволява ли проверка на електронната поща и файлове, свалени от интернет, както и преносими записващи устройства, преди да бъдат отворени?

115. Извършена ли е оценка на ефективността на мерките за защита от зловреден софтуер за периода от една календарна година назад от датата на настоящата проверка?

116. Има ли инсталиран сертификат на уеб сървърите, издаден от доверена система за сертифициране (trusted certification authority system)?

117. Сертификата издаден ли е за съответния уеб сайт или група сайтове?

118. Сертификата уникален ли е?

119. Сертификата използва ли алгоритъм за криптиране поне SHA2?

120. Сертификата актуален ли е?

121. Сертификатите с изтекъл срок анулирани ли са?

122. Уебсайта достъпен ли е само по протокол Hypertext Transfer Protocol Secure (HTTPS)?

123. В уеб сайта използват ли се само криптографски транспортни протоколи TLS (Transport Layer Security) версия 1.2, дефиниран в RFC 5246 на IETF (The Internet Engineering Task Force – Специализирана работна група за интернет инженеринг) през 2008 г., версия 1.3, дефиниран в RFC 8446 на IETF през 2018 г., или следващи по-нови версии?

124. Криптира ли се информацията, обменяна между уеб сървъра и потребителите му?

125. Има ли Web Application Firewall (WAP), който наблюдава и филтрира трафика от и към съответното приложение?

126. Забранено ли е вмъкване на данни от страна на потребителя, освен на определените за това места?

127. Валидират ли се всички входни данни, постъпващи от клиента?

128. Забранено ли е въвеждането на специални символи?

129. Кодирани ли са всички данни, изпращани от клиента и показвани в уеб страница с HTML?

130. Наложено ли е ограничение на заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по Url?

131. Конфигуриран ли е конфигурират типът и размерът на headers, които уеб сървърът ще приеме?

132. Ограничени ли са времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка?

133. Има ли ограничение на броя неуспешни опити за влизане в системата?

134. Забранено ли е извеждането на списък на уеб директориите?

135. Имат ли бисквитките (cookies) флаг за защита (security flag)?

136. Имат ли бисквитките (cookies) флаг HTTP only?

137. Скрита/премахната ли е информацията за платформите и версиите на използвания софтуер в Headers на отговорите на заявките?

138. Headers на отговорите на заявките съдържат ли опция HTTP Strict Transport Security (HSTS)?

139. Headers на отговорите на заявките съдържат ли опция X-Content-Type-Options?

140. Headers на отговорите на заявките съдържат ли опция X-XSS-Protection?

141. Headers на отговорите на заявките съдържат ли опция X-Frame-Options?

142. Headers на отговорите на заявките съдържат ли опцияContent-Security-Policy?

143. Headers на отговорите на заявките съдържат ли опция X-Frame-Options?

144. Headers на отговорите на заявките съдържат ли опция X-Frame-Options?

145. Headers на отговорите на заявките съдържат ли опция HTTP Public Key Pinning (HPKP)?

146. В главната директория на уеб сайта (website) има ли сложен файл robots.txt?

147. Ако се използва Система за управление на съдържанието (CMS) променено ли е наименованието по подразбиране на папката за достъп до администраторския панел?

148. Ако се използват повече от един DNS сървър, всеки от тях разположен ли е в различна мрежа/подмрежа?

149. Прилага ли се DNSSEC (Domain Name System Security Extensions)?

150. Минимализирани ли са DNS заявките?

151. Забранен ли се zone-transfers?

152. В конфигурационния файл има ли сложен dmarc (Domain-based Message Authentication, Reporting and Conformance) запис?

153. В конфигурационния файл има ли сложен SPF (Sender Policy Framework) запис?

154. Осигурена ли е защита на информационните активи от пожар, наводнение, химическа и физическа промяна на въздуха?

155. Извършва ли се наблюдение на информационните активи?

156. Използват ли се система/системи за автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността системи?

157. Има ли вътрешни правила и/или инструкции регламентиращи действията за наблюдение и реакция на сигналите от система/системи за автоматично откриване на събития?

158. Регистрират ли се автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори?

159. В записите за всяко от тези събития отбелязано ли е астрономическото време, когато е настъпило събитието?

160. Поддържат ли всички компоненти на системите единно време?

161. За синхронизация на компонентите на информационните и комуникационните системи използва ли се протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен?

162. Достъпът до информацията на системните записи само за четене ли е?

163. Информацията за системните записи съхранява ли се за период не по-малко от 12 месеца?

164. Във вътрешните правила регламентирани ли са всички дейности при обработката на сигнали и реакция при инциденти?

165. Във вътрешните правила съдържа ли се реда за подаване на сигнали за настъпили или потенциални събития, оказващи негативно влияние върху мрежовата и информационната сигурност?

166. Във вътрешните правила съдържа ли се информация за лицата, отговорни за регистъра на инцидентите?

167. Във вътрешните правила съдържа ли се реда за регистриране на сигнала, проверката на неговата достоверност, класифицирането му, приоритизирането му и последващото уведомяване за това на подателя?

168. Във вътрешните правила съдържа ли се реда за уведомяване за инцидента?

169. Във вътрешните правила съдържа ли се реда за подаване на информация за начина за разрешаване на инцидента?

170. Във вътрешните правила съдържа ли се реда за приключване на инцидента?

171. Във вътрешните правила съдържа ли се процеса за събиране, съхраняване и предаване на доказателства, когато инцидентът предполага извършването на процесуални действия срещу лице или организация, включително необходимите за това записи?

172. Във вътрешните правила съдържа ли се правата на достъп до регистъра на инцидентите?

173. Има ли планове за справяне с инцидентите, които да съдържат информация за отговорника за организацията при настъпване на инцидент; реда за информиране; мерките, които следва да се предприемат и отговорното за това лице; реда за консултиране; реда за следене на параметрите по време на инцидента и лицето, което ще събира и съхранява необходимата информация?

174. Има ли разработена стратегия за комуникация, която определя реда за

споделяне на информацията за инцидента със служители, партньори, доставчици, клиенти, медии, държавни органи?

175. Има ли вътрешни правила за резервиране и архивиране на информацията?

176. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за информацията (бази данни, конфигурационни файлове, имиджи на системи и др.), която ще се резервира и/или архивира?

177. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за технологията, която ще се използва за архивиране и резервиране?

178. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за типът на резервиране (частично, пълно и др.)?

179. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за периодът на извършване на архивирането и резервирането?

180. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за броят на копията, които ще се правят?

181. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за времето за съхраняване на всяко копие съгласно изискванията на нормативните актове и оценката на риска?

182. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за мястото на съхраняване на всяко копие?

183. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за начинът на защита от неправомерен достъп (физическа и логическа);?

184. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за случаите на използване?

185. В съдържанието на вътрешните правила за резервиране и архивиране на информацията включени ли са записи за лицето, което дава разрешение за използването?

186. Правят ли се регулярно резервирането и/или архивирането на информацията?

187. Копията на информацията етикетирани ли са по начин, указващ еднозначно поне каква е информацията, за коя система, какъв метод е използван за създаване на копието, дата и час?

188. Копията на чувствителната информация в криптиран вид или защитени с парола ли са?

189. Копията на информацията съхраняват ли се на отделна машина?

190. Съхранява ли се едно от копията на критичната за дейността информация?

191. Правена ли е проверка на годността на резервните копия за период от една календарна година назад от датата на настоящото оценяване?

192. Предприети ли са мерки по резервиране на системите и устройствата, балансиране на натоварването на критичните устройства или системи и резервиране на центрове за данни?

193. Има ли разработени планове за действия в случай на аварии, природни бедствия или други непредвидени обстоятелства, които биха причинили прекъсване на предоставяната услуга?

194. Плановете съдържат ли обстоятелствата, за които се отнасят; праговете, при които се задействат; лицето, което дава разрешение за задействането им и реда за възстановяване на услугите и дейностите до определено ниво?

195. Плановете проигравани ли са за период от една календарна година назад от датата на проверката?

196. Плановете актуализирани ли са за период от една календарна година назад от датата на проверката?

197. Плановете достъпни ли са само за лицата, които имат отговорности за тяхното изпълнение?

198. Плановете съхраняват ли се най-малко на две места, едното от които е извън сградата, в която се намират системите, за които се отнасят?

VI. ДОПЪЛНИТЕЛНИ ВЪПРОСИ ПРИ ИЗВЪРШВАНЕ НА ПРОВЕРКИ НА ШЕНГЕНСКАТА ИНФОРМАЦИОННА СИСТЕМА (ШИС)

А. ЗАКОНОДАТЕЛСТВО

1. Кое общо национално законодателство за защита на данните е приложимо за обработването на лични данни от Шенгенската информационна система (ШИС)?

2. Има ли на национално равнище специално законодателство и/или разпоредби относно обработването на лични данни във връзка с правната уредба на ШИС? Има ли изключения или специални правила по отношение на обработването на данни от ШИС, по-специално за целите на правоприлагането и миграцията? Какви законодателни промени са направени или са планирани в резултат на влизането в сила на Директива (ЕС) 2016/680 на Европейския парламент и на Съвета на Регламент (ЕС) 2016/679?

Б. ОРГАН (И) ЗА ЗАЩИТА НА ДАННИТЕ

1. Кои национални надзорни органи за защита на данните (ОЗД) са компетентни по отношение на надзора на ШИС, за да се гарантира съответствие с изискванията за защита на данните? Компетентният по отношение на надзора върху защитата на данните в ШИС ОЗД компетентен ли и е също и да упражнява надзор върху защитата на данните във всички органи, имащи достъп до данни от ШИС, напр. правоприлагащите органи?

2. Ако има няколко ОЗД, отговарящи за надзора върху защитата на данните в ШИС, моля, уточнете и обяснете разпределението на задачите между различните органи, както и тяхното сътрудничество и координация.

3. Представете преглед на организацията, независимостта, бюджета и числеността на персонала на ОЗД.

4. Моля, опишете изискванията, разпоредбите и процедурата за назначаване на член(ове) на ОЗД. Моля, опишете разпоредбите и процедурата за уволнение на член на ОЗД. Направете по-подробно описание на човешките, финансовите и техническите ресурси на компетентните ОЗД:

4.1. като предоставите наред с другото данни за броя на правните експерти и експертите в областта на ИТ и др., включително и за развитието му през последните три години и за планираните промени, и по-специално за броя на експертите, работещи по въпроси, свързани с ШИС, включително надзор. Моля, представете информация за това кой подбира и назначава персонала на ОЗД на всички нива, както и информация дали персоналът на органите е под изключителното ръководство на члена(овете) на съответния ОЗД,

4.2. като предоставите информация за бюджетните процедури за определяне на

бюджета на ОЗД, както и данни за бюджета, включително развитието му през последните три години и планираните промени,

4.3. включително и информация за програмите за обучение.

5. Моля, представете информация дали е възможно оказването на външно влияние, било то пряко, или непряко, върху изпълнението на задачите и упражняването на правомощията от ОЗД — напр. право на правителството да осъществява надзор върху работата на ОЗД. Моля, представете информация дали ОЗД могат да търсят или приемат указания от когото и да било.

6. Представете задълженията на ОЗД и компетенциите му в общ план и в частност в случаите на нарушения на сигурността на данните и на злоупотреба с данни (т.е. правото да образува разследване, включително правомощия като правото на влизане във всички помещения на Н.ШИС, както и в помещенията, в които се съхраняват резервни копия, при наличие на такива, да достъпва всички бази данни и да издава решения със задължителна сила и др.).

7. Как ОЗД си сътрудничи(ат) с Н.ШИС, бюрото SIRENE, компетентните министерства и вътрешното длъжностно лице по защита на данните с цел да се контролира обработването на лични данни от Н.ШИС?

8. Разполага ли ОЗД с план за надзора на обработването на данни в ШИС? Ако отговорът е положителен, моля, уточнете и представете копие на този план.

9. Моля, опишете всички дейности на ОЗД за надзор на ШИС (инспекции, одити и др.), които са проведени след предишната оценка по Шенген. Моля, посочете датата/периода на всяка надзорна дейност, опишете нейното приложно поле и резултати, както и последващите действия във връзка с нея.

10. Моля, посочете по-специално дали и кога е проведен национален одит на Н.ШИС в съответствие с член 44, параграф 2 от Регламент (ЕО) № 1987/2006 и член 60, параграф 2 от Решение 2007/533/ПВР и ако да, опишете обхвата и резултатите от одита, както и последващите действия.

11. Проверява ли периодично ОЗД съдържанието на ШИС, както и регистрационните файлове на ШИС?

12. Моля, посочете по-специално дали и кога е проведен национален одит на Н.ШИС в съответствие с член 41, параграф 2 от Регламент (ЕО) № 767/2008 и член 8, параграф 6 от Решение 2008/633/ПВР и ако да, опишете обхвата и резултатите от одита, както и последващите действия.

13. Моля, представете копие от докладите/решенията от надзорните дейности.

14. Каква информация предоставят органите по ШИС (администраторът на лични

данни в Н.ШИС и органите, които имат достъп до ШИС, например полицията, граничната охрана) на гражданите относно ШИС като цяло?

В. ОБЩЕСТВЕНА ОСВЕДОМЕНОСТ И ПРАВА НА СУБЕКТИТЕ НА ДАННИ

1. Каква информация предоставят органите по ШИС (администраторът на лични данни в Н.ШИС и органите, които имат достъп до ШИС, например полицията, граничната охрана) на гражданите, по-специално относно обработването на лични данни в ШИС, както и относно правата на субектите на данни, включително правото на жалба/обжалване до ОЗД и обжалване пред националните съдилища? Моля, посочете каква информация се предоставя, в каква форма (например листовки, интернет) и на какви езици, както и къде тя може да бъде намерена (включително връзките).

2. Каква информация предоставя(т) ОЗД на гражданите относно ШИС като цяло, и по-специално относно обработването на лични данни в ШИС, както и относно правата на субектите на данни, включително правото на жалба/обжалване до ОЗД и обжалване пред националните съдилища? Моля, посочете каква информация се предоставя, в каква форма и на какви езици, както и къде тя може да бъде намерена (включително връзките).

3. Кой орган (и кой отдел по-точно) отговаря за разглеждането на отправени от субекти на данни искания, свързани с ШИС? Имат ли субектите на данни право на пряк достъп (искането трябва да бъде отправено до органите по ШИС - в случая администратора на лични данни) или непряк достъп (искането трябва да бъде отправено до ОЗД) или могат ли да бъдат използвани и двете възможности? Моля, опишете процедурата за упражняването на правата на субектите на данни във връзка с ШИС, включително дали исканията са безплатни, на какви езици се приемат искания и се изпращат отговори, както и относно приложимите крайни срокове за отговорите. В случай на непряк достъп какъв е обхватът на задачите на ОЗД? Предоставят ли органите по ШИС (по-специално администраторът на лични данни) и ОЗД образци на писма за упражняването на правата на субектите на данни? Имате ли стандартни отговори на субектите на данни?

4. Съществуват ли законови ограничения за упражняването на правата на субектите на данни (моля, посочете подробности)?

5. Предоставяте ли информация на субектите на данни, ако няма данни за тях в ШИС? В кои случаи се отказва достъп? Каква е формулировката на отговора, който изпращате на заявителите, подали искане за достъп, в случай, когато трябва да се откаже предоставянето на информация?

6. Включвате ли в отговора информация относно възможностите за обжалване и правото да се подаде жалба до ОЗД?

7. Колко искания имате след последната оценка по Шенген? Моля, посочете (ако е възможно) колко искания са били за достъп, за поправка или за заличаване и по какъв начин те са били обработени.

8. Средно колко време отнема на органите разглеждането на искания на субекти на данни, свързани с обработването на данни в ШИС?

9. Какви средства за правна защита съществуват (член 43 от Регламент (ЕО) № 1987/2006 и член 59 от Решение 2007/533/ПВР)? Имало ли е жалби, предявени срещу решения относно искания, свързани с правата на субекти на данни? Колко, относно какво и какъв е бил резултатът?

10. Има ли съдебни производства, инициирани от субекти на данни? Колко, относно какво и какъв е бил резултатът?

11. Колко жалби или обжалвания във връзка с правата на субектите на данни в ШИС са изпратени до ОЗД? Относно какво и какъв е бил резултатът? Какво точно проверява(т) ОЗД в случай на жалби или обжалвания от физически лица относно техни лични данни, включени в ШИС? Средно колко време отнема на ОЗД да разгледа(т) случай (жалба или обжалване), свързан с обработването на данни в ШИС?

12. Какви процедури са установени, за да се гарантира изпълнението на решение на упълномощен орган на друга шенгенска държава, постановено в съответствие с член 43, параграфи 1 и 2 от Регламент (ЕО) № 1987/2006 и членове 1 и 2 от Решение 2007/533/ПВР? Приведени ли са в изпълнение съдебните решения на друга държава и ако не - защо?

Г. ОРГАНИЗАЦИОННИ И ТЕХНИЧЕСКИ ВЪПРОСИ

1. Кой е администраторът на лични данни за Н.ШИС? Администраторът на лични данни компетентен ли е и по отношение на бюрото SIRENE? Има ли съвместни администратори на лични данни? Има ли публични органи, действащи като администратори на лични данни за Н.ШИС? Моля, обяснете по-подробно.

2. Възлагате ли на външни изпълнители определени услуги, свързани с ШИС? Опишете подробно кои услуги се възлагат на външни изпълнители. Колко външни изпълнители са ангажирани? Публични или частни са външните изпълнители? Съществува ли писмен договор между администратора на лични данни на Н.ШИС и външния изпълнител, в който са заложени клаузи относно защитата на данните? Моля, опишете какъв вид изисквания са заложени в договора. Възложените на външни

изпълнители услуги дистанционно ли се предоставят, или на място? Моля, представете подробности. Ползват ли се външните изпълнители с привилегии на администратори на бази данни? Какви мерки сте въвели, за да гарантирате осъществяването на контрол върху действията на външните изпълнители?

3. Моля, опишете правомощията, задачите и участието на вътрешното длъжностно лице по защита на данните на администратора на лични данни в ШИС във връзка с Н.ШИС, включително бюрото SIRENE. Има ли длъжностното лице за защита на данните редовни контакти с ОЗД? Моля, обяснете по-подробно.

4. Опишете мерките за физическа сигурност на основния и резервния център на Н.ШИС.

5. Какви технически и организационни мерки за сигурност са въведени с оглед защита на данните от ШИС? По отношение на изискванията за сигурност съгласно член 10 от Регламент (ЕО) № 1987/2006 и Решение 2007/533/ПВР, относно които се иска информация в главата за ШИС на настоящия въпросник, моля, в допълнение опишете по-подробно:

5.1. Системата на разрешенията за достъп, включително изискванията за предоставяне и подновяване на правата за достъп. Колко често и по какъв начин се предоставя подновяване на разрешение за достъп? Кой взема тези решения? Имате ли правила и/или политика за актуализиране/заличаване на права за достъп след промяна на ролята на служители или след напускане на служители?

5.2. Системата за автентификация, за да се получи достъп до базата данни на ШИС.

5.3. Имате ли правила/политика относно паролите?

5.4. Дали всички органи с право на достъп до ШИС II или до съоръженията за обработване на данни са създали профили с описание на функциите и задълженията на лицата, които имат разрешение за достъп и за въвеждане, актуализиране и заличаване на данни и търсене в тях? Предоставят ли се тези профили на националните надзорни органи при поискване? Моля, предоставете списък на тези профили.

5.5. Какви мерки са взети, за да се наблюдава ефективността на мерките за сигурност, посочени в член 10, параграф от Регламент (ЕО) № 1987/2006 и в Решение 2007/533/ПВР? Какви организационни мерки са предприети (самоконтрол), свързани с вътрешното наблюдение за гарантиране на спазването на Регламент (ЕО) № 1987/2006 и Решение 2007/533/ПВР?

5.6. По какъв начин длъжностното(ите) лице(ца) по защита на данните е(са) ангажирано(и) с въпросите на сигурността?

5.7. Ангажирано(и) ли е(са) длъжностното лице(ца) по защита на данните с някой от въпросите на сигурността?

6. Колко дълго се съхраняват сигналите и допълнителната информация? Какви са разпоредбите/политиката за тяхното заличаване?

7. Моля, обяснете дали, от кои органи и как се съхраняват на национално равнище регистри (записи) относно създаването, актуализирането, заличаването и други действия, предприети във връзка със сигнали? Колко дълго се съхраняват такива регистри? Каква е процедурата за заличаването им?

8. Моля, обяснете дали и от кои органи се съхраняват на национално равнище регистри (записи) за всеки достъп до данни и всеки обмен на данни от ШИС. Какво е съдържанието на тези регистри?

9. Колко дълго се съхраняват посочените регистри? Моля, включете данни за регистрите относно достъпа до данни от ШИС, включително, ако такива регистри се съхраняват в приложение за достъп до ШИС.

10. Моля, опишете политиката и практиката за прочистване/заличаване на записи.

11. Моля, обяснете дали, от кои органи и как регистрите (записите), които се съхраняват на национално равнище, относно всеки достъп до данни и всеки обмен на данни от ШИС се подлагат на проверка с цел наблюдение, наред с другото, на законосъобразността на обработването на данни. Моля, опишете подробно методите на проверка и честотата на проверките. Използват ли се инструменти за автоматична проверка на записите? Какъв беше резултатът от тези проверки на записите след последната оценка по Шенген?

12. Имате ли политика за осъществяване на защита на личния живот още при проектирането и по подразбиране за всяко ново обработване на лични данни? Извършвате ли оценка на въздействието на предвидените операции по обработване върху защитата на личните данни (оценка на въздействието върху защитата на данните)? Моля, предоставете информация (ако е възможно копие) за резултатите от оценката (оценките) на въздействието върху защитата на данните. Провеждате ли консултации с ОЗД или други специалисти по защита на данните при създаването на ново обработване на данни?

13. Имате ли правила и/или политика относно носенето на собствени устройства (напр. използване на USB устройства, лаптопи)? Имате ли правила и/или политика относно работата от разстояние?

14. Как служба Н.ШИС се справя с инциденти, свързани със сигурността (засягащи поверителността и/или целостта на данните от ШИС; нарушения на сигурността на личните данни)?

15. Съществуват ли правила/политики за начина, по който следва да се процедира при случаи на злоупотреба със самоличност?

16. Моля, опишете подробно какви мерки са предприети в изпълнение на задължението за самонаблюдение на всеки орган, имащ право на достъп до данни от ШИС, и дали е налице сътрудничество с ОЗД.

17. Каква информация относно сигурностга на данните и защитата на данните се предоставя на персонала на органите, които управляват ШИС и имат достъп до ШИС? Моля, посочете каква информация се предоставя на служителите на бюрото SIRENE и на крайните потребители на ШИС. Моля, опишете по-подробно съдържанието и формата. Участват ли в разработването на информационните материали органът по защита на данните (отговарящ за надзора на Н.ШИС) и вътрешното длъжностно лице по защита на данните на администратора на лични данни?

18. Какво обучение относно сигурността на данните и защитата на данните се предоставя на персонала на органите, които управляват ШИС и имат достъп до ШИС? Моля, посочете какво обучение се предоставя на служителите на бюрото SIRENE и на крайните потребители на ШИС. Моля, представете копие на плановете за обучение, ако са налични. Колко често се предоставя обучението? Участват ли в изготвянето на програмата за обучение ОЗД (отговарящ за надзора на националната Н.ШИС) и вътрешното длъжностно лице по защита на данните на администратора на лични данни? Участват ли те в самите мерки за обучение?

Д. МЕЖДУНАРОДНО СЪТРУДНИЧЕСТВО

1. По какъв начин си сътрудничат органите по защита на данните, органите по ШИС с органите на други държави членки, по-специално по отношение на въпроси, свързани с ШИС?

VII. ДОПЪЛНИТЕЛНИ ВЪПРОСИ ПРИ ИЗВЪРШВАНЕ НА ПРОВЕРКИ НА ВИЗОВАТА ИНФОРМАЦИОННА СИСТЕМА (ВИС)

А. ЗАКОНОДАТЕЛСТВО

1. Кое общо национално законодателство за защита на данните е приложимо за обработването на лични данни от Визовата информационна система (ВИС)?

2. Има ли на национално равнище специално законодателство и/или разпоредби относно обработването на лични данни във връзка с правната уредба на ВИС? Има ли изключения или специални правила по отношение на обработването на данни от ВИС? Какви законодателни промени са направени или са планирани в резултат на прилагането на Директивата относно правоприлагането в областта на защитата на данните и Общия регламент относно защитата на данните?

Б. ОРГАН (И) ЗА ЗАЩИТА НА ДАННИТЕ

1. Кой национален ОЗД е компетентен по отношение на надзора на ВИС, за да се гарантира съответствие с изискванията за защита на данните? Компетентният по отношение на надзора върху защитата на данните във ВИС ОЗД компетентен ли е също и да упражнява надзор върху защитата на данните във всички органи, имащи достъп до данни от ВИС, напр. правоприлагащите органи?

2. Ако има няколко ОЗД, отговарящи за надзора върху защитата на данните в ВИС, моля, уточнете и обяснете разпределението на задачите между различните органи, както и тяхното сътрудничество и координация.

3. Представете преглед на организацията, независимостта, бюджета и числеността на персонала на ОЗД.

4. Моля, опишете изискванията, разпоредбите и процедурата за назначаване на член(ове) на ОЗД. Моля, опишете разпоредбите и процедурата за уволнение на член на ОЗД. Направете по-подробно описание на човешките, финансовите и техническите ресурси на компетентните ОЗД:

4.1. като предоставите наред с другото данни за броя на правните експерти и експертите в областта на ИТ и др., включително и за развитието му през последните три години и за планираните промени, и по-специално за броя на експертите, работещи по въпроси, свързани с ВИС, включително надзор. Моля, представете информация за това кой подбира и назначава персонала на ОЗД на всички нива, както и информация дали персоналът на органите е под изключителното ръководство на члена(овете) на съответния ОЗД,

4.2. като предоставите информация за бюджетните процедури за определяне на

бюджета на ОЗД, както и данни за бюджета, включително развитието му през последните три години и планираните промени,

4.3. включително и информация за програмите за обучение.

5. Моля, представете информация дали е възможно оказването на външно влияние, било то пряко, или непряко, върху изпълнението на задачите и упражняването на правомощията от ОЗД — напр. право на правителството да осъществява надзор върху работата на ОЗД. Моля, представете информация дали ОЗД могат да търсят или приемат указания от когото и да било.

6. Представете задълженията на ОЗД и компетенциите му в общ план и в частност в случаите на нарушения на сигурността на данните и на злоупотреба с данни (т.е. правото да образува разследване, включително правомощия като правото на влизане във всички помещения на ВИС, както и в помещенията, в които се съхраняват резервни копия, при наличие на такива, да достъпва всички бази данни и да издава решения със задължителна сила и др.).

7. Как ОЗД си сътрудничи(ат) с органа(ите), управляващ(и) ВИС, компетентните министерства и вътрешното длъжностно лице по защита на данните с цел да се контролира обработването на лични данни във ВИС?

8. Разполага ли ОЗД с план за надзора на обработването на данни в ВИС? Ако отговорът е положителен, моля, уточнете и представете копие на този план.

9. Моля, опишете всички дейности на ОЗД за надзор на ВИС (инспекции, одити и др.), които са проведени след предишната оценка по Шенген, включително в консулски служби и при външни доставчици на услуги. Моля, посочете датата на всяка надзорна дейност, опишете нейното приложно поле и резултати, както и последващите действия във връзка с нея.

10. Проверява ли периодично ОЗД съдържанието на ВИС, както и регистрационните файлове на ВИС?

11. Моля, представете копие от докладите/решенията от надзорните дейности.

В. ОБЩЕСТВЕНА ОСВЕДОМЕНОСТ И ПРАВА НА СУБЕКТИТЕ НА ДАННИ

1. Каква информация относно ВИС като цяло предоставят на гражданите (и по-специално на кандидатите) различните визови органи/органи по ВИС (на централно равнище, а също и в посолствата и консулствата), както и външните доставчици на услуги?

2. Каква информация предоставят различните визови органи/органи по ВИС (на

централно равнище, а също и в посолствата и консулствата), по-специално относно обработването на лични данни във ВИС, както и относно правата на субектите на данни, включително правото на жалба/обжалване до ОЗД и обжалване пред националните съдилища? Моля, посочете каква информация се предоставя, в каква форма (например листовки, интернет) и на какви езици, както и къде тя може да бъде намерена (включително връзките).

3. Каква информация предоставя(т) ОЗД на гражданите относно ВИС като цяло, и по-специално относно обработването на лични данни във ВИС, както и относно правата на субектите на данни, включително правото на жалба/обжалване до ОЗД и обжалване пред националните съдилища? Моля, посочете каква информация се предоставя, в каква форма и на какви езици, както и къде тя може да бъде намерена (включително връзките).

4. Кой орган (и кой отдел по-точно) отговаря за разглеждането на отправени от субект на данни искания, свързани с ВИС? Моля, опишете процедурата за упражняването на правата на субектите на данни във връзка с ВИС, включително дали исканията са безплатни, на какви езици се приемат искания и се изпращат отговори, както и относно приложимите крайни срокове за отговорите. Предоставят ли органите по ВИС и ОЗД образци на писма за упражняването на правата на субектите на данни? Имате ли стандартни отговори на субектите на данни?

5. Съществуват ли законови ограничения за упражняването на правата на субектите на данни (моля, посочете подробности)?

6. Колко искания имате след последната оценка по Шенген? Моля, посочете (ако е възможно) колко искания са били за достъп, за поправка или за заличаване и по какъв начин те са били обработени.

7. Средно колко време отнема на органите разглеждането на искания на субекти на данни, свързани с обработването на данни във ВИС?

8. Какви средства за правна защита съществуват (член 40 от Регламент (ЕО) № 767/2008 и член 14, параграф 8 от Решение 2008/633/ПВР)? Имало ли е жалби, предявени срещу решения относно искания, свързани с правата на субекти на данни? Колко, относно какво и какъв е бил резултатът?

9. Имало ли е съдебни производства, инициирани от субекти на данни? Колко, относно какво и какъв е бил резултатът?

10. Колко жалби или обжалвания във връзка с правата на субектите на данни във ВИС са изпратени до ОЗД? Относно какво и какъв е бил резултатът? Какво точно проверява(т) ОЗД в случай на жалби или обжалвания от физически лица относно техни лични данни, включени във ВИС? Средно колко време отнема на ОЗД да разгледа(т)

случай (жалба или обжалване), свързан с обработването на данни във ВИС?

Г. ОРГАНИЗАЦИОННИ И ТЕХНИЧЕСКИ ВЪПРОСИ

1. Моля, опишете подробно процедурата за подаване на заявление за виза и начина, по който различните органи и служби си сътрудничат относно обработването на лични данни.

2. Кой е администраторът на лични данни за националната ВИС? Администраторът на лични данни компетентен ли е и по отношение на посолствата и консулствата? Отговаря ли същият администратор за процеса на издаване на визи на границата? Има ли съвместно администриране от страна на различните органи, участващи в процедурата по издаване на визи? Ако е така, дали тези органи са сключили споразумение или друга договореност с цел изясняване на отговорностите им при обработването на лични данни, например споразумение (споразумения) между администратор и обработващ лични данни? Моля, представете копие от това споразумение(я) или тази договореност(и). Каква е ролята на другите органи, които участват в процеса на издаване на визи? Има ли обработващ лични данни?

3. Възлагате ли на външни изпълнители услуги, свързани с процедурата по издаване на визи, включително на външни доставчици на услуги? Опишете подробно кои услуги се възлагат на външни изпълнители. Колко външни изпълнители са ангажирани? Публични или частни са външните изпълнители? Съществува ли писмен договор между администратора на лични данни на Н.ВИС и външния изпълнител, в който са заложени също клаузи относно защитата на данните? Моля, опишете какъв вид изисквания са заложени в договора. Възложените на външни изпълнители услуги дистанционно ли се предоставят, или на място? Моля, представете подробности. Ползват ли се външните изпълнители (на централно равнище) с привилегии на администратори на бази данни и имат ли те достъп до данни от ВИС? Какви мерки сте въвели, за да гарантирате осъществяването на контрол върху действията на външните изпълнители?

4. Поддържат ли Вашите консулства „местни списъци за предупреждение” с данни за лица с установено минало с нередности, които могат да обосноват отказ за издаване на виза? Изпълнени ли са изискванията съгласно националното законодателство за защита на данните относно съставянето и поддържането на такъв местен списък за предупреждение? Дали органите за защита на данните са били консултирани, или са участвали по друг начин по отношение на този въпрос?

5. Моля, опишете правомощията, задачите и участието на администратора на лични данни от ВИС/вътрешното длъжностно лице по защита на данните на администратора на

лични данни във връзка с националната ВИС. Има ли длъжностното лице за защита на данните редовни контакти с ОЗД? Моля, обяснете по-подробно.

6. Моля, представете най-общо системата и архитектурата на мрежата на националните системи (без технически подробности), които са свързани с ВИС (както за основния, така и за резервния център, ако такъв съществува). Как се прави резервно копие?

7. Моля, предоставете списък на услугите или органите, които са упълномощени да обработват, да влизат и да имат достъп до данните от ВИС. Разграничете формата на достъп, т.е. пряк, непряк. Посочете кои органи имат „достъп само за четене" на данни и по отношение на какво. Посочете правомощията, които обосновават необходимостта от достъп до такива данни.

8. По какъв начин се осъществява надзор върху достъпа до данните от ВИС от администратора(ите) на лични данни в консулствата, централните органи по издаване на визи, външните гранични контролно-пропускателни пунктове и т.н.?

9. Какви технически и организационни мерки за сигурност са въведени с оглед на защитата на личните данни, свързани с ВИС? Моля, опишете всички мерки за сигурност и национални изисквания, въведени по отношение на националната ВИС в съответствие с член 32 от Регламент (ЕО) № 767/2008 и член 9 от Решение 2008/633/ПВР, като в допълнение, моля, обяснете по-подробно:

9.1 Има ли официален план за сигурност, който да е предназначен за националната ВИС и да отговаря на изискванията, определени в член 32 от Регламент (ЕО) № 767/2008? Опишете процеса на приемане и актуализиране на плана за сигурност и свързаните мерки.

9.2 Моля, опишете Вашите политики за управление на потребителите и паролите.

9.3 По какъв начин гарантирате, че само оторизирани потребители имат достъп до ВИС, както и че този достъп съответства на разрешените от закона цели?

9.4 Моля, опишете нивото на защита, мерките за защита и организацията на сигурността, прилагани към компютризирани национални приложения, които имат достъп до или обработват данни във ВИС. В описанието следва да се посочат мерките за сигурност, които се прилагат за контролиране на достъпа от външния свят (защитни стени, откриване на проникване и др.), както и достъпът от изпълнители по договори.

9.5 Въведените методи за контрол на физическия достъп до помещенията на националната ВИС;

9.6 Въведените правила за защита, които да се прилагат относно обработването

на данни от ВИС в националната система (посочете също така процедурите за документите на хартиен носител, тяхното архивиране, срок на съхранение и унищожаване);

9.7 Системата на разрешенията за достъп, включително изискванията за предоставяне и подновяване на правата за достъп. Моля, опишете мерките и прегледите, проведени, за да се гарантира, че всеки потребител има достъп само до категориите данни, за които е оторизиран, и за целите, за които е оторизиран. Колко често и по какъв начин се предоставя подновяване на разрешение за достъп? Имате ли правила и/или политика за актуализиране/заличаване на права за достъп след промяна на ролята на служители или след напускане на служители?

9.8 Системата за автентификация, за да се получи достъп до базата данни на ВИС.

9.9 Имате ли правила/политика относно паролите?

9.10 Дали всички органи с право на достъп до ВИС или до съоръженията за обработване на данни са създали профили с описание на функциите и задълженията на лицата с право на достъп и въвеждане, актуализиране и заличаване на данни и търсене в тях, както и дали тези профили се предоставят на националните надзорни органи при поискване; моля, предоставете списък на тези профили.

9.11 Регистрирането на всеки достъп и всички трансакции на крайни потребители, и на техническия персонал, който се занимава например с поддръжка или ремонт, включително трансакциите за разпечатване и екранно отпечатване („print screen”).

9.12 Какви мерки са взети, за да се наблюдава ефективността на мерките за сигурност, посочени в член 32 от Регламент (ЕО) № 767/2008 и в Решение 2008/633/ПВР, и какви организационни мерки са предприети (самоконтрол), свързани с вътрешното наблюдение за гарантиране на спазването на Регламент (ЕО) № 767/2008 и на член 9 от Решение 2008/633/ПВР?

9.13 По какъв начин длъжностното(ите) лице(а) по защита на данните е(са) ангажирано(и) с въпросите на сигурността?

9.14 Ангажирано(и) ли е(са) длъжностното(ите) лице(ца) по защита на данните с някой въпрос на сигурностга?

10. Моля, обяснете дали, от кои органи и как регистрите, които се съхраняват на национално равнище, относно всеки достъп до данни и всеки обмен на данни от ВИС се подлагат на проверка с цел наблюдение, наред с другото, на законосъобразността на обработването на данни. Моля, опишете подробно методите на проверка и честотата на проверките. Използват ли се инструменти за автоматична проверка на записите? Какъв

беше резултатът от тези проверки на записите след последната оценка по Шенген? Колко дълго се съхраняват посочените регистри? Налични ли са статистически данни за неоторизиран достъп и опити за достъп?

11. Моля, обяснете колко дълго се съхраняват визовите досиета на национално равнище, къде и в какъв формат. Съществуват ли правила/политика относно тяхното унищожаване?

12. Имате ли политика за осъществяване на защита на личния живот още при проектирането и по подразбиране за всяко ново обработване на лични данни? Извършвате ли оценка на въздействието на предвидените операции по обработване върху защитата на личните данни (оценка на въздействието върху защитата на данните)? Моля, предоставете информация (ако е възможно копие) за резултатите от оценката (оценките) на въздействието върху защитата на данните. Провеждате ли консултации с ОЗД или други специалисти по защита на данните при създаването на ново обработване на данни?

13. Имате ли правила и/или политика относно носенето на собствено устройство (напр. използване на USB устройства, лаптопи)? Имате ли правила и/или политика относно работата от разстояние?

14. Как администраторът на лични данни на ВИС се справя с инциденти, свързани със сигурността (засягащи поверителностга и/или целостга на данните от ВИС; нарушения на сигурностга на личните данни)?

15. Моля, опишете подробно какви мерки са предприети в изпълнение на задължението за самонаблюдение на всеки орган, имащ право на достъп до данни от ВИС, и дали е налице сътрудничество с националния надзорен орган.

16. Моля, опишете мярката за наблюдение на обработването на лични данни от страна на консулствата. Колко често централните органи правят проверки в консулствата? Какви мерки се използват за тази цел? Участва ли ОЗД в тези дейности за наблюдение? По какъв начин?

17. Моля, опишете мярката за наблюдение на обработването на лични данни от външните доставчици на услуги (ако се използват техни услуги). Колко често централните органи подлагат на проверка външните доставчици на услуги, какви мерки се използват за тази цел? Участва ли ОЗД в тези дейности за наблюдение? По какъв начин?

18. Каква информация относно сигурността на данните и защитата на данните се предоставя на персонала на органите, които управляват националната ВИС и имат достъп до ВИС? Моля, посочете каква информация се предоставя на консулските служители и местния персонал в консулствата, както и на другите крайни потребители на ВИС. Моля, опишете по-подробно съдържанието и формата. Участват ли в разработването на

информационните материали органът по защита на данните (отговарящ за надзора на ВИС) и вътрешното длъжностно лице по защита на данните на администратора на лични данни?

19. Какво обучение относно сигурността на данните и защитата на данните се предоставя на персонала на органите, които управляват ВИС и имат достъп до ВИС? Ако имате специална програма за обучение на консулските служители преди тяхното назначаване/на местните служители, преди да заемат определена длъжност, тя включва ли части относно защитата на данните? Моля, опишете по-подробно и представете копие на плана(овете) на обучението. Моля, уточнете какво обучение се предоставя на други крайни потребители на ВИС; моля, представете копие на плановете за обучение, ако са налични. Колко често се предоставя обучението? Участват ли в изготвянето на програмата за обучение надзорният орган по защита на данните (отговарящ за надзора на националната ВИС) и вътрешното длъжностно лице по защита на данните на администратора на лични данни? Участват ли те в самите мерки за обучение?

Д. МЕЖДУНАРОДНО СЪТРУДНИЧЕСТВО

1. По какъв начин си сътрудничат органите по защита на данните, органите по ВИС с органите на други държави членки, по-специално по отношение на въпроси, свързани с ВИС?

2. По какъв начин си сътрудничите с други държави членки, за да гарантирате правото на физическите лица на достъп, поправяне и заличаване на данни от ВИС (член 39 от Регламент № 767/2008)? Това специално международно сътрудничество регламентирано ли е в националното законодателство?

VIII. ДОПЪЛНИТЕЛНИ ВЪПРОСИ ПРИ ИЗВЪРШВАНЕ НА ПРОВЕРКИ НА ИНФОРМАЦИОННАТА СИСТЕМА НА ЕВРОПОЛ

ХАРМОНИЗИРАНИ КРИТЕРИИ ЗА ВКЛЮЧВАНЕ НА ИНФОРМАЦИЯ В ИНФОРМАЦИОННАТА СИСТЕМА НА ЕВРОПОЛ

А. УВОД

Изложените по-долу критерии за включване на информация в Информационната система на Европол (ИСЕ) имат за цел да установят хармонизиран подход между държавите членки (ДЧ) за оценка на съответствието с приложимите разпоредби на Решението на Съвета за Европол (РСЕ). Те дават възможност на Националните звена „Европол“ (НЗЕ) и останалите компетентни органи да извършват проверки на данните, които се въвеждат в ИСЕ, съгласно единен набор от критерии.

Критериите са разработени въз основа на резултатите от дейността на Работната група на Ръководителите на Националните звена „Европол“, изложени в доклад EDOC#693642 от 30 октомври 2013 г. Изготвеният от Работната група доклад беше одобрен от Управителния съвет на заседанието му на 3 декември 2013 г. и обсъден от Председателя на Работната група и делегацията на Съвместния надзорен орган (СНО) на Европол на 14 януари 2014 г. (EDQC#704559v1A).

Целта на документа е да предостави практически насоки, които пряко повишават качеството на информацията, която се въвежда в ИСЕ. Във връзка с това контекстът, в който следва да се въведе информацията, е представен без използването на сложни правни понятия. Взети са предвид приложимите разпоредби и правила за прилагане на РСЕ, и по-конкретно „Политиката за използване и управление на ИСЕ“ (документ (EDOC#132O92).

Когато това е уместно, в текста са включени примери, които илюстрират практически критериите за включване в информационната система. Това важи и за критериите за невключване в системата, които в определени случаи също могат да подпомогнат вземането на решение.

Б. КОМПЕТЕНТНОСТ НА ЕВРОПОЛ

Заподозрените и осъдените лица, както и т.нар. потенциални бъдещи престъпници, могат да бъдат включени в ИСЕ, единствено във връзка с престъпления в рамките на компетентността на Европол.[1]

Правомощията на Европол включват организираната престъпност, тероризма и други форми на тежки престъпления, изброени в Приложението към РСЕ. Задължително

1 Член 12, параграф 1 наРСЕ.

условие за въвеждането на лице в ИСЕ е две или повече държави членки да са засегнати от престъплението по начин, който налага следването на общ подход, поради мащаба, значението и последиците от престъплението.[2]

Неизчерпателният списък по-долу съдържа критериите, които следва да бъдат изпълнени, за да бъде преценено, че деянието засяга две или повече държави членки по смисъла на РСЕ:

- Гражданство на извършителите
- Известни сфери на дейност на извършителите
- Предходни осъждания (регистри за съдимост) или полицейско досие на извършителите
- Чести международни пътувания на извършителите
- Разузнавателни данни за престъпната дейност (наблюдение, GPS данни, информатори, операции под прикритие и т.н.)
- Информация от други канали/системи, напр. съвпадение на ДНК или на пръстови отпечатъци/отпечатъци от длани в ШИС II или системата Prum
- Място на произход/поток/местоназначение на стоките
- Тежки престъпления, които се явяват трансгранични по своето естество
- Местожителство на жертвата
- Свидетелски показания

Информационната система на Европол може да бъде използвана като „международен инструмент за сигнализация", който позволява включването в ИСЕ на данните на извършители на престъпления в по-горе упоменатия смисъл, включително такива чиято вина все още не е доказана извън всяко разумно съмнение, които имат връзки с две или повече държави членки.

Пример, предоставен от СНО: Националните правоохранителни органи в ДЧ „А" разследват извършено убийство. Може да бъде установено, че използваният пистолет е произведен в друга ДЧ.

В приложението към РСЕ „убийството" е изрично упоменато като форма на сериозно престъпление в обхвата на правомощията на Европол. Сам по себе си, обаче, фактът, че използваният пистолет е произведен в друга ДЧ не обосновава в достатъчна степен включването на заподозряното лице в ИСЕ.

- Данните, свързани с престъпления от изцяло национален характер, не подлежат на включване в ИСЕ
- Допускането на трансграничен елемент във връзка с извършването на тежки престъпления трябва да бъде разумно обосновано и при съмнение да бъде

2 Член 4, параграф 1 на РСЕ.

подробно обосновано в поле „допълнителни бележки“.

Мащабът, значението и последствията от престъпленията трябва да налагат следването на общ подход.

Пример, предоставен от СНО: Бракониер застрелва мечка, защитена като застрашен вид, за което следва да понесе санкция съгласно националното законодателство за опазване на околната среда. Преди да бъде застреляна, мечката е забелязана на територията на няколко ДЧ.

В приложението към РСЕ „престъпленията спрямо околната среда“ са изрично упоменати като форма на сериозно престъпление в обхвата на правомощията на Европол. Сам по себе си, обаче, фактът, че мечката е забелязана в няколко ДЧ не обосновава в достатъчна степен въвеждането на данните бракониера в ИСЕ.

В. ВЪВЕЖДАНЕ НА ДАННИТЕ НА НЕПЪЛНОЛЕТНИ ЛИЦА

Обработката на лични данни, свързани с непълнолетни лица, се счита за операция по обработване на чувствителни данни, която изисква специално внимание от страна на екипа, който въвежда информацията.

Включването на данни на непълнолетни лица в ИСЕ е регламентирано в глава 3.4.1 на Политиката за използване и управление на ИСЕ (EDOC#132Q92).

- Съображенията за включването на лични данни на непълнолетно лице в ИСЕ следва да почиват на Конвенцията на ООН за правата на детето.
- За целите на ИСЕ всяко упоменаване на непълнолетно лице означава: всяко лице на възраст под 18 години. Това е опростено тълкуване на член 1 на Конвенцията, който гласи:*„За целите на тази Конвенция „дете“ означава всяко човешко същество на възраст под 18 години освен ако съгласно закона, приложим за детето, пълнолетието настъпва по-рано.“*
- В ИСЕ не подлежат на въвеждане данни на малолетни лица на възраст до 15 години.

Самата Конвенция призовава за установяването на минимален възрастов праг на наказателна отговорност, под който се счита, че децата не са способни да нарушат наказателния закон. Възрастовата граница от 15 години обаче не е изрично упомената.

Наблюдават се съществени различия в националните законодателства, регламентиращи въвеждането на данни на непълнолетни лица в националните бази данни на правоохранителните органи на отделните държави, като в някои случаи тези прагове са под 15 години.

Независимо от това възрастовият праг за включването на данни на непълнолетни лица, установен в Политиката за използване и управление на ИСЕ, се счита за уместен

предвид обстоятелството, че операциите по обработка в ИСЕ могат да имат по-тежки последици за лицата в сравнение с тези в националните бази данни.

Възможността за въвеждането в ИСЕ на данните на заподозрени или осъдени за престъпления непълнолетни лица, почива на два елемента. Първият е опитът на служителите на правоохранителните органи с непълнолетни лица на възраст между 15 и 18 години, осъдени за престъпления в сферата на компетентност на Европол, които по своя мащаб вече не се считат за изключително редки. С други думи, това са непълнолетни лица на възраст от 15 до 18 години, извършили престъпления, които не са рядко срещани.

Вторият елемент е, че Конвенцията на ООН за правата на детето изключва *произволната* и *незаконосъобразна* намеса в личния живот:

*Член 16, алинея 1 гласи: „*Никое дете не трябва да бъде подлагано на произволна или незаконна намеса в неговия личен живот, семейство, дом или кореспонденция, нито на незаконно посегателство срещу неговата чест и репутация.“

Това означава, че подозрението, че непълнолетно лице е извършило престъпление, което попада в сферата на компетентност на Европол и е наказуемо съгласно приложимото национално законодателство, трябва да съответства на горната разпоредба. По отношение на осъдените непълнолетни лица, изискването за съответствие се прилага по подразбиране, а тежестта на извършеното престъпление автоматично изключва възможността за произволна намеса.

Глава 3.4.2 на Политиката за използване и управление на ИСЕ (документ EDOC#132Q92) съдържа следното пояснение:

▪ Необходимо е в поле „допълнителни бележки“ да бъде посочена препратка към разпоредбите съгласно националното законодателство, въз основа на които лицето може да бъде подведено под отговорност и осъдено за извършеното престъпление.

Г. ВЪВЕЖДАНЕ НА ДАННИТЕ НА НЕИЗВЪРШИЛИ ПРЕСТЪПЛЕНИЯ ЛИЦА

В ИСЕ могат да бъдат въвеждани данните единствено на заподозрени или осъдени за извършено престъпление лица или на т.нар. потенциални бъдещи престъпници (във връзка с престъпления в сферата на компетентност на Европол).[3]

По-конкретно, в областта на трафика на хора има случаи, в които въведените в ИСЕ данни не разграничават жертвите на престъпления и лицата, заподозрени в тяхното извършване.

Признава се, че има примери за бивши жертви на престъплението трафик на хора,

[3] Член 12, параграф 1 наРСЕ.

които впоследствие стават активни участници в наказуемото деяние. Обстоятелството, че заподозряно лице в миналото е било считано за жертва, не е пречка за въвеждането на данните му в ИСЕ.

▪ В случаи на съмнение относно ролята на заподозряно лице като жертва в миналото, това следва да се упомене в поле „допълнителни бележки“ за яснота.

▪ За осъдените за този вид престъпление лица не се изисква упоменаване на ролята на жертва в миналото, тъй като активното участие в извършването на престъплението вече е установено от съд.

Д. ПРИЛОЖЕНИЕ: ПРИЛОЖИМИ РАЗПОРЕДБИ НА РСЕ

Член 4

Правомощия

1. Компетентността на Европол обхваща организираната престъпност, тероризма и другите тежки форми на престъпност, посочени в приложението към настоящото решение, които засягат две или повече държави членки по начин, изискващ от държавите членки общ подход поради размера и значимостта на престъпленията и последствията от тях.

2. По препоръка на управителния съвет Съветът определя приоритетите за Европол, по-специално като взема предвид изготвените от Европол стратегически анализи и оценки на заплахите.

3. Компетентността на Европол обхваща също така свързаните престъпления. За свързани престъпления се считат следните деяния:

а) престъпления, извършени с цел придобиване на средства за извършване на деяния, за които Европол е компетентен;

б) престъпления, извършени с цел помагане или извършване на деяния, за които Европол е компетентен;

в) престъпления, извършени с цел да се осигури безнаказаност на деяния, за които Европол е компетентен.

Член 8

Национални звена

1. Всяка държава членка създава или определя национално звено, което да осъществява посочените в настоящия член задачи. Във всяка държава-членка има назначен служител за ръководител на националното звено.

(...)

4. Националните звена:

а) предоставят на Европол по собствена инициатива информация и разузнавателни данни, от които той се нуждае за осъществяване на своите задачи;

б) отговарят на искания на Европол за информация, разузнавателни данни и консултации;

в) грижат се за актуализиране на информацията и разузнавателните данни;

г) извършват оценка на информацията и разузнавателните данни в съответствие с националното законодателство, отнасящо се за компетентните органи, и им предават тези материали;

д) подават до Европол искания за консултации, информация, разузнавателни данни и анализи;

е) предоставят на Европол информация, която да се съхранява в неговите бази данни;

ж) гарантират спазването на законодателството при всеки обмен на информация между тях и Европол.

Член 12

Съдържание на информационната система на Европол

1. Информационната система на Европол може да се използва само за обработка на онези данни, които са необходими за изпълнение на задачите на Европол. Въведените данни се отнасят до:

а) лица, които съгласно националното законодателство на съответната държава членка са заподозрени в извършване или в участие в престъпление, за което Европол е компетентен, или които са осъдени за такова престъпление;

б) лица, за които съобразно националното законодателство на съответната държава членка са налице факти или приемливи основания да се счита, че ще извършат престъпления, за които Европол е компетентен.

2. Данните, свързани с посочените в параграф 1 лица, могат да включват само следните сведения:

а) фамилно име, моминско име, собствени имена и всякакви псевдоними и приети имена;

б) дата и място на раждане;

в) гражданство;

г) пол;

д) пребиваване, професия и местонахождение на съответното лице;

е) номера за социално осигуряване, шофьорски книжки, документи за самоличност и паспортни данни; и

ж) при необходимост – други отличителни белези, които биха могли да спомогнат за идентификацията, включително всякакви специфични, конкретни и непроменливи физически отличителни белези като дактилоскопни данни и ДНК профил (установен от некодиращата част на ДНК).

3. Освен за данните, посочени в параграф 2, информационната система на Европол може да се използва и за обработка на следните сведения за посочените в параграф 1 лица:

а) престъпления, предполагаеми престъпления, както и време, място и начин на тяхното (предполагаемо) извършване;

б) средства, които са били използвани или могат да бъдат използвани за извършване на престъпленията, включително информация за юридически лица;

в) служби, които се занимават със случая, и съответни регистрационни номера на досиетата;

г) предполагаемо членство в престъпна организация;

д) осъждания, когато те са свързани с престъпления, за които Европол е компетентен;

е) страната, която е въвела данните.

Тези данни може да се въвеждат и когато все още не съдържат информация за конкретни лица. Когато Европол въвежда данните самостоятелно, както и когато предоставя съответните номера на досиета, се посочва също и източникът на данните.

4. Допълнителната информация, с която разполагат Европол или националните звена относно лицата, посочени в параграф 1, може да се предоставя съответно на всяко национално звено или на Европол при поискване. Националните звена предоставят информация в съответствие с националното си законодателство.

Когато допълнителната информация касае едно или повече свързани престъпления съгласно посоченото в член 4, параграф 3, съхранените в информационната система на Европол данни се отбелязват по съответен начин, за да могат националните звена и Европол да обменят информация относно свързаните престъпления.

5. Ако производството срещу въпросното лице е окончателно прекратено или ако това лице е окончателно оправдано, данните относно делото, по което е взето такова решение, се заличават.

Член 13

Използване на информационната система на Европол

1. Националните звена, служителите за връзка, директорът, заместник-директорите или надлежно упълномощените служители на Европол имат право директно да въвеждат данни в информационната система на Европол, както и да извличат данни от нея. Европол може да извлича данни, когато това е необходимо за изпълнение на неговите задачи във връзка с конкретен случай. Извличането на данни от националните звена и от служителите за връзка се осъществява в съответствие със законовите, подзаконовите и административните разпоредби и процедури на имащата достъп страна, като се спазват всички допълнителни разпоредби на настоящото решение.

2. Единствено страната, която е въвела данните, може да ги изменя, поправя или заличава. Когато друга страна има причини да смята, че данните, посочени в член 12, параграф 2, са неточни или желае да ги допълни, тя незабавно уведомява страната, която е въвела данните. Страната, която е въвела данните, незабавно разглежда това уведомление и ако е необходимо, незабавно изменя, допълва, поправя или заличава данните.

3. Когато системата съдържа данни, посочени в член 12, параграф 3, относно дадено лице, всяка страна може да въведе допълнителни данни съобразно тази разпоредба. В случай на явно противоречие между въведените данни съответните страни се консултират помежду си и постигат съгласие.

4. Когато една страна възнамерява изцяло да заличи данните, посочени в член 12, параграф 2, които е въвела за дадено лице, и когато данните по член 12, параграф 3 за същото лице са били въведени от други страни, отговорността по отношение на законодателството за защита на данните в съответствие с член 29, параграф 1 и правото да се изменят, допълват, поправят и заличават тези данни съгласно член 12, параграф 2 се прехвърлят на следващата страна, която е въвела данни за това лице по член 12, параграф 3. Страната, която възнамерява да заличи данни, уведомява за своето намерение страната, на която е прехвърлена отговорността по отношение на защитата на данните.

5. Отговорността за допустимостта на извличането, въвеждането и измененията в информационната система на Европол се носи от извличащата, въвеждащата или изменящата страна. Трябва да е възможно тази страна да бъде идентифицирана. Предоставянето на информация между националните звена и компетентните органи на държавите-членки се урежда от националното законодателство.

6. Освен националните звена и лицата по параграф 1, компетентните органи, определени за тази цел от държавите-членки, също могат да отправят запитвания до

информационната система на Европол. В резултатите от търсенето обаче ще се посочва единствено дали търсените данни са налични в информационната система на Европол. Допълнителна информация може да бъде получена след това чрез националното звено.

7. Информацията относно определените в съответствие с параграф 6 компетентни органи, включително последващите изменения, се предава на генералния секретариат на Съвета, който я публикува в Официален вестник на Европейския съюз.

Член 29

Отговорност в работата по защита на данните

1. Отговорността за данните, които се обработват в Европол, по-специално по отношение на законосъобразността на тяхното събиране, предаването им на Европол и въвеждането им, както и на тяхната точност и актуалност и проверката на сроковете за съхранение, се носи от:

а) Държавата членка, която е въвела или по друг начин е съобщила данните;

(...)

Въпросник

15-10

През 2012 г. Съвместният надзорен орган (СНО) публикува доклад относно изискванията към Националните звена на Европол във връзка с обработването на данни в информационната система на Европол[4] (ИСЕ) с цел преглед на нивото на национален контрол върху данните, които се въвеждат в ИСЕ и гарантиране, че тези данни подлежат на проверка и отговарят на приложимите критерии.

Целта на въпросника е да се получи информация за последващите действия за изпълнение на препоръките, отправени от СНО на Европол, и нивото на съответствие с хармонизираните критерии.

1.Известно ли Ви е съществуването на документ, наречен „Хармонизирани критерии за въвеждане на информация в Информационната система на Европол (ИСЕ)“?

Да ☐ Не ☐

Ако ***да***, кои от следните дейности са изпълнени от Националното звено във връзка с документа?

- документът е изпратен по електронната поща на всички служители на звеното ☐
- качен е на вътрешен уебсайт, до който имат достъп служителите на звеното ☐
- обсъден е в рамките на звеното ☐
- съществува документ, съдържащ насоки за служителите в звеното ☐
- организирано е обучение за изпълнение на установените хармонизирани критерии ☐
- организирана е среща с други компетентни органи за обсъждане на препоръките ☐
- не са предприемани конкретни действия в резултат на документа. ☐

2. Използвате ли програма за автоматично въвеждане на данни в ИСЕ?

Да ☐ Не ☐

3. Какви действия се предприемат в случай на съмнение относно това дали извършено престъпление попада в обхвата на компетентността на Европол?

[4] ***Доклад относно изискванията към Националните звена на Европолвъв връзка с обработването на данни вИнформационната система на Европол:***
http://europoljsb.consilium.europa.eu/media/257488/12-61%20rev%2007%20final%20report%20survey%20national%20units.pdf

- изпраща се информация до Европол ☐
- изпраща се информация до Европол с разяснения в полето за допълнителни бележки ☐
- информацията не се изпраща на Европол
- прави се преценка на мащаба, значението и последиците на престъплението преди да се вземе решение относно последващите действия ☐
- използване на определените от Европол критерии за идентифициране на необходимостта от общ подход ☐
- други *(моля, посочете)* ☐

……

IX. ДОПЪЛНИТЕЛНИ ВЪПРОСИ ПРИ ИЗВЪРШВАНЕ НА ПРОВЕРКИ НА ИНФОРМАЦИОННАТА СИСТЕМА НА ЕВРОДАК

1. УВОД

Системата Евродак е създадена с Регламент (ЕО) № 2725/2000 на Съвета от 11 декември 2003 година (Регламент Евродак), допълнен с Регламент (ЕО) № 407/2002 на Съвета от 28 февруари 2002 година. Двата текста бяха преработени в Регламент (ЕС) № 603/2013 от 26 юни 2013 година (преработен текст на Регламент Евродак), който влезе в сила на 20 юли 2015 г.

През 2012 г. Групата за координация на надзора на Евродак (ГКН) прие стандартизиран план за извършването на национални проверки. В светлината на новата правна рамка, уреждаща системата Евродак, на своята среща на 15 април 2016 г. Групата за координация на надзора прие документът да бъде адаптиран към новите правни изисквания, залегнали в преработения Регламент.

Първоначалният преглед на образеца от 2012 г. беше извършен от органите по защита на данните на Обединеното кралство и Румъния в периода май—септември 2016 г. Документът беше приет на срещата на ГКН на 23 ноември 2016 г. след двумесечни консултации с членовете на ГКН.

2. ОБХВАТ

Стандартизираният план за проверки е структуриран по начин, който помага на органите по защита на данните да осъществяват надзор (съгласно член 30) и извършват задължителни ежегодни одити (съгласно член 32, параграф 2) и проверки на системата Евродак. Документът и неговата структура предоставят надеждна методология за проверка на националните пунктове за достъп (НПД) до системата Евродак, като същевременно позволяват и по-добър анализ и сравнение на резултатите.

Стандартизираните планове за проверка съдържат набор от въпроси относно защитата на данните и сигурността, които оценяват организационните и техническите мерки за използване на системата, както и нивото на съответствие на Националните пунктове за достъп с изискванията на Регламент (ЕС) № 603/2013.

Въпросникът обхваща въведените формални и неформални процедури, които гарантират законосъобразното събиране, съхранение, предаване и други видове обработване на данни от Евродак от и между Националните пунктове за достъп (НПД) и Централното звено. Събраната чрез въпросника информация, включително някои препратки към подкрепящи документи, позволява по-добро разбиране и преценка на

съществуващите различия на национално ниво, разсейва потенциални тревоги във връзка с рисковете за сигурността, улеснява конструктивния диалог между държавите членки, установява общи най-добри практики и идентифицира области, в които е необходимо подобрение — от законодателно или друго естество — с оглед на изпълнението на изискванията.

Въпросникът съдържа седем части:

А. Общо описание.

Въпроси относно компетентността, позицията и вътрешната организационна структура на националните органи, отговорни за НПД на Евродак (3 въпроса)

Б. Предаването на данни между местните служби на НПД (3 въпроса) — включва въпроси относно естеството на събирането, съхранението и предаването на данни за пръстови отпечатъци в местните служби (1 въпрос в 6 части).

Въпросите се отнасят до това дали и какви мерки за сигурност (дигитални (1 въпрос в 4 части) и физически (1 въпрос в 3 части) се предприемат за гарантиране на сигурността на данните (напр. проследяване на достъпа до данни) и трансфер на събрани данни.

В. Съхранение на данни и операции между пунктовете за достъп и централната система (това е основната част на въпросника, която обследва въведените в НПД технически мерки и мерки за сигурност)

Този раздел обследва:

▪ Процедурите за съхранение на данни в НПД и последващото им предаване и сравнение с данните на Централното звено (2 въпроса);

▪ Организационните мерки за сигурност (1. относно персонала, напр. ролите и отговорностите на служителите, вкл. по отношение на управлението на сигурността на данните, съхранението на данните като професионална тайна и познаването, разбирането и обучението по теми, свързани със сигурността на информацията; и 2. относно данните, напр. периода на съхранение след обработката) (5 въпроса)

▪ Техническите мерки за сигурност (относно ИТ оборудването, напр. мрежова архитектура и топология, софтуер/приложения и електронна поща, управление на потребителите, удостоверяване на потребителите, политика за преносими носители на електронно съдържание (напр. CD/USB), последващи проверки на въведените в Евродак данни, криптиране на данни, съхранявани на място, политика за резервни копия на съхраняваните от НПД данни, сигурност на предаването на информация от и до Централното звено на Евродак, дигитално сертифициране на сигурността на

комуникациите с Централното звено на Евродак (т.е. електронна поща) (10 въпроса), както и

▪ Мерки за физическа сигурност (т.е. контрол на физическия достъп до помещенията и ИТ оборудването, сигурност на физическите документи и на помещенията за съхранение на дигитални данни на Евродак) (2 въпроса)

Г. Трансфер на данни до компетентните органи по Дъблинския регламент/Регламента за убежището (1 въпрос)

Д. Процедура за сравнение и предаване на данни за целите на правоприлагането (1 въпрос в 4 части)

Е. Предаване на данни между национални органи (3 въпроса)

Въпроси относно предаването на свързани с Евродак данни на други компетентни национални органи и — в случаите на такова предаване на такива данни — неговите цели, начин на документиране и съхранение на данните (1 въпрос в 5 части), както и въведените организационни и технически мерки за проследяване на предаването на данни (2 въпроса).

Ж. Трансфери на данни до трети страни, международни организации или частни субекти (1 въпрос)

Въпросите имат за цел да установят дали свързани с Евродак данни се предават на трети страни, международни организации или частни субекти и, ако това е така, с каква цел.

З. Общи процедури за сигурност (включва целия процес на обработване на данни). (7 въпроса)

Въпроси относно съществуването или естеството на свързаните с дейността на НПД процедури за сигурност по отношение на:

▪ Политиката за сигурност (т.е. нейния обхват, преглед и оценка на риска) (1 въпрос в 4 части);

▪ Планове за възстановяване след бедствия (напр. уебсайтове за резервни копия на данните и процедури за непрекъснатост на работата) (1 въпрос в 3 части);

▪ Нарушение на сигурността на данните (напр. управление и докладване а инциденти, включително проследяване) (1 въпрос)

▪ Управление на активи (напр. проследяване, надзор и разпределение на ИТ активите, използвани за обработване на събраните данните) (1 въпрос в 7 части);

▪ Лица, обработващи данни/аутсорсинг (въпроси, свързани с подизпълнители или външни страни, вкл. приложими мерки за сигурност, ако лицата имат достъп до ИТ/мрежовата инфраструктура за обработването на данни за свързаните с Евродак дейности) (1 въпрос), както и

▪ Собствени (вътрешни) одити (т.е. въпроси, свързани с вътрешния мониторинг и одит на общите мерки за сигурност и на мерките за сигурност на ИТ системата) (2 въпроса)

И. Информация и права на субектите на данни (2 въпроса)

Обследване дали и ако да как жалбоподателите биват информирани за правата им за защита на данните в рамките на процеса на обработване на данни за целите на Евродак. Въпросникът цели да установи и дали причината за неинформираност на субектите на данни относно техните права в рамките на процеса не е основната причина за липсата на жалби до националните ОЗД от страна на търсещи убежище лица във връзка с процедурата по снемане на отпечатъци и потенциалните проблеми, които могат да възникнат във връзка с тази процедура (напр. нечетими пръстови отпечатъци).

3. ЗАКЛЮЧЕНИЕ

Въпросникът цели да подпомогне властите в оценката на изпълнението на преработения Регламент Евродак от държавите членки и да установи прилаганите мерки за сигурност. ГКН предлага той да бъде използван от националните надзорни органи като част от извършваните одити. С други думи, използването на въпросника и методологията ще гарантира, че обхватът на одитите в отделните държави членки ще бъде идентичен, което от своя страна ще предостави на ГКН възможност за сравнение на ситуациите в тях.

Към въпросника е добавена колона за събрани доказателства, в която следва да се дадат допълнителни разяснения относно мерките за приложение, които всяка държава членка предприема за повишаване на сравнимостта на информацията, която ще бъде събрана от надзорните органи на държавите членки.

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
Раздел А: ОБЩО ОПИСАНИЕ — НПД НА ЕВРОДАК					
Описание на НПД на Евродак	В 1	Опишете вътрешната организация и компетенциите на органа, в рамките на който функционира Националния пункт за достъп (НПД) на Евродак: а) Моля да предоставите съответната органограма. б) Моля да посочите нормативните актове, съгласно които е създаден и функционира НПД. в) Органът отговаря ли за процедурите по предоставяне на убежище съгласно Дъблинския регламент? Ако не, моля да предоставите информация за тези органи. г) Съществува ли друг орган, който предоставя техническо или организационно съдействие на институцията, която отговаря на НПД? Моля, посочете. д) Изградени ли са други национални системи за отпечатъци (например за търсещи убежище лица или с по-широк обхват? Ако да, моля посочете съответните компетентни институции, които отговарят за тези системи. НПД свързан ли е с тези системи? е) Коя институция притежава правомощия да подписва актове във връзка с дейността на НПД? ж) От колко лица се състои екипът? з) Моля, посочете адреса, на който се помещава НПД.	Въпросникът не се отнася до други национални системи за пръстови отпечатъци, но въпреки това изследването на техни евентуални връзки със системата на НПД, представлява интерес.	Общи разпоредби – член 3, параграф 2	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
Органи, определени за целите на правоприлагането	B 2	Кои институции имат правомощия да отправят искания за сравнение на данни за пръстови отпечатъци с данните, които се съхраняват в централната система за целите на правоприлагането? 1) Има ли списък на оперативните звена, които имат правомощия да изискват сравнения на пръстови отпечатъци с тези в системата Евродак? 2) Колко оперативни звена имат правомощия да правят такива сравнения? 3) Какви процедури са установени във връзка с тази функционалност? 4) Каква е процедурата при неактивни звена?		Член 5 , параграф 1 (Органи на държавите членки, определени за целите на правоприлагането)	
Проверяващи органи, определени за целите на правоприлагането	B 3	Кой е проверяващият орган по член 6 на Регламента Евродак? 1) Проверяващият орган подчинен ли е на контролен орган или на структура, на която докладва за дейността си? 2) Ако това е така, по какъв начин е гарантирана неговата независимост при извършването на проверки за съответствие с условията за сравнения с данните в системата Евродак? 3) Каква е процедурата за назначаване или оправомощаване на служители в рамките на проверяващия орган?		Член 6 , параграф 1 (Проверяващи органи на държавите членки, определени за целите на правоприлагането)	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		4) На какво основание се упълномощават служителите (напр. длъжност, категория или степен) за извършване на сравнения с данните в системата Евродак? 5) Наличен ли е списък на надлежно упълномощените лица?			
Раздел Б: Предаване на данни между служби по места и НПД					
Описание на свързаните с Евродак дейности	B 4	Опишете процедурите за събиране и предаване на данни за пръстови отпечатъци и други лични данни от службите по места към НДП: а) Кои са местните служби, компетентни за събирането на пръстови отпечатъци и други лични данни за целите на Евродак? б) Какви технически и процедурни методи за събиране и съхранение на пръстови отпечатъци се използват в местните служби? в) Какви контролни механизми се прилагат на ниво местни служби за гарантиране на качеството на пръстовите отпечатъци? г) Каква е процедурата/какви мерки се предприемат при предаването на данни на НПД?	Параграфи б) и е) се отнасят до събирането и съхранението на данни от/в местните служби и следователно не са пряко свързани с проверката на НПД (но независимо от това представляват интерес с оглед общия поток на свързани с Евродак данни).	Общи разпоредби - член 3, параграф 5	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		Процедурата предвижда ли конкретен срок за предаване на данните на НПД? Процесът документира ли се? Ако това е така, моля, приложете копие от документа. д) Какви средства се използват за предаване на данните на НПД (електронна поща, факс, поща, куриер, други)? е) Местните служби съхраняват ли копия на данните след предаването им на НПД? Ако да, за какъв срок? Изпращат ли се данните на други национални органи? ж) Какви данни събират местните служби от субектите на данни (категории лични данни)? з) Каква е процедурата при лица на възраст до 14 години? Събират ли се техни лични данни?			
Технически мерки за сигурност	B 5	а) Как предотвратявате неоторизираното четене, копиране, промяна или изтриване на данните при електронното им предаване между местните служби и упълномощения орган, който има достъп до НПД? б) Защитени електронни канали ли се използват? Ако да, пояснете, кои са тези канали и как функционират. в) Съществува ли възможност за проверка на самоличността на изпращача и получателя? Ако да, пояснете основните механизми.		Член 34, параграфи 1 и 2, точка „й“ (сигурност на данните)	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		г) Данните криптират ли се в точката на предаване? Ако да, обяснете използвания метод за криптиране.			
Мерки за физическа сигурност	B 6	а) Как предотвратявате неоторизираното четене, копиране, промяна или заличаване на данните при електронното им предаване между местните служби и упълномощения орган, който има достъп до НПД ? б) Защитени електронни канали ли се използват? Ако да, пояснете кои са тези канали и как функционират. в) Документира ли се процедурата (напр. чрез полагане на подписи на отговорните лица). Ако да, моля, приложете копие.	Този въпрос включва и свързаните с процедурата организационни мерки.	Член 34, параграфи 1 и 2 (сигурност на данните)	
Раздел B: Съхранение на данни в НПД и предаване на данни от и до централната система на Евродак					
Описание на свързаните с Евродак дейности	B 7	Опишете процедурите за съхранение на данни в системата на НПД: а) Данните на място в НПД ли се съхраняват? Ако да, кои данни или формуляри? В каква форма? Съществува ли електронна база данни и/или информацията се съхранява на хартия? Данните периодично ли се съхраняват? Какъв е срокът на съхранение на данни в НПД? б) Каква е процедурата на съхранение на данни в системата на НПД след предаването им от местните служби (напр. има ли система за номериране, как се създават нови файлове и т.н.). Процедурата документира ли се? Ако да, моля, приложете копие.		Член 3, параграф 4	
	B 8	Опишете процедурата за подаване на данни до централната	По време на проверката	Член 22, параграф 2	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		система и работата с резултатите от сравненията: а) Как се осъществява предаването на информация към централната система? (електронно, чрез имейл)	могат да бъдат дадени примери за такива информационни потоци		
		б) Какви видове данни се предават за кандидатите за убежище и лицата по членове 9, 14 и 17 на Регламент (ЕС) № 603/2013?			
		в) Каква процедура се следва при съвпадение и липсата на съвпадение с данни при извършена проверка? Резултатите от сравнението проверяват ли се незабавно от експерт по пръстови отпечатъци съгласно член 25, параграф 4?		Член 25, параграф 4	
		г) Резултатите от централната система съхраняват ли се на място в НПД?			
		д) Каква процедура се следва в случай на предварително заличаване на данни (член 13 от Регламент (ЕС) № 603/2013)?			
		е) Каква процедура се следва при искане за маркиране на данни (член 13 от Регламент (ЕС) № 603/2013)?			
Организационни мерки за сигурност	B 9	Роли и отговорности на служителите на определените проверяващи органи: а) Функциите, ролите и задълженията на всеки служител		Член 34, параграф 2, точка „ж“	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		ясно дефинирани и документирани ли са? б) По какъв начин се разпределят задачите и функциите на всеки служител? Въведена ли е документирана процедура? Ако да, моля да предоставите копие. в) Следва ли се принципа на разделение на ролите/отговорностите? Ако да, обяснете как този принцип се следва на практика.			
	B 10	Как гарантирате запазването на професионалната тайна от страна на служителите, ангажирани с обработването на свързани с Евродак данни?		Член 34, параграф 2, точки „д“, „е“ и „и“	
	B 11	а) Назначен ли е ръководител по сигурността или друг служител с еквивалентна роля? Ако да, опишете съответните му отговорности и задължения. б) Ако не, кой в рамките на определения орган отговаря за сигурността и интегритета на ИТ системите? в) Кой носи отговорност за оперативното изпълнение на политиките/процедурите?		Член 23, параграф 2 – не е изрично упоменат, но е необходим за предприемане на необходимите мерки за сигурност.	
	B 12	а) Съществува ли документирана и формална процедура за повишаване на информираността/образованието/обучението на потребителите/служителите по информационна сигурност? б) Обучението съобразено ли е с нуждите, ролите и отговорностите на персонала? Какво включва то?		Член 23, параграф 2 – не е изрично упоменат, но е необходим за повишаване на сигурността на персонала.	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		в) Как е организирано (напр. електронно, практическо)? г) Имат ли всички служители достъп до курсовете? д) Кога се провежда обучението? Предвидени ли са опреснителни курсове? На какви интервали е обучението? е) Предвидено ли е обучение за служителите на граждански договори/подизпълнителите? ж) Моля, пояснете как гарантирате, че служителите са достатъчно квалифицирани и разбират изискванията за своите роли в организацията? з) Съществуват ли документи/доказателства за предходни или планирани обучения на служителите за работа със системата?			
	В 13	а) Как институцията Ви гарантира, че данните, свързани с кандидатите за убежище и чуждите граждани не се съхраняват извън законоустановените срокове? б) Колко дълго се съхраняват резултатите от търсения в системата в НПД? в) Съществува ли процедура за сигурно унищожаване на съхраняваните в НПД данни след края на периода на обработването им? Процедурата предвижда ли съхранение на документи на хартия и в електронен формат? Документира ли се? Ако да, моля, приложете копие.		Член 34, параграф 2, точка „г“; член 23, параграф 1, точка „г“; Член 33, параграф 5 Член 29, параграф 11	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент	Събрани доказателства
		г) За какъв период се съхраняват исканията за достъп?			
Технически мерки за сигурност	B 14	Опишете подробно архитектурата и топологията на използваните ИТ системи (сървъри, работни места, мрежа, операционни системи и т.н.). Опишете също така мрежите, използвани за комуникация между НПД и Централното звено, както и мрежите за комуникация между НПД и други национални системи.		Член 22, параграф 1	
	B 15	Опишете софтуера/приложението и имейл услугата, използвана за комуникация с Централното звено на Евродак в контекста на Регламента Евродак.		Член 34, параграф 2, точка „з“	
	B 16	Какви процедури за управление на потребителите са разработени и се прилагат за недопускане на неоторизиран достъп, запис, копиране, изменение или заличаване на данни от системата Евродак? а) Как контролирате логическия достъп до данните от Евродак в приложението за обработване, оперативните системи и софтуера? б) Има ли уникални партиди на потребители (акаунти) за всеки потребител? в) Колко потребители имат права на „администратор“? Кои профили на потребители съответстват на профила на администратор?	Въпросът е свързан с управлението на потребителите на всички нива (операционна система, приложения, мрежа)	Член 34, параграф 2, Точки „б“, „в“, „г“ и „е“	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		г) Поддържате ли списък на потребители и потребителски профили (групи) и съответните им права на достъп и/или оторизационни права? На какви интервали се извършва преглед на списъците с потребители и с правата на достъп на потребители? д) Достъпът на потребителите ограничен ли е само до данните, които са в тяхната компетентност? Как се постига това? Правата на достъп на потребителите дефинирани ли са съобразно техните роли? е) Документират ли се горните процедури? Ако да, моля, приложете копие.			
	B 17	а) Какъв метод за идентифициране на потребителите се прилага? Предоставя ли той възможност за достъп в режим на конфиденциалност? б) По отношение на паролите: 1. Разработена ли е политика за паролите? Ако да, опишете нивата, на които са необходими пароли (BIOS, операционна система, софтуерни приложения за свързани с Евродак дейности), дължина, специални символи,	Въпросът е свързани с идентифицирането на потребителите на всички нива (операционна система, приложения, мрежа)	Член 34, параграф 1, точка „ж“	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		интервали, през които паролите задължително се променят. 2. Документирана ли е политиката? Ако да, приложете копие. в) Каква е процедурата за неизползвани имена на бивши служители за достъп (*log names*)? Остават ли те в системата или се изтриват автоматично? Ако да, след какъв период от време? Колко често се прави преглед на неизползваните имена за достъп?			
	B 18	а) Какви процедури са въведени по отношение на преносимите носители на данни (напр. CD/USB) за предотвратяване на неоторизираното прочитане, копиране, променяне или изтриване от неоторизирани лица на данни (или носители на данни), свързани с Евродак? б) Каква е политиката Ви по отношение на преносимите носители на данни? в) Какво е нивото на контрол — липса на възможност за физическо свързване или забрана за физическо свързване, но съществуваща техническа възможност за това? г) Ако преносимите носители на данни са разрешени, криптирани ли са? Използват ли се само вътрешни и/или препоръчителни преносими носители на данни?		Член 34, параграф 2, буква „в“ (Контрол на носителите на данни)	
	B 19	а) Какви механизми за валидиране са изградени за проверка на информацията, въведена в Евродак?		Член 34, параграф 2, точка „и“ член 25, параграф 1	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		б) По какъв начин се гарантира, че въведената в системата Евродак чрез НПД информация е с необходимото качество? Прави ли се проверка за качество преди въвеждане на информацията? Каква е процедурата, ако данните за пръстовите отпечатъци бъдат отхвърлени от системата? Тази процедура документира ли се? в) Колко често получавате съобщения от Централната система, че изпратената информация не е с необходимото качество? В тези съобщения посочва ли се причината за тази преценка? г) Достъпът до свързани с Евродак данни регистрира ли се? Какво показват регистровите данни? Моля, опишете информацията, която се съдържа в протоколните файлове (logs) или в документацията? д) Кой има достъп до протоколните файлове и какво е нивото на достъп на съответните служители? е) Използват ли се редовно протоколните файлове за одитни цели? ж) Какви механизми са установени за гарантиране на автентичността на протоколните файлове?			
	B 20	Какви мерки са предприети за предотвратяване на неоторизираното въвеждане или преглеждане на данни, които се обработват в Евродак? Моля, опишете механизмите/процедурите/техниките/стандартите за предотвратяване на неоторизирания преглед, изменение или заличаване на данни (напр. криптиране, сегментиране)?		Член 34, параграф 2, буква „г“ – неизрично упоменат, но важен, особено за сигурността на данните за пръстовите отпечатъци.	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
Физически мерки за сигурност	B 24	Какви мерки се предприемат за физически контрол на достъпа до помещенията и съответното ИТ оборудване (компютри, кабели, табла), използвани за операциите, свързани данни от системата Евродак?		Член 34, параграф 2, букви „а“ и „б“	
	B 25	а) Какви мерки се предприемат за гарантиране на сигурността на физическите документи и носителите, на които се съхраняват данни от системата Евродак (напр. документи, свързани с кандидати за убежище, резервни копия на данни)? б) Как са защитени данните от неоторизиран достъп, копиране, промяна или заличаване (напр. документира ли се достъпът до файлове, могат ли да се правят копия и ако да, за кого и с каква цел и т.н.)? в) Как се гарантира, че оторизираните лица има достъп до данните единствено в рамките на своите компетенции?		Член 34, параграф 2, букви „а“, „б“, „д“ и „е“	
Раздел Г: Предаване на данни от системата Евродак на компетентните национални органи по Дъблинския регламент (убежище)					
Описание на свързаните с Евродак дейности	B 26	Опишете процедурите за изпращане на данни от Евродак от НПД до компетентните национални органи във връзка с процедури по предоставяне на убежище или Дъблинския регламент (вж. Въпрос 1): а) По какъв начин въведените в Евродак данни се изпращат на компетентните национални органи? б) Какви са конкретните процедури за предаването на данни? Документират ли се? Ако да, моля, приложете копие. в) Допълнителна информация за достъпа и обработването на		Неприложимо	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		данни от съответните органи и мерките, които те предприемат, за да гарантират сигурното боравене и предаване на данни от системата Евродак като елемент от Дъблинската процедура, включително използването на DubliNET. Документират ли се тези			
Раздел Д: Процедура за сравняване и предаване на данни за целите на правоприлагането					
	В 27	а) Когато бъде изготвено искане за сравняване на данни с данните от системата Евродак, документира ли се това? Ако да, от кого? б) Документира ли се и обосновката на искането? в) Изпълнени ли са условията по член 20, параграф 1, букви „а“, „б“ и „в“, които са правното основание за исканията за сравнение? г) Има ли доказателства за неуспешни сравнения с данните от други системи?		Членове 19, 20, 32, параграф 2 и 33	
Раздел Е: Предаване на данни от Евродак на други национални органи					
Описание на свързаните с Евродак дейности	В 28	а) Изпращат ли се/предоставят ли се данните на други органи, участващи пряко в процедурите по Дъблинския регламент? б) Ако да, моля, посочете тези органи както и правното основание за предаване на данни от системата Евродак до тях.	Въпрос в) не е пряко свързан с проверката, но отговорът на въпроса представлява интерес с оглед проследяване на цялостния поток на информация	Член 20	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		в) Какви са точните процедури за това предаване? Документирани ли са? Ако да, предоставете копие. г) Данните от EURODAC изпращат ли се или се свързват с други национални системи за пръстови отпечатъци (например, за да се провери дали засегнатото лице е имало престъпна дейност)? Ако отговорът е да, те съхраняват ли се в тази система ? д) Извършват ли се проверки, за да се гарантира, че данните на EURODAC се обработват от тези други национални органи в съответствие с регламента и са обхванати от същите изисквания за защита на данните?	.		
Организационни мерки за сигурност	B 29	Какви организационни мерки са предприети за извършването на проверки и до кои други компетентни национални органи се предават данни от Евродак чрез оборудването за пренос на данни?		Член 34, параграф 2, буква „з“	
Технически мерки за сигурност	B 30	Какви технически мерки са предприети за извършването на проверки и до кои други компетентни национални органи се предават данни от Евродак чрез оборудването за пренос на данни?		Член 34, параграф 2, буква „з“	
Раздел Е: Предаване на данни от системата Евродак на трети страни, международни организации и частни субект					
Забрана за трансфер на данни	B 31	а) Предават ли се или предоставят ли се данни на трети държави, международни организации или частни субекти, установени извън територията на Европейския съюз?		Член 35, параграф 1, (Забрана за трансфер на данни до	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		б) Ако да, кои са те и какво е правното основание за трансфер на данни от системата Евродак до тях?		трети страни, международни организации или	
Раздел Ж: Общи процедури за сигурност (приложими за всички свързани с Евродак дейности)					
Политика за сигурност	В 32	Разработена ли е политика за сигурност и/или установени ли са процедури за сигурност, които обхващат част или всички дейности на НПД? Документират ли се те? Ако това е така: а) Какъв е обхватът на политиката/процедурите? б) На какви интервали подлежат на преразглеждане? в) Как се свеждат до знанието на потребителите? г) Правили ли сте оценка на риска и/или извършвате ли дейности по управление на риска и как се документират те?		Член 23, параграф 2 – не е изрично упоменат, но е необходим за приемането на мерки за сигурност.	
План за непрекъснатост на работния процес	В 33	а) Има ли разработени планове за действие в извънредни ситуации за защита на критична инфраструктура (с изключение на резервните копия на данни)? Ако това е така, моля, пояснете. б) Има ли разработени планове/процедури за непрекъснатост на работния процес? Опишете основните елементи на тези процедури. в) Документирани ли са тези процедури? Ако да, моля, приложете копие.		Член 34, параграф 2, буква „а“	
Нарушаване на сигурността на	В 34	Установен ли е формален процес за докладване на инциденти,		Член 23, параграф 2 –	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
управление и докладване на инциденти		свързани с нарушаването на сигурността на данните или информацията? а) Кой отговаря за тази процедура? На какъв интервал се преразглежда? б) Има ли процес по отношение на „научените уроци“? в) Включва ли той събиране на доказателства за инциденти? г) Докладван ли е някога инцидент, свързан със сигурността на данните?		не е изрично спомената, но е необходим за гарантирането на ранен отговор и за смекчаване на рисковете за сигурността.	
Управление на активи	B 35	Какви са процедурите за управление на активи? а) Имате ли регистър на ИТ активите (различни от финансовите активи)? На какви интервали се преразглежда? б) Разполагате ли със софтуер за управление на активите? в) Как се идентифицират информационните активи? г) Заприходен ли е на конкретен служител всеки актив, съществува ли ясно дефинирана класификация на сигурността и ограничения на достъпа, които подлежат на редовно преразглеждане? Опишете този процес? д) Какви са правилата за приемливо използване на информацията и активите, свързани с техниката за обработване на информация? е) По какъв начин се идентифицират, документират и прилагат тези правила?		Член 23, параграф 2 – не е изрично упоменат, но се счита за добра практика при управлението на	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		ж) Какви системи са въведени за идентифициране на ИТ устройствата за съхранение на данни и по какъв начин се регистрира в системата бракуването на устройства?			
Лица, обработващи данни/ аутсорсинг	B 36	а) Възлагате ли услуги на подизпълнители (аутсорсинг) по отношение на някои ИТ системи и/или мрежова инфраструктура за обработването на данни за свързани с Евродак дейности? б) Има ли официално сключено споразумение за предоставянето на определено ниво на услуги? Какви мерки предприемате за гарантиране на сигурността по отношение на подизпълнителите (напр. проверки за изпълнението на договорени мерки)? в) Споразумението съдържа ли разпоредби относно ИТ инфраструктурата, използвана за обработване на данни от Евродак, и по-конкретно във връзка с мерки за защита на интегритета, наличността и сигурността на тази инфраструктура?		Член 23, параграф 2 – не е изрично упоменат, но е необходим за сигурността на лицата, обработващи данни.	
Самостоятелни (вътрешни) одити	B 37	Как следите ефективността на мерките за сигурност във връзка с данните от Евродак и какви са организационните мерки за вътрешен мониторинг (вътрешни одити)?		Член 34, параграф 2, буква „к“	
	B 38	Моля, опишете въведените процедури за вътрешни одити на ИТ сигурността. Каква е честотата на тези одити?			

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
Раздел 3: Информация и права на субектите на данни					
Информация	B 39	а) По какъв начин субектите на данни се информират относно събирането на данни за тях? Моля, приложете декларации за защита на личните данни или други информационни материали за обществеността, ако такива съществуват. б) По-конкретно, моля, опишете дали и по какъв начин субектите на данни се информират относно използването на техните данни за целите на правоприлагането. в) Разяснете процедурите за предоставяне на информация относно обработването на субектите на данни (срокове и вид информация). Документират ли се тези процедури? Ако да, моля, приложете копие. г) Как оценявате средствата, използвани за информиране на субектите относно техните права? (напр. брошури за системата Евродак).		Член 29, параграфи 1—3	
Права на субекта на данни	B 40	а) Моля, опишете въведените процедури за предоставяне на право на достъп до данните (напр. формални изисквания, срокове за отговор, такси, евентуални изключения). Колко искания годишно получавате? б) Моля, опишете общите процедури за предоставяне на правото на коригиране на данни съгласно член 29, параграф 5 на Регламент Евродак, като предоставите налични статистически данни (относими към конкретни искания от субекти на данни). в) Процедурите документират ли се? Ако да, приложете копие. г) Как компетентните органи си сътрудничат активно за спазване на		Член 29, параграфи 4—15	

	№	Въпрос	Коментари	Правно изискване (съгласно Регламент Евродак)	Събрани доказателства
		правата по член 29, параграф 10 от Регламент Евродак? В случай на отказ на искане за достъп/информация/поправка/заличаване на данни, пред кого субектът на данни може да обжалва този отказ? д) Има ли (понастоящем или в миналото) съдебни дела (жалби) пред националните съдилища относно откази за предоставянето на права на поправка или заличаване на незаконно въведени в системата данни? (Ако да, опишете естеството на делата/жалбите и посочете броя на съдебните дела по години)			

Текуща правна рамка Регламент (ЕС) на Съвета № 603/2013)

Член 34

Сигурност на данните

1. Държавата членка по произход осигурява сигурността на данните преди и по време на предаването им на централната система.

2. Всяка държава членка приема във връзка с всички обработени данни от нейните компетентни органи, съгласно настоящия регламент, необходимите мерки, включително план за сигурността, с цел:

а) физическа защита на данните, включително чрез изготвяне на планове за действие в извънредни ситуации за защита на критичната инфраструктура;

б) предотвратяване на достъпа на неоправомощени лица до националните съоръжения, в които държавата членка извършва операции съобразно целите на Евродак (проверки на входа на съоръжението);

в) предотвратяване на неоторизираното прочитане, копиране, променяне или изнасяне на носители на данни (контрол на носителите на данни);

г) предотвратяване на неоторизираното въвеждане на данни и неоторизираната проверка, променяне или заличаване на съхраняваните лични данни (контрол на съхраняването);

д) предотвратяване на неоторизираното обработване на данни в Евродак и на всяка неоторизирана промяна или заличаване на обработените в Евродак данни (контрол на въвеждането на данни);

е) гарантиране на това, че лицата, имащи право на достъп до Евродак, имат достъп само до данните, до които им е разрешен достъп, посредством индивидуални и уникални потребителски имена и единствено режими на поверителен достъп (контрол на достъпа до данни);

ж) гарантиране на това, че всички органи с право на достъп до Евродак създават профили с описание на функциите и задълженията на лицата, на които е разрешен достъп и които имат право да въвеждат, актуализират, заличават данни и да търсят в тях, както и че при поискване от националните надзорни органи, посочени в член 28 от Директива 95/46/ЕО и в член 25 от Рамково решение 2008/977/ПВР, незабавно им предоставят тези профили (профили на служителите), както и всяка друга относима информация, която органите биха

могли да поискат за целите на надзора;

з) гарантиране на възможност да се провери и установи на кои органи могат да се предават лични данни чрез използване на комуникационно оборудване (контрол на комуникацията);

и) гарантиране на възможност да се провери и установи кои данни са били обработени в Евродак, от кого и с каква цел (контрол на регистрирането на данните);

й) предотвратяване на неоторизираното четене, копиране, променяне или заличаване на лични данни по време на предаването на лични данни на или от Евродак или по време на превоза на носителите на данни, по-специално чрез подходящи техники на криптиране (контрол на транспортирането);

к) контролиране на ефективността на мерките за сигурност по настоящия параграф и предприемане на необходимите организационни мерки, свързани с вътрешния контрол, за да се гарантира спазване на настоящия регламент (собствен одит) и за да се установява автоматично в срок от 24 часа всяко относимо събитие, произтичащо от прилагането на мерките, изброени в букви б) – й), което може да показва възникването на инцидент, свързан със сигурността.

3. Държавите членки уведомяват Агенцията за инциденти, свързани със сигурността, които са установили в своите системи. Агенцията уведомява държавите членки, Европол и Европейския надзорен орган по защита на данните в случай на инциденти, свързани със сигурността. Съответните държави членки, Агенцията и Европол си сътрудничат по време на инцидент, свързан със сигурността.

4. Агенцията взема необходимите мерки за постигане на целите, посочени в параграф 2, във връзка с функционирането на Евродак, включително приемане на план за сигурност.