

ДОКЛАД

Общ контролен орган за Шенген

Доклад за дейността: декември 2005 г. — декември 2008 г.

СЪДЪРЖАНИЕ

Предговор.....	3
1. Въведение.....	5
2. Нови моменти: ШИС II.....	7
2.1. Миграция от ШИС I+ към ШИС II.....	9
2.2. Разширяване на Шенгенското пространство	10
3. Работа по контрола	14
3.1 Проверки по член 99	14
3.2 Общ преглед на член 111	16
3.3 Мерки, следващи проверката по член 96	20
4. Становища на Общия контролен орган	24
4.1 Тълкуване на член 111 от Шенгенската конвенция.....	24
4.2 Становища относно прилагането на член 102A (SCHAC 2501/07)/ SCHAC 2504/08.....	28
4.3 Становище относно внедряването на сървър за предаване на електронни съобщения за целите на SIRENE, разположен централно в сградата на Ц.ШИС (SCHAC 2502/07).....	30
4.4 Становище относно проекта за мерки за прилагане, включително наръчник SIRENE за Шенгенската информационна система от второ поколение (SCHAC 2503/07).....	32
4.5 Становище относно принципите, ръководещи сътрудничеството между националните контролни органи на основата на Шенгенската конвенция	34
4.6 Становище относно Шенгенската информационна система и извършителите на противообществени прояви 08/10.....	36
5. Права на субектите на данни.....	40
6. Съвместен надзор в бъдеще.....	42
7. Членове на Общия контролен орган за Шенген	45
8. Наблюдатели в Общия контролен орган за Шенген.....	47

Предговор

Шенгенското пространство може да се счита за значително постижение при създаването на отворено пространство без граници в Европа. Всички лица в това пространство са пряко засегнати от въпросите, свързани с тяхната сигурност и със зачитането на техния личен живот и права, включително правото на защита на техните лични данни.

Всички национални органи за защита на данните, работещи съвместно в Общия контролен орган за Шенген, показаха своята решимост да защитават неприкосновеността на личния живот на физическите лица по отношение на огромното количество лични данни, обработвани от Шенгенската информационна система.

През този тригодишен период (декември 2005 г. — декември 2008 г.) съсредоточихме усилията си върху правилното тълкуване на Шенгенската конвенция и направихме оценка дали Шенгенските държави са въвели прилагане на въпросната правна рамка по хармонизиран и подходящ начин.

С общата цел да предоставят на лицата висока степен на сигурност чрез специфичен граничен и друг вид контрол в Шенгенското пространство, Шенгенските държави разработиха също така разнообразни нови политики в областта на контрола на имиграцията и борбата срещу тежките престъпления. Това ново развитие доведе до подобряване на сътрудничеството между националните органи за защита на данните и до създаване на бази за сравнение на добрите практики. Общият контролен орган за Шенген изрази загрижеността си относно някои аспекти на това ново развитие.

Сега сме изправени пред две значителни предизвикателства: разширяването на Шенгенското пространство, което засилва необходимостта от по-добра хармонизация между всички Шенгенски държави, и развитието на Шенгенската информационна система от второ поколение (ШИС II), включително сложната миграция от сега действащата към новата система.

Настоящият доклад изтъква също работата, извършена от всички национални органи за защита на данните, както и съществения принос на секретариата за насърчаване на хармонизацията и по-доброто взаимно разбирателство.

Най-голямото предизвикателство за нас остава отговорът на всяко ново развитие чрез борбата срещу престъпленията и незаконната имиграция, утвърждаването на европейското пространство на правосъдие, повишаването на равнището на сигурност за всички лица чрез разкриване на опасностите от тероризъм и тежки престъпления и осигуряването на добър баланс между сигурността и неприкосновеността на личния живот.

Председател

George de La LOYERE

1. ВЪВЕДЕНИЕ

Гражданите на Европейския съюз имат право да пътуват свободно от една страна в друга. Въпреки че това право води началото си от създаването на ЕС, премахването на вътрешните граници на ЕС със Споразумението от Шенген го превръща в реалност и дава по-голяма свобода на движение като привилегия за гражданите на ЕС. Очевидна е необходимостта да се намери адекватен заместител на тези граници, с което да се гарантира, че ЕС ще продължи да бъде пространство на свобода, сигурност и справедливост. Премахването на една защита води до създаване на друга — Шенгенската информационна система, чрез която се обработват личните данни на физическите лица с оглед поддържане на обществения ред и сигурност, включително националната сигурност, на териториите на шенгенските държави и се прилагат разпоредбите на конвенцията, отнасящи се до движението на хора на тези територии, като се използва информацията, предавана чрез тази система. Основателно би било да се каже, че Шенгенската информационна система е предшественик на всички настоящи и бъдещи мащабни информационни системи на ЕС, с които се създава мрежа за надзор на данни в ЕС. Най-скорошният пример, а именно системите, въведени с Договора от Прюм, отразяват до голяма степен концепцията и функциите на Шенгенската информационна система, въпреки че по принцип техен обект са гражданите на ЕС. Наскоро бяха предприети редица мерки за улесняване на обмена на информация, без да се извърши необходимата оценка на съществуващите системи и на евентуалните последици за защитата на правата на физическите лица — не само на правото на неприкосновеност на личния живот и правото на защита на данните, но и на свободата на движение на тези лица и принципа на недискриминация.

С Шенгенската конвенция бе създаден Общият контролен орган, независим орган, чиято задача е да осъществява контрол върху централната секция на Шенгенската информационна система, да разглежда трудностите при прилагането и тълкуването относно експлоатацията на системата и да гарантира, че системата спазва съответните разпоредби за защита на данните.

В настоящия — осми подред — доклад за дейността на Общия контролен орган, се прави обзор на ангажираността и участието на Общия контролен орган в разработката на Шенгенската информационна система от второ поколение (ШИС II), на ролята му в процеса на разширяването и инициативите му за съвместни действия с националните органи за защита на данните по въпросите на съответствието на личните данни, въведени в ШИС като сигнали по член 99 от Шенгенската конвенция, в т.ч. на отчета за общия преглед на прилагането на член 111 от Шенгенската конвенция.

В доклада са отразени също така дейностите на Общия контролен орган в отговор на жалби, подадени от физически лица, становищата на органа по различни въпроси от областта на защитата на данни и бъдещите перспективи за съвместен контрол на ШИС.

2. НОВИ МОМЕНТИ: ШИС II

Общият контролен орган, който е тясно ангажиран с наблюдението на разработката на Шенгенската информационна система от второ поколение (ШИС II), даде насоки и оказва помощ на институциите на ЕС, които имат за цел да гарантират, че ШИС II отговаря на необходимите стандарти за защита на данните. През септември 2006 г. Общият контролен орган даде становище относно предлаганото правно основание за ШИС II.

Приносът на Общия контролен орган за разработката на ШИС II датира от 2004 г. В становището си от 19 май 2004 г. относно бъдещата разработка на ШИС II Общият контролен орган посочи някои основни въпроси, предизвикващи загриженост, и действията, които следва да се предприемат. През октомври 2005 г. Общият контролен орган даде становище по предлаганото правно основание за ШИС II, на базата на проект за регламент¹ и проект за решение², в което той прави систематична оценка на новата архитектура на системата спрямо съществуващата рамка и предлаганата нова рамка за защита на данните. Общият контролен орган направи много подробни забележки и предложения за подобряване на проектите за правни текстове. Оттогава новите предложения за правното основание на ШИС II се обсъждат непрекъснато в Съвета и Европейския парламент, като това води до много изменения на първоначалните предложения. Общият контролен орган разгледа някои важни въпроси във връзка с преразглежданите предложения на финландското председателство³ от 27 юли 2006 г. относно създаването, функционирането и използването на ШИС II. По този начин той допринесе за усъвършенстване на правното основание от гледна точка на защитата на данни. В становището си Общият контролен орган приветства ограничаването на ролята на ШИС II до компенсаторната ѝ роля, тъй като това изглеждаше важна стъпка към едно стесняване на целта на ШИС II, застъпвано от Общия контролен орган. В становището се подчертава, че предвижданите технически изисквания, които предстои да се разработят за ШИС II, с оглед на въздействието им върху физическите лица не трябва по никакъв начин да понижават нивото на защита на данните.

Контролният орган подчерта силното си желание за участие по време на преходния период, по-специално предвид създаването на администратор на базата данни. Общият контролен орган изрази известна загриженост по повод използването на биометрични данни в ШИС II и приветства някои ограничения във връзка с употребата на такива данни, като посочи, че биометричните данни биха могли да се разглеждат единствено като допълнително средство

¹ COM (2005) 236, 2005/0106 (COD).

² COM (2005) 230, 2005/0103 (CNS).

³ 5709/9/06 и 5710/5/06.

за проверка на самоличността на съответното лице, ако изискванията за техническо качество, които предстои да се разработят, са адекватни и съдържат необходимите гаранции.

Безусловното използване на биометрични данни с цел идентификация несъмнено би довело до използване на тази функционална възможност от все по-голям брой органи за различни цели. Такова „изместване на функцията“ — като се вземе също така предвид желанието за функционална съвместимост между ШИС II, ВИС и Евродак — следва да бъде предотвратено. В становището си Общият контролен орган предлага да се добави в предложенията разпоредба, според която използването на биометрични данни за идентифициране на физическо лице е строго ограничено до целите на сигналите. Общият контролен орган стига до заключението, че биометричните данни (дактилоскопните отпечатьци), обработвани в ШИС II, следва да се използват единствено за проверка на самоличността на засегнатите лица — да се ограничават до целите на сигналите и да не се използват за други търсения за идентифициране. Техническите средства, които се използват за сравняване на „един с много“, поради самата природа на дактилоскопните отпечатьци, следва не само да отговарят на най-високите стандарти, но и да включват средства за правна защита на физическите лица. Използването на посоченото сравняване следва освен това да бъде не само възможност, избрана единствено по технически причини, но и да изисква оценка на потребността и пропорционалността, като се имат предвид последиците, които би имало то за правата на физическите лица. Общият контролен орган изтъква, че механизмите трябва да осигуряват точна и правомерна обработка на данните, за да се гарантират правата на гражданите. Общият контролен орган също така предлага текстовете на предложенията да бъдат изменени по такъв начин, че случаите на спорове между държавите-членки да подлежат на съответстващ координиран контрол от страна на ШИС II.

Още преди да започнат дискусиите по ШИС II, се оказа, че е налице силно желание да се даде достъп на Европол и Евроюст до някои специфични сигнали, които биха им били от полза при изпълнение на задълженията им. Във всичките си становища Общият контролен орган предупреждава, че такъв достъп не следва да доведе до рутинен достъп от страна на тези организации. Сигналите, до които те имат право на достъп, не съдържат непременно информация, свързана с целите на Европол и Евроюст.

Приети бяха Регламент (ЕО) № 1987/2006, Решение № 2007/533/ПВР на Съвета относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) и Регламент (ЕО) № 1986/2006 относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II), които послужиха за правно основание за дейностите на ШИС II, както и за

установяване на правилата за защита на данните и за режима за надзор на защитата на данните.

2.1 Миграция от ШИС I+ към ШИС II

С увеличаване на броя на държавите-членки на Европейския съюз след разширяването на Съюза стана ясно, че ШИС трябва да се разработи така, че да обхване над два пъти повече държави-членки от обхванатите от сегашната ШИС. Същевременно въпросът за миграцията на данни от ШИС I+ към ШИС II и подготвителната работа привлякоха вниманието на Общия контролен орган. На този етап беше от значение по време на преминаването на данните от едната система към другата да се осигури спазване на важните принципи на защитата на данни (цялост на данните, поверителност на данните, цел).

На 19 април 2006 г. Общият контролен орган получи искане от председателя на Комитет „Член 36“ да направи преглед на предлаганите правила за създаване на тестова база данни на ШИС I+ с оглед подготовка на преминаването от ШИС I+ към ШИС II.

Въпреки че напълно подкрепяше създаването на тестова база данни за ШИС II, Общият контролен орган отбеляза в Становище 06—05, че полетата за данни в предложението биха могли по случайност да възпроизведат данни на реални лица и че по тази причина следва да се приложат допълнителни мерки за сигурност. В становището си Общият контролен орган също така изтъква, че използването на лични данни като тестови данни по време на разработката на информационните системи води до ред рискове. При създаване на тестови данни за информационни системи като ШИС II бе прието, че създаването на такива тестови данни следва да се ръководи от разбиране за миграцията на данни, което зачита неприкосновеността на личния живот — разработка на точни модели без достъп до точна информация в отделните записи на данни, като по този начин се намира решение на стълкновение между неприкосновеността на личния живот и миграцията на данни. Методите за осигуряване на анонимност на данните следва да дадат възможност за използване на масиви от данни без разкриване на самоличност. Контролният орган отбеляза, че миграцията на данни, при която се зачита неприкосновеността на личния живот, следва да почива на разбирането, че преди съобщаването им личните данни могат да бъдат предпазени, като бъдат криптирани и рандомизирани. Чрез прилагане на специфичен метод могат да се генерират много точни модели на данни, без да се разкрива лична информация. Общият контролен орган отбеляза, че когато бе представено предложението, бе отчетено, че съществува възможност при генерирането на тестови данни да бъдат разкрити действителни данни. Доколкото предложението беше да се оставят непроменени полетата на имената (собствено и фамилно име), като се извършат единствено взаимни замени между сходни записи на данни, съществуваше значителен риск от разкриване на самоличността на отделни лица. Отчетено бе,

че предвид този риск в предложението са включени допълнителни процедурни мерки за ограничаване на използването на тестовата база данни.

Тези мерки обаче въобще не биха могли да предотвратят разкриване на данни пред трети лица. Общият контролен орган изрази подкрепа за допълнителните мерки като обща допълнителна защита, но изтъкна, че те не биха могли да заменят необходимостта от осигуряване на анонимност на тестовите данни. Той даде също така редица препоръки за разработване на специални политики за сигурност, за избягване на използването на чувствителни данни в тестова среда, за методологията за осигуряване на анонимност на данните, за протоколиране на достъпа до тестови данни, за предоставяне на одитни пътеки дори и за Общия контролен орган, както и за ограничения във времето за използване на тестовата база данни.

През април 2008 г. Комисията представи две предложения за регламент на Съвета и за решение на Съвета относно миграция от Шенгенската информационна система (ШИС I+) към Шенгенска информационна система от второ поколение (ШИС II), за да бъде създадена правна рамка, която да урежда миграцията от ШИС I+ към ШИС II. На 30 юни 2008 г. Комисията на Европейския парламент по граждански свободи, правосъдие и вътрешни работи организира Кръгла маса по въпросите на свободата и сигурността в интегрираното управление на границите на ЕС, в рамките на която бе проведена сесия „ШИС II: Кога? Защо? Как?“. Председателят на Общия контролен орган за Шенген присъстваше на това събитие и взе участие в дискусиите относно последствията за защитата на данни от миграцията от ШИС I към ШИС II. През октомври 2008 г. Съветът прие Решение на Съвета и Регламент на Съвета относно миграция от Шенгенската информационна система (ШИС I+) към второ поколение Шенгенска информационна система (ШИС II).

2.2 Разширяване на Шенгенското пространство

Едно от важните събития през периода 2005—2008 г., което заслужава да бъде специално посочено, беше разширяването на Шенгенското пространство, което позволи на девет нови държави-членки да се присъединят към Шенгенското пространство и на гражданите им да се ползват изцяло от свободата да пресичат вътрешните граници, без да трябва да представят паспорти или лични карти, освен ако пътуват за Обединеното кралство, Ирландия и Кипър, както и за България и Румъния, които се присъединиха едва през 2007 г. Дългият процес на посещения и повторни посещения за оценка по линия на Шенген продължи две години. Оценката се състоеше по-специално от проверки дали съпътстващите мерки, даващи възможност за премахване на граничния контрол по вътрешните граници, се прилагат

правилно и ефикасно от страна на новите държави-членки. Посещения за оценка бяха извършени в областта на външния граничен контрол, визите, защитата на данни, полицейското сътрудничество и Шенгенската информационна система.

Разработването на ШИС II бе свързано със създаване и осъществяване на нови функционални възможности в рамките на системата (засилване на сигурността и по-ефикасно използване на данните), както и с осигуряване на техническа възможност системата да обслужва над 18 държави. Забавянето на пускането в действие на новата система и необходимостта нови държави-членки да се присъединят към нея възможно най-скоро принуди държавите-членки да търсят бързо алтернативно решение. През декември 2006 г. Съветът взе решение за изпълнение на предложението на Португалия „ШИС — един за ВСИЧКИ“ (SISone4ALL) за временна интеграция в ШИС 1+ на девет от държавите-членки, присъединили се към Европейския съюз през май 2004 г. Целта на проекта „ШИС — един за ВСИЧКИ“ беше да се улесни процесът, водещ до премахване на контрола по вътрешните граници с въпросните държави-членки между декември 2007 г. и март 2008 г. Съгласно Решение 2007/471/ЕО на Съвета от 12 юни 2007 г., държавите-членки можеха да въвеждат данни в ШИС и да използват данни от ШИС от 1 септември 2007 г. нататък.

На 21 декември 2007 г. Естония, Чешката република, Литва, Унгария, Латвия, Малта, Полша, Словакия и Словения станаха част от Шенгенското пространство. На 30 март 2008 г. процесът на разширяване бе приключен с премахването на контрола по границите между тези страни и между тях и 15-те страни, които бяха вече част от Шенгенската система.

Още преди разширяването ШИС представляваше една от най-значителните и големи бази данни, използвани за контрол на имиграцията и границите в ЕС. На 1 януари 2007 г. общият брой на валидните записи в ШИС беше 17 615 945.

След като девет нови държави се присъединиха към Шенгенското пространство и започнаха да работят с ШИС на 1 януари 2008 г., броят на валидните записи в ШИС нарасна на 22 933 370. Като цяло броят на валидните записи в базата данни нарасна с 23 % по време на този период. Като се сравнят статистиките от 1 януари 2008 г. с тези от 2007 г.¹, се вижда, че най-голямото нарастване на записи, съдържащи лични данни, е при ID (издадените документи), при които броят се повиши от 13 752 947 на 17 876 227 (23%). Статистиката е както следва (по членове от Шенгенската конвенция):

¹ 5441/08, 30 януари 2008 г.; 6178/07, 13 февруари 2007 г.

Член 95 (издирва се с цел арест/екстрадиция)	+ 16%
Член 96 (нежелан чужденец)	- 7,4%
Член 97 (безследно изчезнало пълнолетно лице)	+ 14%
Член 97 (безследно изчезнало непълнолетно лице)	+ 6,8%
Член 98 (установяване на местопребиваване или местожителство)	+ 22%
Член 99, параграф 2 (контрол/наблюдение)	- 5%
Член 99, параграф 3 (контрол/наблюдение)	- 22%

Намаляването на броя на сигналите за нежелани чужденци може да се обясни просто с факта, че с присъединяването на новите държавите-членки към ЕС, гражданите на тези държави станаха граждани на ЕС, поради което записите за тези лица следва да са заличени от системата. Предвид горното, инициативата на Общия контролен орган за по-нататъшна проверка по член 96 бе навременна, а резултатите — удовлетворителни. В получените отговори не се съдържа информация за случаи на обработка на данни на граждани на ЕС по член 96. Поради неголемия брой на получените отговори, обаче, очевидно е необходимо този вид работа да се извърши във всички шенгенски държави.

Разширяването означаваше също така увеличаване на броя на членовете на Общия контролен орган. Тези нови членове вече участваха в качеството си на наблюдатели в работата на Общия контролен орган и по този начин бяха натрупали значителни познания като подготовка за новите си задачи и задължения. С предоставянето на този статут на наблюдатели, Общият контролен орган изигра важна роля за повишаване на осведомеността и познанията на бъдещите членове, като даваше становища и консултации по въпроси, зададени от наблюдателите относно различни тълкувания на разпоредбите на Шенгенската конвенция.

Същевременно опитът на новите членове, придобит в дългия процес на подготовка и оценка (участие в подготвителната работа за национално законодателство по ШИС, предварителни одити на системите за информационни технологии, консултации с компетентните институции, информационни кампании за правата на физическите лица в

ШИС, работата по надзора в консулските представителства, полицейските органи и т.н.) беше от голямо значение и за така наречените „стари членове“ на Общия контролен орган.

Всичко това има голяма стойност за съвместната координирана работа в подкрепа на ефективната защита на правата и свободите на физическите лица и бъдещия контрол на ШИС II.

3. Работа по контрола

Член 115, параграф 3 от Шенгенската конвенция постановява, че Общият контролен орган има компетентност и относно анализа на трудностите, които могат да възникнат при прилагането или тълкуването относно експлоатацията на Шенгенската информационна система, както и за разглеждане на проблеми, които могат да възникват при изпълнение на независимия контрол на националните части на договарящите страни или при упражняване правото на достъп до системата и изготвяне на хармонизирани предложения за намиране на общи решения на съществуващите проблеми. За да приложи на практика тази разпоредба на конвенцията, Общият контролен орган реши да извърши проверки на национално равнище. Очевидната практическа полза от такива дейности бе навлизането и запознаването с начините, по които шенгенските държави изпълняват и използват членовете на Шенгенската конвенция, както и придобиването на общ поглед върху практическите проблеми, които могат да възникнат при прилагането им.

3.1 Проверки по член 99

Една от основните характеристики на Шенгенската информационна система е съвместната отговорност за използването на системата в съответствие с разпоредбите на Шенгенската конвенция и националните закони. Има основания да се твърди, че Общият контролен орган за Шенген е първият контролен орган, който насърчава съвместни координирани надзорни дейности в областта на прилагането на законодателството при инспектиране на мащабни бази данни. Този нов подход към надзорната роля имаше голям успех и даде идеи за бъдещ координиран контрол. Системата на общи прегледи подпомогна значително хармонизацията на прилагането на Шенгенската конвенция и използването на ШИС.

През юни 2006 г. Общият контролен орган отправи искане към националните органи за защита на данните да направят проверки на сигналите по член 99, въведени в Шенгенската информационна система (ШИС) от техните компетентни органи.

Това бе вторият общ преглед, проведен от Общия контролен орган, на прилагането на специфичен член от Шенгенската конвенция (*напр. на член 96 през 2005 г.*). Често резултатите сочеха различия от всякакъв характер между шенгенските държави, което даде възможност на Общия контролен орган да направи изводи и да препоръча необходимите мерки.

Целта на проверката беше да се гарантира, че данните по член 99 се обработват в съответствие с член 99, както и със залегналите в Шенгенската конвенция принципи на защита на данните, с наръчника SIRENE и с приложимото национално законодателство. Методът за проверка даде възможност на Общия контролен орган да направи преценка дали съществуват проблеми при тълкуването на член 99.

За целта Общият контролен орган разработи един несложен метод за проверка, който да се използва и от всички национални органи за защита на данните. Изготвен бе изчерпателен въпросник. Този въпросник имаше за цел да даде общ поглед върху съответното национално право в шенгенските държави и да провери дали са налице всички необходими процедури за изпълнение на изискванията за защита на данните от страна на отговорните органи. В него се съдържаха също така специфични въпроси, имащи за цел да се провери дали сигналите отговарят на разпоредбите на член 99 и дали се съхраняват в ШИС съобразно разпоредбите на Шенгенската конвенция.

Съвместните усилия на националните органи за защита на данните за проверяване на националните записи по член 99 в ШИС за определен период и с използване на един и същ модел за проверка още веднъж подчертаха общия стремеж за правилно използване на ШИС. Това второ съвместно действие беше следващият знаменателен етап в сътрудничеството между отговарящите за защита на данните национални власти в Европейския съюз, който подчерта необходимостта от полагане на усилия за създаване на рамка за проверка на защитата на данните в онези области, в които сътрудничеството между шенгенските държави води до обработка на лични данни. Същевременно тази проверка помогна на националните органи за защита на данните да установят как тяхната страна използва сигналите по член 99, което несъмнено ще има положителен ефект за бъдещите действия на тези органи.

Въз основа на констатациите от проверката по член 99 Общият контролен орган прие редица препоръки. Главните препоръки са както следва:

- органите, отговарящи за сигналите по член 99, следва да разработят официални писмени структурирани процедури, за да се гарантира точността, актуалността и законността на данните по член 99;
- съществува необходимост от ясна дефиниция на видовете престъпления, които биха могли да водят до сигнал по член 99. Въпреки че в новото правно основание за ШИС II се съдържа понятието „тежки криминални престъпления“, бе изказано

мнението, че следва да се постигне съгласие на европейско равнище за еднакво тълкуване на понятието „тежко престъпление“. За целта може да се използва списъкът на тежките престъпления, по които е компетентен Европол, или Рамковото решение на Съвета относно европейската заповед за арест;

- съответните национални органи, отговарящи за сигналите по член 99, следва да упражняват контрол и да правят проверки на тези сигнали веднъж на шест месеца. Следва да се изготвят допълнителни насоки;
- списъкът на органите (включително службите за национална сигурност), имащи достъп до сигналите по член 99, следва да се хармонизира във всички държави-членки на ЕС;
- там, където различни органи носят отговорност за качеството и целостта на данните, следва да се осигури такава организация и връзка между различните отговорности, че да се поддържа точността, актуалността и законосъобразността на данните и да се гарантира контролът над тях;
- сигнал, отнасящ се до лицата за контакт, не е допустим предвид формулировката на член 99, параграф 2;
- националните органи за защита на данните следва да правят периодична проверка на сигналите по член 99.

3.2 Общ преглед на член 111

Пред октомври 2006 г. Общият контролен орган отправи искане към националните органи за защита на данните да представят информация за прилагането и използването на член 111 от Шенгенската конвенция. Това беше третият общ преглед на използването на конкретен член от Шенгенската конвенция (*напр. член 96 през 2005 г., член 99, който понастоящем е подложен на оценка*). Необходимостта от такъв общ преглед бе констатирана по време на разглеждането на конкретен случай, отнасящ се до практическите последици на член 111, който бе представен на вниманието на Общия контролен орган.

Шенгенската конвенция урежда както правилата за обработка на личните данни, така и правата на лицата, чиито лични данни се обработват. Член 109 от Шенгенската конвенция постановява, че правото на достъп до въведени в системата данни следва да се упражнява в съответствие със законодателството на договарящата страна по Шенгенската конвенция, в която е изразена претенцията за това. Необходимо е да се отбележи, че според тази разпоредба, в националното законодателство може да се конкретизира дали националният

контролен орган, предвиден в член 114, параграф 1 от Конвенцията, следва да вземе решение дали информацията да бъде съобщена на засегнатото лице и по какви процедури. Член 109 също урежда положението, при което физическо лице възнамерява да упражни право на достъп в държава, член на Шенгенската конвенция, която не е въвела сигнала. В такъв случай шенгенската държава, която не е въвела сигнала, може да съобщи данните само ако преди това е дала на шенгенската държава, въвела сигнала, възможност да изложи позицията си. Съгласно член 114, параграф 2 всяко лице има право да поиска от контролните органи посочени в член 114, параграф 1 от Шенгенската конвенция, да извършат проверка на данните, които се отнасят за него и са включени в Шенгенската информационна система, както и да получи информация относно тяхното използване. Както вече бе посочено, това право се урежда от националното законодателство на шенгенската държава, към която е отправено искането. Когато данните са въведени от друга шенгенска държава, проверката се извършва в тясно сътрудничество с контролния орган на тази държава.

Съгласно член 109, параграф 2 от Шенгенската конвенция, правото на достъп не е абсолютно право и, следователно, на лице, искащо достъп до свои данни, съхранявани в Шенгенската информационна система, следва да се откаже предаване на информация, когато това е необходимо за изпълнението на законно задължение във връзка със сигнала или за защита на права и свободи на трети лица. Освен това, съгласно член 109, параграф 2 се забранява съобщаването на каквито и да е данни, които са въведени в системата за целите на скрито наблюдение, извършвано на основание член 99 от Конвенцията.

С член 106, параграф 1 се въвежда „принципът на собственост“ в Шенгенската информационна система. Въпреки че във всички шенгенски държави се обработват лични данни, свързани със сигнали, това не означава, че дадена шенгенска държава може да изменя данни, въведени в системата от друга държава. Независимо от приложимостта на националното законодателство на обработващата държава, специалната разпоредба на Конвенцията позволява единствено на държавата, подала сигнала, да изменя или заличава данни.

Член 111 дава допълнителни гаранции за правата на лицата. Съгласно член 111, параграф 1 всяко лице може на територията на всяка договаряща страна по Шенгенската конвенция да заведе иск пред съдилищата или пред органа, компетентен по националното законодателство за поправка, заличаване или получаване на информация, или за обезщетение във връзка със сигнал, който се отнася до това лице. Съгласно параграф 2 от същия член, договарящите страни по Шенгенската конвенция следва взаимно да изпълняват окончателните решения, постановени от съдилищата или от органите, посочени в параграф 1.

В съответствие с „принципа на собственост“ и задължението да се изпълняват посочените в член 111, параграф 2 окончателни решения, тези окончателни решения се изпълняват от шенгенската държава, въвела сигнала.

Освен това, договарящите страни по Шенгенската конвенция носят отговорност в съответствие със своето национално законодателство за щетите, причинени на лице, при използване на националната база данни на Шенгенската информационна система. Цитираната разпоредба на член 116 от конвенцията е приложима също така за щетите, причинени от договарящата страна, подала сигнала, ако е въвела фактически неточни данни или е запазвала данни неправомерно.

Общият преглед имаше за цел да провери дали член 111 се прилага последователно във всички шенгенски държави, като защита правата на физическите лица и им осигурява справедливо и равнопоставено отношение.

Прегледът на съдилищата и компетентните органи показва, че в шенгенското пространство редица органи биха били компетентни да постановяват решения по член 111. Само в една държава органът за защита на данните бе компетентен да постанови окончателно решение (Австрия). В други шенгенски държави това става чрез съчетаване на компетентността на националните органи за защита на данните и на съдилищата или на конкретен съд.

Що се отнася до сигнали, въведени от друга шенгенска държава, повечето отговори сочеха, че съществува официална процедура за консултации с подаващата сигнала държава или за официалното им включване в производствата. Това обаче не важи за всички шенгенски държави, или поне не е задължително.

Що се отнася до участието на националните органи за защита на данните в съдебни производства, резултатите показаха, че не всички национални органи за защита на данните участват официално или биват информирани.

Бяха посочени седемнадесет случая, при които е приложим член 111.

Що се отнася до изпълнението на решения, като се изключи Португалия, нямаше данни за наличие на конкретни процедури за проверка дали се изпълняват окончателните решения. Като правило, субектът на данните трябва да провери дали решението е било изпълнено.

Съвместните усилия на националните органи за защита на данните за контрол на националните практики по член 111 от конвенцията, за определен период и с използване на

един и същ модел за проверка, още веднъж подчертаха общия стремеж за правилно използване на ШИС. Третото съвместно действие изтъкна необходимостта от тясно сътрудничество между националните органи за защита на данните в шенгенското пространство и подчерта необходимостта от по-нататъшно инвестиране в сътрудничеството между шенгенските държави, когато това е от особено значение за защитата на правата на лицата.

С член 111 от Шенгенската конвенция се въвежда важна мярка за гарантиране на правото на субекта на поправка, заличаване или получаване на отнасяща се до него информация, въведена в ШИС, като се предвижда възможност за подаване на иск пред съдилищата или пред органа, компетентен по националното законодателство, на всяка шенгенска държава. Общият преглед показва, че тази разпоредба се прилага с известни вариации, дължащи се на националните законодателства.

Важен крайъгълен камък за гарантиране на правата на субектите на данни е прилагането на окончателните решения от подалата сигнала шенгенска държава. Системата за изпълнение на всяко окончателно решение и практическото ѝ прилагане са от голямо значение. Въпреки малкото статистически данни, след анализа на представените случаи и по-специално на случаите, представени на вниманието на Общия контролен орган, налице са достатъчно основателни съмнения за това дали член 111, параграф 2 функционира на практика.

Никоя от участващите шенгенски държави не докладва за наличие на процедура за проследяване на изпълнението на окончателни решения. В повечето случаи компетентните органи не участват в прилагането на окончателните си решения. Това може би се дължи на националните правни рамки, които са различни в отделните шенгенски държави. Факт е обаче, че прилагането на окончателното решение от въвелата сигнала шенгенска държава е оставено на практика на личната инициатива на субекта на данните, което представлява прекалено голяма тежест за този субект.

Като взе предвид констатациите от проверката по член 111, Общият контролен орган направи следните препоръки.

- шенгенските държави следва да направят оценка на националните си процедури, за да проверят дали са налице гаранциите, предвидени в член 111;
- окончателните решения по член 111 трябва да се прилагат по един и същи начин от всички шенгенски държави;

- окончателните решения, постановени от съдилищата по член 111, трябва да бъдат съобщавани на националните органи за защита на данните. Може да се окажат необходими разпоредби на национално равнище за прилагане на посоченото по-горе;
- всички шенгенски държави се нуждаят от национална процедура за проследяване на изпълнението на окончателните решения по член 111. За целта е необходима комуникация между съответните органи за защита на данните. Не отделното лице трябва да отговаря за контрола над изпълнението на свързаните с него решения в друга шенгенската държава;
- националните органи за защита на данните следва да си сътрудничат за целта. Трябва да се актуализират съществуващите принципи на сътрудничество между националните контролни органи.

3.3 Мерки, следващи проверката по член 96

Един от важните аспекти на контролните дейности е периодичното предприемане на по-нататъшни мерки с цел да се осигури практическото приложение на направените препоръки в контролирания орган, така че да се постигне по-добро съответствие.

По инициатива на Общия контролен орган националните органи за защита на данните на всички шенгенски държави направиха проверка на използването на сигналите по член 96 в Шенгенската информационна система за периода 2004—2005 г.

Тъй като сигнал с цел отказ за влизане може да има сериозни последствия за засегнатото лице, а също и предвид установените при проверките проблеми, Общият контролен орган постигна съгласие за по-нататъшна проверка с оглед проследяване на извършеното на национално равнище във връзка с констатациите от доклада и осъществените подобрения.

Последващата проверка показа, че на национално равнище са взети следните мерки в отговор на направените в доклада констатации — като се изключи фактът, че в някои държави-членки не бяха установени никакви проблеми, в други страни бяха взети много успешни последващи мерки. Изготвени бяха вътрешни насоки за разглеждане на случаи и процедури за контрол при обработката на случаи, които трябва да се докладват по член 96 от Шенгенската конвенция, като бе обърнато специално внимание на изпълнението на една от препоръките, направени в доклада по член 96 — *следва да се осъществят или доразвият мерките за предотвратяване на сигнали по член 96, отнасящи се до граждани на държавите-членки на ЕС*. При последващите проверки не бяха установени сигнали за граждани на държави-членки на ЕС. Много положителен резултат в рамките на тази

последваща дейност даде активната кампания за повишаване на осведомеността, предприета от редица държави-членки с цел информиране на лицата за правата им, залегнали в Шенгенската конвенция.

Това за пореден път доказва значението на работата, извършена от Общия контролен орган заедно със националните органи за защита на данните, като демонстрира тяхната ангажираност с ценностите им на пазители на индивидуалните права и свободи.

Бъдещите разпоредби за сигналите, отнасящи се до нежелани граждани на трети държави, предвидени в правната рамка на ШИС II, ще изискват допълнителна индивидуална оценка и отговорност преди въвеждане на сигнал.

Член 24, параграф 1 от Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета за създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II)¹ посочва критериите за въвеждане на сигнал в ШИС II: данните на граждани на трети страни, по отношение на които е бил издаден сигнал с цел отказ за влизане или пребиваване, се въвеждат на основата на национален сигнал след решение, взето от компетентните административни органи или съдилища, в съответствие с правилата на процедурата, предвидена в националното законодателство и което е взето въз основа на *подробна индивидуална оценка*. Това означава, че решението за въвеждане на сигнал не може да бъде въведено автоматично в системата. В решението си от 31 януари 2006 г. (*Комисия на Европейските общности/Кралство Испания*) Европейският съд, като изтъква необходимостта от конкретна оценка за всеки отделен случай, посочва, че *договаряща държава може да издаде сигнал за гражданин на трета държава, съпруг(а) на гражданин на държава-членка едва след като установи, че присъствието на това лице представлява действителна, непосредствена и сериозна заплаха по отношение на основен интерес на обществото (...)*². Съдът посочва, че отказът за издаване на виза трябва да има за основание не просто съществуване на запис в ШИС или предишна присъда. Съдът постанови, че *съществуването на предишно осъждане по наказателно дело може, следователно, да бъде взето предвид единствено доколкото обстоятелствата, довели до тази присъда, свидетелстват за личностно поведение, представляващо непосредствена заплаха спрямо изискванията на обществената политика*³. Това решение на Съда и разпоредбите на правната рамка на ШИС II дават много повече отговорност на националните органи, когато вземат решения, които могат да доведат до отрицателни последици за отделни лица, да спазват международните принципи за защита на данните от самото начало на национално равнище.

¹ ОВ L 381, 28.12.2006 г., стр. 4.

² ОВ С 86, 8.4.2006 г., стр. 3.

³ ОВ С 86, 8.4.2006 г., стр. 3.

Друго важно изменение, установено с член 42 от регламента, е правото на граждани на трети страни, които са обекти на сигнал, издаден в съответствие с регламента, да се уведомяват в съответствие с членове 10 и 11 от Директива 95/46/ЕО. Това представлява значително подобрение спрямо сегашното положение, установено от Шенгенската конвенция.

Същевременно, новите инициативи на ЕС, свързани с обработката на личните данни на граждани от трети държави, предизвикват известна загриженост относно последиците им за правото на неприкосновеност на личния живот на засегнатите лица. Според Европейската комисия, общата политика на Съюза в подкрепа на усилията на държавите-членки следва непрекъснато да се развива и да се засилва, за да може да реагира на новите заплахи, на промените в миграционния натиск и на установените проблеми, като в голяма и същевременно съразмерна степен се използват новите технологии¹. Според Комисията, Съюзът би могъл да обмисли възможността за въвеждане на ефикасно средство за откриване на лицата с просрочен престой, тъй като датите на движенията на граждани на трети държави през външните граници понастоящем не се регистрират. Данните на граждани на трети държави (отказ за влизане) понастоящем се обработват въз основа на сигнали по член 96, въпреки че това става без да се отчита продължителността на просрочения период. Тъй като това изглежда недостатъчно, се предлагат възможности за инструменти, които да се прилагат по отношение на граждани на трети държави, пътуващи до държава-членка, участник в шенгенското сътрудничество, или до асоциирана към това сътрудничество държава, и които биха могли да включват:

- улесняване на преминаването на границите за добросъвестните пътници;
- евентуално въвеждане на регистрация на влизане/излизане; както и
- проучване на възможността за въвеждане на електронна система за разрешение за пътуване.

Въпреки че е все още на предварителен етап, в заключения на Съвета относно разработка на ВИС² бе приветствано проучването за осъществимост, представено от Комисията, като бяха потвърдени изложените в насоките цели за визова информационна система и Комисията бе приканена да продължи подготвителната си работа по разработката на ВИС в сътрудничество с държавите-членки на базата на централизирана архитектура, вземайки предвид възможността за обща техническа платформа с ШИС II, при което данните да се

¹ COM(2008) 69 окончателен, 13.2.2008 г.

² 6535/04, 20 февруари 2004 г.

съхраняват в една система и до тях да имат достъп едни и същи крайни потребители. Това би могло да означава, че ако и двете системи бъдат създадени на обща техническа платформа, ще стане възможно въвеждане на технически мерки/улеснения за оперативна съвместимост между ШИС II и ВИС.

Въпреки че още не е доказано, че тази нова система ще осигури добавена стойност за външните граници на ЕС в сравнение със съществуващите системи на ЕС (ШИС), очевидно е, че този по-мощен, сложен и взаимосвързан модел за обработка на данни ще има сериозно значение за неприкосновеността на личния живот на физическите лица и ще изисква големи усилия от националните органи и органите на ЕС за защита на данните за осигуряване на правилна и ефективна защита на индивидуалните права. Цената на тези инициативи би могла да се опише по следния начин: „Модернизирането на имиграционната политика с цената на нейното дехуманизиране е резултат от асиметрия при разработване на политиката, при която контролът над мигрантите се разширява, без да има съответстващо развитие на правата им.“¹.

¹ Alice Garside (2006), „Политически генезис и правно въздействие на предложенията за ШИС II: каква е цената на защитата на данните и сигурността в ЕС?“, Работен доклад № 30 на Центъра за изследване на миграцията в Университета в Съсекс (Sussex Migration Working Paper no. 30).

4. СТАНОВИЩА НА ОБЩИЯ КОНТРОЛЕН ОРГАН

4.1 Тълкуване на член 111 от Шенгенската конвенция

В съответствие с член 115, параграф 3 от Шенгенската конвенция, през юни 2006 г. Общият контролен орган получи искане от австрийския орган за защита на данните да разгледа трудностите при прилагането на член 111 от Шенгенската конвенция и да изготви предложения във връзка с евентуално съществуващи проблеми. Предвид обстоятелствата, довели до искането, Общият контролен орган разгледа също така въздействието на едновременно протичащи процедури върху прилагането на член 111.

Със създаването на Шенгенската информационна система между държавите, които са страни по конвенцията, се обменят специфични сигнали за физически лица. Конвенцията определя основанията и условията за такива сигнали, както и действията, които следва да се предприемат. Вероятно едно от най-важните постижения на конвенцията е задължението на държавите, които участват в Шенгенската информационна система, да предприемат (преки) действия по сигнал на друга държава.

Взаимодействието между националното законодателство на шенгенските държави и конвенцията е ясно определено в член 104, параграф 2: *„Доколкото в настоящата конвенция не се съдържат особени разпоредби при използването на данни от националната част на Шенгенската информационна система, за включените данни в националната част на Шенгенската информационна система се прилага националното законодателство на съответната договаряща страна.“*

Това показва, че специалните разпоредби в конвенцията са с предимство в случаите, когато отделните национални законодателства съдържат различни разпоредби.

Пример за такава специална разпоредба е т.нар. „принцип на собственост“ в член 106, параграф 1: *„Само регистриращата договаряща страна може да прави изменения, допълнения, корекции или да заличава данни, които е въвела.“*

Въпреки че във всички шенгенски държави се обработват лични данни, свързани със сигналите, това не означава, че обработващата държава може да измени данните, въведени в системата от друга държава. Независимо от прилагането на националното законодателство на обработващата държава, специалната разпоредба на конвенцията позволява единствено на държавата, подала сигнала, да изменя или да заличава данни.

Постигнатата хармонизация със създаването на Шенгенската информационна система включва положението на лицата, които са субекти на данни. Техните права бяха уточнени,

включително като бяха предвидени разпоредби, които не допускат процедурни „препятствия“ пред тези лица при защита на правата им. Фактът, че лицето не може да пътува до Шенгенското пространство, сам по себе си не следва да възпрепятства завеждането на правен иск.

Като отчита тяхното положение, конвенцията не задължава субектите на данни да започнат (съдебно) производство по отношение на сигнала в държавата, която го е подала. Лицата решават дали да започнат такава процедура в някоя от шенгенските държави по свой избор. По този начин шенгенските държави ясно изразяват доверието си в хармонизираното прилагане на приложимите правила за защита на данните.

Правата на субектите на данни са определени в член 109, параграф 1 — право на достъп — и в член 110 — право да се поправят фактически неточни данни или да се заличат неправомерно запаметени данни.

Тези права се упражняват в съответствие със законодателството на шенгенската държава, в която е изразена претенцията за това (член 109, параграф 1). Ако данните са вписани в Шенгенската информационна система от друга шенгенска държава, на тази държава се предоставя възможност да изложи позицията си, преди да бъде взето решение.

Освен това субектът на данни има право да поиска от националните надзорни органи по защита на данните на шенгенската държава да извършат проверка на неговите данни (член 114, параграф 2). Ако тези данни са вписани в Шенгенската информационна система от друга шенгенска държава, националният надзорен орган трябва да координира проверката с националния надзорен орган на шенгенската държава, която отговаря за сигнала.

Субектът на данни има право да заведе иск пред съдилищата или пред органа, компетентен по националното законодателство, за поправка, заличаване или получаване на информация, или за обезщетение във връзка със сигнал, който се отнася до него (член 111, параграф 1).

Член 111, параграф 2 задължава шенгенските държави взаимно да изпълняват окончателните решения, посочени в член 111, параграф 1.

С оглед на системата за гарантиране на правата на субектите на данни в конвенцията, и по-специално съществуването на „принцип на собственост“, е необходим механизъм, който да гарантира, че окончателните решения на съдилищата или органите, посочени в член 111, параграф 1, се изпълняват дори и от други шенгенски държави. Без подобен механизъм

основните права за защита на данните, предоставени на лицето в Шенгенската конвенция, няма да бъдат гарантирани в достатъчна степен.

Едно от условията за влизането в сила на конвенцията е участващата държава да е приела необходимите национални разпоредби, за да постигне ниво на защита на личните данни, поне равно на това, което произтича от принципите, залегнали в Конвенцията на Съвета на Европа от 28 януари 1981 г. за защита на физическите лица при автоматична обработка на лични данни, и в съответствие с Препоръка № R(87) 15 на Комитета на министрите на Съвета на Европа от 17 септември 1987 г., регулираща използването на лични данни в сектора на полицията.

Всички шенгенски държави са предвидили необходимото законодателство за защита на данните, но в начина на прилагане може да се открият известни различия. В някои държави правата на субекта на данни се разглеждат основно в пряк контакт между лицето и органа, отговорен за националната част на Шенгенската информационна система. В други държави националните надзорни органи играят важна роля на посредник между този орган и субекта на данни.

Шенгенската конвенция отчита тези различия в някои от специалните разпоредби относно правата на субектите на данни (напр. член 109). Когато обаче липсва разпоредба за съчетаване на шенгенските и националните норми, се прилага шенгенската разпоредба, предвиждаща специално правило (член 104, параграф 2).

Такъв е случаят, когато посоченият в член 111, параграф 1 иск е заведен пред национален съд или компетентен орган на държава, която не отговаря за сигнала, и когато в същото време този сигнал е предмет и на съдебна процедура в държавата, която отговаря за него. Член 111 не съдържа разпоредба, която да урежда такава ситуация. Като се вземе предвид специалният и основополагащ характер на член 111, е обосновано заключението, че в описаната ситуация с предимство се прилага член 111.

На практика това не следва да създава проблеми, тъй като всички шенгенски държави признават в своите процедури принципа да се изслушват всички замесени страни. На практика посочената в член 111 процедура не следва да доведе до окончателно решение без изслушване на държавата, която отговаря за сигнала. Посоченият в член 111 съд или орган без съмнение ще вземе под внимание наличието на друга съдебна процедура.

Когато не е предоставена такава информация, или ако е предоставена, не е довела до друго решение, специалният характер на член 111 задължава шенгенските държави да изпълнят окончателното решение.

Освен това следва да се отбележи, че ако това решение води до заличаването на шенгенския сигнал, подалата го държава може да избере да въведе национален сигнал в националните си системи. Може да се открие сходство с член 25 от Шенгенската конвенция: ако шенгенска държава издаде разрешение за пребиваване на чужд гражданин, за който е подаден сигнал за целите на отказ за влизане, държавата, която е подала сигнала, оттегля сигнала, но въпреки това може да регистрира този чужд гражданин в националния си списък на сигнали.

Въпреки че член 111 от Шенгенската конвенция не дава ясно определение за „окончателно решение“, някои автори смятат, че „окончателните решения“ не следва да се тълкуват прекалено стеснително. Не следва да се възприема, че се включват единствено решенията на висшите съдилища (административни, граждански или наказателни). Фактът, че член 111 от Конвенцията за прилагане на споразумението от Шенген и член 43 от Регламента относно ШИС II се позовават и на решения на националните органи за защита на данните, означава, че дадено решение следва да се разглежда като окончателно, когато подлежи на изпълнение и никоя от страните не го обжалва.¹

Независимо от евентуални различия в тълкуването на термина „окончателно решение“ поради различия в правните системи и процедури, Общият контролен орган заключи в становището си, че всяко окончателно решение на съд или орган, посочен в член 111, което се отнася до подаден от друга договаряща страна сигнал, следва да се изпълнява от тази друга страна при всички обстоятелства.

Като се отчита решението на Съда на ЕО (*Комисия на Европейските общности/Кралство Испания*)² и се направи аналог между задължението на шенгенските държави да приемат и изпълняват решенията, взети от други шенгенски държави да откажат влизане или виза, и задължението и приемането на окончателните решения на съд или орган да се заличи сигнал в ШИС, на практика се наблюдават случаи на неизпълнение на решения на национални съдилища или органи да се заличат сигнали, което води до отрицателни последици за съответното физическо лице.

¹ Evelien Brouwer, „The Other Side of Moon. The Schengen Information System and Human Rights: A Task for National Courts“, Работен документ № 288 на Центъра за европейски политически изследвания от април 2008 г.

² ОВ С 86, 8.4.2006 г., стр. 3.

4.2 Становища относно прилагането на член 102A SCHAC 2501/07)/ SCHAC 2504/08

В съответствие с член 102A, параграф 4, Съветът трябва да представи на Европейския парламент доклад относно прилагането на член 102A от Шенгенската конвенция, и по-специално относно действащите правила за защита на данните, след като поиска становището на Общия контролен орган.

След като председателят на работна група „SIS/SIRENE“ отправи искане на 31 май 2007 г., Общият контролен орган прие становище през юни 2007 г.

Член 102A от Шенгенската конвенция предоставя на службите в държавите-членки, които отговарят за издаването на сертификати за регистрация на превозните средства, право на достъп до специфични данни, вписани в Шенгенската информационна система. Това право се отнася до данни относно моторни превозни средства, ремаркета и каравани, които са откраднати, незаконно присвоени или изгубени, както и до данни относно сертификати за регистрация на превозни средства и табели с номера на превозни средства.

Съгласно Решение 2006/228/ПВР данните относно тези сертификати и табели с номера могат да бъдат обработвани в Шенгенската информационна система, считано от 31 март 2006 г.

Докладът ясно показва, че общото прилагане на член 102A все още не е приключило във всички държави-членки. С оглед на това становището се съсредоточи главно върху някои специфични елементи за защита на данните, свързани с прилагането на този член.

Предвид липсата на ясни и видими резултати през първата година, Общият контролен орган можеше само да заключи, че контролът върху използването на данните относно вещите, предвидени в член 102A, не съответства на член 103, и че Съветът следва да проучи допълнително дали държавите-членки изпълняват задълженията си по член 103 във връзка с член 102A.

Тъй като стриктното прилагане на член 103 е важно не само по отношение на достъпа на службите за регистрация на превозни средства, Общият контролен орган посочи, че следва да се отправи искане към националните органи за защита на данните да докладват за начина, по който член 103 се прилага в техните държави.

В проекта за доклад се съдържаха бележка, че сертификатите за регистрация на превозни средства и табелите с номера не са лични данни. Общият контролен орган подчерта, че тази бележка, както и контекстът, в който е направена, не съответстват на разбирането за лични данни.

Общото определение за лични данни, използвано във всички имащи отношение правни инструменти за защита на данните, описва личните данни като „всяка информация, свързана

с физическо лице с установена или подлежаща на установяване самоличност; лице с подлежаща на установяване самоличност е лице, чиято самоличност може да бъде установена пряко или косвено“.

Общият контролен орган отбеляза, че националните органи за защита на данните разглеждат като цяло сертификатите за регистрация и табелите с номера като лични данни, освен ако обстоятелствата по обработката не предоставят никаква възможност за установяване на самоличността на притежателя на сертификата или табелата с номер.

Освен това Общият контролен орган отбеляза с известна загриженост, че проверките, предвидени в член 102А, вече са били извършвани в някои държави преди прилагането на този член. Единственото заключение, което можеше да бъде направено, е, че тези дейности трябва да се считат за злоупотреба съгласно националното законодателство на тези държави. Това заключение затвърди политиката на Общия контролен орган да насърчава непрекъснато развитието на механизмите за контрол, включително периодични проверки на използването на Шенгенската информационна система.

В заключение и като отчита, че прилагането на член 102А и обработката на сертификати за регистрация и табели с номера на превозни средства все още не е приключило във всички държави-членки, Общият контролен орган изрази своята загриженост във връзка с това прилагане. Тази загриженост се отнася по-специално до очевидната липса на контрол върху използването. Общият контролен орган настойчиво прикани Съвета да гарантира, че държавите-членки изпълняват задълженията си съгласно член 103 във връзка с член 102А.

Общият контролен орган отправи молба това становище да бъде приложено към доклада до Европейския парламент.

На 7 юли 2008 г. Общият контролен орган получи искане от работна група „SIS/SIRENE“ да представи становище относно прилагането на член 102А през 2007 г.

В становището си Общият контролен орган отбеляза, че не е взето под внимание прилагането на Конвенцията за прилагане на споразумението от Шенген в девет нови шенгенски държави, считано от 1 септември 2007 г.

Съгласно приложение I към Решение 2007/471/ЕО на Съвета, разпоредбите на член 64 и членове 92—119 на Шенгенската конвенция, както и Регламент (ЕО) № 1160/2005, са

приложими за новите шенгенски държави, считано от 1 септември 2007 г. Въпреки че тези нови държави реално може да се не прилагали член 102А, докладът не представя информация по този въпрос.

Общият контролен орган изтъкна още веднъж необходимостта да се записва правилно използването на определени данни от службите за регистрация на превозни средства, за да се установи дали дадено превозно средство е откраднато, незаконно присвоено или изгубено. Тъй като докладът представя сходни данни както през 2006 г., Общият контролен орган повтори заключението си от 2006 г., *„че контролът върху използването на данни за вещи, предвидени в член 102А, все още не е в съответствие с член 103“*. Общият контролен орган припомни също така възприетата позиция от националните органи за защита на данните по въпроса дали данните, вписани в ШИС в съответствие с член 102А, се считат за лични данни, както и задълженията на държавите-членки по отношение на правилното прилагане на член 103 във връзка с член 102А.

4.3. Становище относно внедряването на сървър за предаване на електронни съобщения за целите на SIRENE, разположен централно в сградата на Ц.ШИС (SCHAC 2502/07)

Общият контролен орган получи искане от председателя на Комитет „Член 36“ да представи становище относно използването на централизирана архитектура с топология тип „звезда“ за обмен на съобщения по SIRENE и относно предложените принципи на комуникация между страните. В становището си Общият контролен орган съсредоточи вниманието си върху описаните в искането принципи на комуникация, както и върху някои принципи относно достъпа до мрежата.

Във връзка с това Общият контролен орган изтъкна, че функцията за техническа поддръжка на Шенгенската информационна система, както и предложеното използване на пощенски сървър в Ц.ШИС, следва да спазват принципите за защита на данните, установени в Шенгенската конвенция, заедно с принципите в Конвенцията на Съвета на Европа от 28 януари 1981 г. и в Препоръка № R(87) 15 на Комитета на министрите на Съвета на Европа. Предвид това следва да се спазят следните изисквания за качество:

- i) Поверителност: да се гарантира, че достъп до информацията се предоставя само на лицата с разрешен достъп, и
- ii) Наличност: да се гарантира, че при необходимост оправомощените потребители разполагат с достъп до информацията и свързаните с нея средства.

Като описва прилагането на принципа на поверителност при използването на сървър за електронни съобщения в Ц.ШИС и представените в искането процедури, Общият контролен орган отбелязва, че това следва да доведе до следните мерки:

1. Запазените съобщения следва да са в криптиран вид по време на целия период на съхранение.
2. Съобщенията, изпратени от Ц.ШИС до получател, трябва се изтриват веднага след получаване на известие за доставено съобщение.
3. Съобщенията, които не са доставени на получателя (след определен брой опити), следва по принцип да се връщат на подателя, придружени с известие за недоставено съобщение.
4. Искането не посочва кой ключ за криптиране да се използва от бюрата SIRENE за изпращане на съобщенията, ако е активиран резервният сървър в Австрия (поради проблем със сървъра на Ц.ШИС).
 - а) Ако в резервното съоръжение се използва и частният ключ на Ц.ШИС, този ключ е изложен на сериозен риск, тъй като е неотменим принципът, че частният ключ не следва да се разкрива на никой друг, освен на собственика на ключа; или
 - б) Използван е отделен австрийски ключ. В този случай следва да се предвиди официална процедура, която да описва задачите за преодоляване на несъответствията, произтичащи от използването на различни публични ключове за изпращане на съобщения от националните бюра до сървъра. Освен това следва да се опише процедурата по предаване на съобщенията, криптирани с резервния публичен ключ на сървъра, към сървъра на Ц.ШИС (и обратното). На последно място, следва да се опише също и процедурата за обратно преобразуване, свързана със съобщенията, криптирани с ключове, които вече не са валидни.
5. Следва да се опише процедура за управление на ключовете.
6. Следва да се опише процедура за обработка на съобщенията, отбелязани като неизползвани (поради някаква причина).

Прилагането на принципа за наличност при използването на пощенски сървър в Ц.ШИС следва да доведе до следните мерки:

1. За да се повиши наличността на подсистемата за изпращане на съобщения, комуникационният поток за съобщения от пощенския сървър следва да се различава от потока между Н.ШИС и Ц.ШИС.
2. Пощенският сървър на Ц.ШИС следва да разполага също с алтернативен поток за маршрутизация на съобщения, в случай че основният поток за маршрутизация не е наличен.
3. Препоръчва се кратък анализ на риска по въпроси, свързани с наличността (време за реагиране, необходимо време за създаване на резервно копие, сценарии в случай на ... и др.). За тази специфична процедура се препоръчва и изготвянето на план за непрекъснатост на дейностите.

4.4. Становище относно проекта за мерки за прилагане, включително наръчник SIRENE за Шенгенската информационна система от второ поколение (SCHAC 2503/07)

След като получи искане от Комисията да представи становище относно проекта за мерки за прилагане, включително преработен наръчник SIRENE за Шенгенската информационна система от второ поколение, Общият контролен орган прие становище през октомври 2007 г.

В становището си Общият контролен орган обърна специално внимание на сроковете за съхранение на записите, като постави въпроса защо е избран най-дългият срок на запазване вместо срокът от една година, посочен в член 18, параграф 3 от Решението на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение¹ и в член 18, параграф 3 от Регламента на Европейския парламент и на Съвета по същия въпрос².

Друг аспект, по който Общият контролен орган изрази загриженост, беше заличаването на европейските заповеди за арест (ЕЗА) с изтекъл срок. Общият контролен орган отбеляза, че ЕЗА с изтекъл срок не се заличават автоматично, а трябва да се заличат от държавите-членки.

Същевременно държавата-членка би проверила дали е въвела други ЕЗА относно същото лице, което може да доведе до удължаване на сигнала. Натрупаният опит с подобни процедури за заличаване не е изцяло положителен, поради което беше отправена препоръка записите с изтекъл срок автоматично да се заличават. Общият контролен орган препоръча да

¹ ОВ L 205, 7.8.2007 г., стр. 63.

² ОВ L 381, 28.12.2006 г., стр. 4.

се използва техническо решение — да се заличава единствено ЕЗА, а не сигналът, в случаите на повече от една ЕЗА относно едно и също лице.

В становището Общият контролен орган насочи вниманието си също към формата и качеството на биометричните данни. Той призова да се обърне повече внимание на по-широкото използване на пръстови отпечатащи отколкото на снимки, което е позволено с решението на Съвета. Тези биометрични данни следва да се използват единствено за потвърждаване на самоличността на лице, което е открито в резултат на буквено-цифрово търсене, осъществено в ШИС II.

Като анализира евентуалното въздействие върху принципите за защита на данните при свързване на сигналите, Общият контролен орган предложи да се гарантира, че разпоредбите в текста са изменени по начин, който подчертава, че правата на достъп са от решаващо значение за осигуряването на достъп до свързаните сигнали.

Като разгледа възможните видове търсене в ШИС II, Общият контролен орган изтъкна, че с оглед целите на ШИС II стандартната заявка следва да стане задължителна с възможност за други заявки за търсене в зависимост от нуждите във връзка с резултатите от първата стандартна заявка. Общият контролен орган твърдо настоя за изменение на текста, така че да се поясни, че стандартното търсене е винаги задължителното първо търсене в ШИС II, последвано при необходимост от друго търсене.

Друг въпрос, на който трябваше да се обърне внимание, беше определението за „разширена заявка“ като функция, предвидена за сложни заявки за търсене, които не са обхванати от други видове заявки, и която може да се определя от потребителите чрез специален програмен език за заявки. Общият контролен орган твърдо настоя за преразглеждане на тази „разширена заявка“ и за определяне на критериите за търсене, които могат да се използват в рамките на Решението на Съвета и на Регламента.

Общият контролен орган представи също така бележките си по преработения наръчник SIRENE. Органът насочи вниманието си към използването на ШИС II за други цели и постави въпроса как бюрото SIRENE на държавата-членка, която въвежда данните, може да изпълнява задълженията си да координира проверката на качеството на информацията, установени в член 7, параграф 2 от Решението на Съвета и от Регламента.

Общият контролен орган разгледа също отделните видове отговорности спрямо качеството на данните и необходимостта от специални правила за това как тези отговорности следва да се изпълняват и проверяват.

Друг въпрос, по който Общият контролен орган изрази загриженост, беше входната маска за въвеждане на данни с 15 категории информация, свързана с пръстовите отпечатъци, и доколко е уместна допълнителната информация, както и съответствието на такава обработка с решението на Съвета и регламента.

Важен елемент от това становище беше взаимодействието между SIRENE и Европол. Общият контролен орган твърдо подкрепи това сътрудничество, когато то допринася за качеството на данните, обработвани в ШИС II, или когато допринася за постигането на съответствие със специални членове от Решението на Съвета, свързани с достъпа на Европол до ШИС II.

Член 41, параграф 2 от Решението на Съвета задължава Европол да информира съответната държава-членка, когато при търсене открие съществуването на сигнал в ШИС II. Глава 2.14 от наръчника се отнася до националното звено на Европол в точките за контакт на държавите-членки. Следва обаче да се отбележи, че съгласно последното изменение¹ на Конвенцията за Европол ще бъде възможно това звено да не е единственото бюро за връзка между Европол и държавата-членка (вж. член 4, параграф 2 от Конвенцията за Европол). Освен това, предвид задачите на Европол, може да съществуват различни по своето естество и степен на поверителност основания да се информира държава-членка чрез националното звено на Европол. Предложеното в наръчника строго задължение да се информира SIRENE за всеки обмен може да не съответства на специалните условия, приложими към обмена между Европол и неговите точки за контакт в държавите-членки. Общият контролен орган предложи да се преформулира глава 2.14, а по отношение на отговорността на държавите-членки спрямо качеството на данните — да се въведе задължение на бюрото SIRENE да се съобщава информацията, предоставена чрез контакти между Европол и държавите-членки, която може да доведе до промяна или заличаване на сигнал в ШИС II.

4.5 Становище относно принципите, ръководещи сътрудничеството между националните контролни органи на основата на Шенгенската конвенция

През ноември 1996 г. Общият контролен орган реши да установи принципи, които да ръководят сътрудничеството между националните контролни органи. Въз основа на натрупания опит с това сътрудничество и общия преглед на прилагането на член 111, извършен от Общия контролен орган, беше взето решение да се актуализират принципите от

¹ ОВ С 2, 6.1.2004 г., стр. 3.

1996 г. Поради това през юни 2008 г. Общият контролен орган прие ново становище относно принципите, ръководещи сътрудничеството между националните контролни органи на основата на Шенгенската конвенция.

Повишеният обмен в рамките на ЕС на информация, свързана с правоприлагането, създава ситуация, при която отнасящите се до дадено лице данни може да се обработват в различни държави-членки и/или организации на ЕС, което затруднява субекта на данни да се възползва от правата си.

Различните национални законодателства и процедури, както и съществуващите езикови бариери, създават и допълнителни затруднения пред субекта на данни.

В Шенгенската конвенция могат да се открият примери за конкретно сътрудничество между националните органи за защита на данните във връзка с правата на субектите на данни. Субектът на данни може да поиска достъп във всяка от шенгенските държави, дори и в случай, че дадената шенгенска държава не отговаря за въвеждането на данните в Шенгенската информационна система (ШИС). Определени са специални правила относно приложимото право и взаимното сътрудничество между националните органи за защита на данните. Въпреки че в Шенгенската конвенция не се съдържа определение за „ясно сътрудничество“, органите за защита на данните са длъжни да си сътрудничат, като си оказват пълно съдействие един на друг и на физическото лице, което упражнява правата си.

Какво означава това на практика? Това означава, че упражняването на дадено право като субект на данни следва да гарантира на физическото лице достъп до правосъдие, което е част от ефективната правна защита.

Значението на конвенцията е, че признава, че субектите на данни невинаги са в състояние да отидат в друга държава или да се обърнат към орган в тази държава, за да защитят правата си, например с оглед на пътните разходи или езиковата бариера. Във връзка с това опитът с ШИС и правата на субектите на данни ни предоставя информация по какъв начин може допълнително да се развие сътрудничеството между националните органи за защита на данните.

Основните принципи се основават на следните членове¹:

¹ В новото правно основание за ШИС II се съдържат сходни разпоредби с изключение на член 114.

член 106, параграф 3 описва процедурата, в случай че шенгенските държави не могат да постигнат споразумение дали данните са неверни или са неправомерно въведени в системата; член 109 описва правото на достъп и процедурата, която трябва да се следва; член 110 описва правото на всяко лице да поиска поправка на фактически неточни данни или заличаване на неправомерно запаметени данни; член 111 описва правото да се отнесе въпросът до съд и ангажимента на шенгенските държави да изпълняват окончателните решения на съдилищата; член 114 описва правото да се поиска от националните контролни органи да извършат проверка на данните и процедурата, която трябва да се следва, ако тези данни са въведени от друга шенгенска държава.

В становището си Общият контролен орган разгледа няколко практически въпроса.

Език: Досегашната практика на сътрудничество показва, че понякога исканията или отговорите на искания се представят на езика на органа, отправил или получил искането. Тъй като може да бъде необходимо изготвяните от националните контролни органи документи да се предоставят на субекта на данни, е възможно да възникне ситуация, при която субектът на данни получава информация на друг език.

Възможните сценарии са два:

— Цялата кореспонденция да се води на един език, като за този случай се предлага английският език.

— Цялата кореспонденция да се води на езиците на участващите страни, като всяка от тях отговоря за официалния превод, който да е разбираем за другия национален контролен орган и за субекта на данни.

Срокове: Предвид засегнатите интереси на субекта на данни, исканията за сътрудничество ще се разглеждат без неоснователно забавяне.

Лица за контакт: За да се улесни допълнително сътрудничеството, ще се състави списък на лица за контакт във всеки от националните контролни органи. Предвид трудностите, свързани с постоянната актуализация на този списък, членовете на Общия контролен орган ще действат като лица за контакт.

4.6 Становище относно Шенгенската информационна система и извършителите на противообществени прояви 08/10

През лятото на 2008 г. Общият контролен орган взе под внимание обсъжданията в работна група „SIS/SIRENE“ относно използването на сигнали по член 99 в Шенгенската информационна система във връзка с извършители на противообществени прояви. Тези

обсъждания се съсредоточиха върху включването на нови категории данни в ШИС: данни за извършители на противообществени прояви, отнасящи се до лица, на които се забранява достъп до определени мероприятия, като напр. европейски срещи на високо равнище или подобни събития, международни спортни или културни мероприятия и други масови събирания, като се използват сигнали по член 99 от Шенгенската конвенция.

Това предложение повдигна редица въпроси във връзка със защитата на данните. Общият контролен орган изпрати писмо до председателя на работна група „SIS/SIRENE“/ Смесен комитет, в което изрази своята загриженост и съмнения по повод на тази инициатива. Общият контролен орган изказа също съжаление, че не е консултиран по този въпрос на по-ранен етап.

На първо място Общият контролен орган отбеляза, че сигналите по член 99 се отнасят по-специално до вече възбудено наказателно преследване на престъпление или до предотвратяване на заплахата за обществената безопасност. Това са предпоставките за сигнали по член 99. Предвид предложената цел за използване на сигнали по член 99 в ШИС, може да се приеме, че предотвратяването на заплахата за обществената безопасност е единствената задача на (предложения) сигнал. Освен това сигнал по член 99 може да се въведе в ШИС единствено относно лице, което е възнамерявало да извърши или е извършило многобройни и **изключително тежки престъпления**, или общата характеристика на даденото лице, по-специално във връзка с по-рано извършени от него престъпления, дава основание да се счита, че и занапред това лице ще извършва **изключително тежки престъпления**. В конвенцията не се съдържа определение на „**изключително тежки престъпления**“, а наказателното право се различава в отделните страни. Предвид описанието на тази група като „извършители на противообществени прояви“ при масови събирания като международни спортни и културни мероприятия, европейски срещи на високо равнище или подобни събития (Г-8), органът изрази съмнение дали описаните действия в предложението може да се класифицират като „**изключително тежки престъпления**“ и да доведат до сигнали по член 99.

Общият контролен орган изтъкна също така, че липсва определение на „извършител на противообществени прояви“ както в Шенгенската конвенция, така и в европейските или международните правни инструменти. Тъй като няма ясно определение и хармонизирано тълкуване на този термин, съществува значителен риск в ШИС да бъдат въведени данни на невинни хора без основание. Целта на сигналите относно тези лица е да им се откаже достъп до мероприятия. Това би означавало да не им се позволи да се намират в близост до тези мероприятия или дори да им се забрани достъпът до държавата, където се провежда мероприятието. Във връзка с това Общият контролен орган отбеляза, че член 99 от Шенгенската конвенция не предвижда принудителни мерки (по този член не може да се извърши арест) и може да се използва само за целите на скрито наблюдение или специален

контрол. Ето защо целта на самото предложение не е ясна и без съмнение би довела до отклонение от първоначалната цел на сигналите по член 99.

Шенгенската конвенция, както и новото правно основание за ШИС II¹, изрично ограничават използването на този вид сигнали до специална категория лица и специална категория престъпления. Категорията престъпления е описана в Шенгенската конвенция като „изключително тежки престъпления“, а в Решението на Съвета като „тежки престъпления“ с ясно позоваване на деянията, обобщени в член 2 от Рамковото решение на Съвета относно европейската заповед за арест и процедурите за предаване между държавите-членки. Убийство и тежка телесна повреда са единствените посочени в рамковото решение престъпления, свързани с насилие, което може да възникне във връзка с мероприятия, до които следва да се откаже достъп на съответните лица.

Друг аспект, който беше изтъкнат, беше целта на сигнала и очакваните действия, които следва да се предприемат. Член 99 от Шенгенската конвенция и член 36 от решението на Съвета описват целта на сигнала като скрито наблюдение или специален контрол (Шенгенска конвенция) или проверки от разстояние или явни проверки (решение на Съвета).

¹ Решение на Съвета относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II).

Общият преглед на член 99, извършен от Общия контролен орган, ясно показва също така, че националното законодателство на някои шенгенски държави не допуска възможност за осъществяване на специален контрол от компетентните органи, докато в други държави се изисква съдебна заповед¹.

С оглед предложението тези сигнали да се използват, за да се откаже достъп на извършители на противообществени прояви до определени мероприятия, което може да включва арест и задържане, Общият контролен орган стигна до заключението, че подобно използване на член 99 ще бъде в нарушение на целта, определена в Шенгенската конвенция и Решението на Съвета. Това, заедно със заключението, че явно липсва реалистична връзка между извършителите на противообществени прояви и категорията лица, определена в Шенгенската конвенция и Решението на Съвета, води до несъответствие на предложената употреба с правното основание и я прави незаконна.

¹ Доклад на Общия контролен орган за Шенген относно проверка на използването на сигнали по член 99 в Шенгенската информационна система, SCHAS 2501/08, Брюксел, 18 януари 2008 г.

5. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

При определянето на правата на субектите на данни Шенгенската конвенция предвижда система, в която субектите на данни да упражняват правата си във всяка шенгенска държава.

Съгласно член 115, параграф 3 от Шенгенската конвенция Общият контролен орган има компетентност и относно анализа на трудностите, които могат да възникнат при прилагането или тълкуването относно експлоатацията на Шенгенската информационна система, както и за разглеждане на проблеми, които могат да възникват при изпълнение на независимия контрол на националните части на договарящите страни или при упражняване правото на достъп до системата и изготвяне на хармонизирани предложения за намиране на общи решения на съществуващите проблеми.

Следва да се отбележи, че дял IV, глава 3 от Шенгенската конвенция разглежда защитата на личните данни и сигурността на данните в Шенгенската информационна система. В тази глава са описани задълженията на държавите, които участват в ШИС, както и правата на субектите на данни. Член 115 създава Общия контролен орган и описва неговите задачи и компетентност. Този член не предоставя на Общия контролен орган компетентност или правомощия да се намесва в конфликти между държавите по конкретни случаи.

Въпреки това, ако вниманието на Общия контролен орган бъде привлечено от случай, в който тълкуването на Шенгенската конвенция се нуждае от пояснение или хармонизирано предложение, органът има компетентност да представи становище.

На 17 август 2005 г. Общият контролен орган е получил искане от законния представител на г-н X, гражданин на трета страна. Към Общия контролен орган е отправено искане да предприеме действия в рамките на своите правомощия във връзка с френски сигнал по член 96 и решение на австрийския орган за защита на данните, с което се постановява заличаването на този сигнал. Сигналят по член 96 е въведен от Франция, като на г-н X е отказан достъп до шенгенската територия; въз основа на сигнала австрийските органи отказват на г-н X издаването на виза. Представителят е поискал достъп до обработените данни и е получил информация от Министерството на вътрешните работи на Австрия, че съществува сигнал по член 96, въведен от френските органи. Чрез френски адвокат, представителят на г-н X е започнал процедура за заличаването на тези данни пред френския орган за защита на данните — CNIL. Процедурата не е довела до заличаване на данните. Представителят на г-н X е започнал процедура срещу Министерството на вътрешните работи на Франция пред австрийската комисия за защита на данните. С решение от 7 юни 2005 г.

австрийската комисия за защита на данните обявява жалбата за валидна и постановява заличаването на сигнала в срок от три седмици. Поради това сигналът е трябвало да бъде заличен на 12 юли 2005 г. Френските органи не са заличили сигнала. Представителят на г-н Х е отправил искане към Общия контролен орган да предприеме действия по случая.

В този конкретен случай Общият контролен орган е установил едновременно протичане на две различни процедури: едната в Австрия, довела до решението на австрийската комисия за защита на данните, а другата във Франция, пред *Conseil d'Etat*, относно отказа на министерството на вътрешните работи на Франция да поправи или заличи сигнала, както е поискано от г-н Х. Предвид специфичното естество на този случай Общият контролен орган представи на всички страни своето тълкуване на член 111.

Ако се разгледа бъдещата правна рамка за ШИС II по отношение правата на субектите на данни, в нея са включени нови, положителни разпоредби в сравнение с Шенгенската конвенция. На първо място в член 42 от Регламент (ЕО) № 1987/2006 се предвижда право на информация за граждани на трети страни, които са обекти на сигнал, издаден в съответствие със същия регламент. Решение 2007/533/ПВР на Съвета и Регламент (ЕО) № 1987/2006 възлагат повече отговорности на шенгенските държави, като ги задължават (член 58 и член 41) в случай на молба от физическо лице за достъп, поправка и заличаване на данни, да уведомяват съответното лице възможно най-рано и във всеки случай не по-късно от 60 дни от датата на подаване на молба за достъп или по-рано, ако така е предвидено в националното законодателство.

От значение е, че както решението на Съвета, така и регламентът съдържат задължение за държавите да уведомяват физическите лица за развитието след упражняването на правата им за поправка или заличаване във възможно най-кратки срокове и във всички случаи не по-късно от три месеца от датата, на която е подадено заявление за поправка или заличаване, или по-рано, ако това е предвидено в националното законодателство. Това право е от изключително значение за субекта на данни, който своевременно може да установи какви лични данни, свързани с него, се обработват в системата.

6. СЪВМЕСТЕН НАДЗОР В БЪДЕЩЕ

Прилагането на Решение 2007/533/ПВР на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) (Решението на Съвета) и на Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) (Регламента) ще доведе до промени в бъдещата рамка за общ контрол на ШИС II. От значение е също така новата координирана рамка да не намали нивото на надзор, установено от Шенгенската конвенция. Член 61 от решението на Съвета предвижда, че Европейският надзорен орган по защита на данните проверява дали дейностите на управителния орган по обработка на личните данни се извършват в съответствие с Решението. Задълженията и правомощията по членове 46 и 47 от Регламент (ЕО) № 45/2001 се прилагат съответно. Член 62 от решението на Съвета създава нова правна рамка за координация между националните надзорни органи и Европейския надзорен орган по защита на данните, като всеки действа в рамките на своите правомощия; те си сътрудничат активно в рамките на своите отговорности и осигуряват координиран надзор на ШИС II. Сходни разпоредби се предвиждат и в Регламента. Бъдещото сътрудничество ще съдържа, както следва: националните надзорни органи и Европейският надзорен орган по защита на данните, в обхвата на съответните си правомощия, ще обменят необходимата информация, взаимно ще си съдействат при извършване на одити и проверки, ще разглеждат трудностите при тълкуването или прилагането на Решението на Съвета (Регламента), ще проучват проблемите при упражняването на независим надзор или при упражняването на правата на субектите на данни, ще съставят хармонизирани предложения за съвместни решения на всеки проблем и ще насърчават информираността по отношение на правата, свързани със защитата на данни, според необходимостта.

За тази цел националните надзорни органи и Европейският надзорен орган по защита на данните ще заседават най-малко два пъти годишно. На първото заседание следва да се приеме правилник. При необходимост, допълнителните методи на работа ще се разработват съвместно. Съвместен доклад за дейностите ще се изпраща на Европейския парламент, Съвета, Комисията и управителния орган веднъж на всеки две години. Поради това режимът и инфраструктурата за общ контрол, които са установени с член 115 от Шенгенската конвенция, ще се изменят в нова рамка за сътрудничество. Важно е да се отбележи фактът, че член 44 от регламента предвижда органът или органите, определени във всяка държава-членка, на които са поверени правомощията по член 28 от Директива 95/46/ЕО, да

извършва/т независимо наблюдение на законността на обработката на личните данни по линия на ШИС II на тяхна територия и на изпращането на тези данни от същата територия, както и обмена и последващата обработка на допълнителна информация. Това означава, че националните органи за защита на данните ще разполагат с по-широки правомощия в сравнение с член 114 от Шенгенската конвенция.

Член 63 от решението на Съвета предвижда разпоредби относно защитата на данни през преходния период, при условие че в случаите, когато Комисията делегира своите задължения през преходния период на друг/и орган/и съгласно член 15, параграф 4, тя обезпечава правото и възможността на Европейския надзорен орган по защита на данните да упражнява изцяло своите задачи, включително да извършва проверки на място, както и да упражнява всяко друго правомощие, възложено му съгласно член 47 от Регламент (ЕО) № 45/2001.

Въпреки това остава отворен въпросът за гаранциите относно защитата на данни при режима за общ контрол по време на миграцията от ШИС I+ към ШИС II. Кои са най-новите предизвикателства пред съвместния надзор? Безпроблемната миграция от ШИС I+ към ШИС II и гладкият преход от Общ контролен орган към координиран надзор? На 30 юни 2008 г. Комисията по граждански свободи, правосъдие и вътрешни работи организира кръгла маса на тема „Свобода и сигурност при интегрираното управление на границите на ЕС“, като една от дискусиите беше посветена на въпроса „Последици за защитата на данни от миграцията от ШИС I+ към ШИС II“. Председателят на Общия контролен орган и Европейският надзорен орган по защита на данните бяха поканени да участват в обсъжданията, като представят своите виждания. И двете страни изразиха единната позиция, че компетентностите на двата надзорни органи не следва да се припокриват. Европейският надзорен орган по защита на данните изрази увереност в гладкото преминаване към същинския надзор на системата; периодът по време на миграцията предоставя възможност да се постави началото на това „партньорство“.

И двамата участници изказаха убеждение в успешния координиран надзор на системата по време на преходния период в подготовка за действителния съвместен надзор на системата. Предвид бъдещата рамка за координиран надзор е обосновано да се изкажат благодарности и да се отчете значението и въздействието от работата на Общия контролен орган за Шенген. Годините на сериозен ангажимент и усилена работа, за да се натрупа опит, знания и доверие

в неговата компетентност, ще бъдат от основополагащо значение за бъдещата дейност на националните надзорни органи, заедно с Европейския надзорен орган по защита на данните. Естествено поради трудностите при надзор на толкова сложни бази данни като ШИС II ще бъдат необходими повече време и усилия, за да се прояви ефективността на подобен координиран надзор. Без съмнение обаче бъдещият надзор ще продължи да се осъществява по успешен начин, като се използва опитът и знанията, натрупани от Общия контролен орган.

7. ЧЛЕНОВЕ НА ОБЩИЯ КОНТРОЛЕН ОРГАН ЗА ШЕНГЕН

Председател: г-н Georges de La LOYERE

Заместник-председател: г-жа Angelika SCHRIEVER-STEINBERG

<p>АВСТРИЯ ЧЛЕНОВЕ г-жа Waltraut KOTSCHY г-жа Eva SOUHRADA-KIRCHMAYER</p> <p>ЗАМЕСТИК-ЧЛЕН г-н Gregor KONIG</p>	<p>БЕЛГИЯ ЧЛЕНОВЕ г-н Willem DEBEUCKELAERE г-н Bart DE SCHUTTER</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Priscilla de LOCHT</p>
<p>ЧЕШКА РЕПУБЛИКА ЧЛЕН г-жа Ludmila NOVAKOVA</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Miroslava MATOUSOVA</p>	<p>ДАНИЯ ЧЛЕН г-жа Lena ANDERSEN г-н Sten HANSEN</p> <p>ЗАМЕСТИК-ЧЛЕНОВЕ г-н Jens Harkov HANSEN г-н Ole TERKELSEN</p>
<p>ЕСТОНИЯ ЧЛЕН г-н Taago RANKEKEL</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Kaja PUUSEPP</p>	<p>ФИНЛАНДИЯ ЧЛЕНОВЕ г-н Reijo AARNIO г-жа Elisa KUMPULA</p> <p>ЗАМЕСТИК-ЧЛЕН г-н Heikki HUHTINIEMI</p>
<p>ФРАНЦИЯ ЧЛЕН г-н Georges de La LOYERE</p> <p>ЗАМЕСТИК-ЧЛЕН г-н Michel MAZARS</p>	<p>ГЕРМАНИЯ ЧЛЕНОВЕ г-н Peter SCHAAR г-жа Angelika SCHRIEVER-STEINBERG</p> <p>ЗАМЕСТИК-ЧЛЕНОВЕ г-н Wolfgang Von POMMER ESCHE г-н Michael RONELLENFITSCH</p>
<p>ГЪРЦИЯ ЧЛЕН г-н Leonidas KOTSALIS</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Maria ALIKAKOU</p>	<p>УНГАРИЯ ЗАМЕСТИК-ЧЛЕН г-жа Agnes RAJO</p>
<p>ИСЛАНДИЯ ЧЛЕНОВЕ г-н Bjorn GEIRSSON г-жа Sigrun JOHANNESDOTTIR г-жа Thordur SVEINSSON</p>	<p>ИТАЛИЯ ЧЛЕНОВЕ г-н Giovanni BUTARELLI г-жа Vanna PALUMBO</p>
<p>ЛАТВИЯ ЧЛЕНОВЕ г-жа Signe PLUMINA г-жа Aiga BALODE</p>	<p>ЛИТВА ЧЛЕНОВЕ г-жа Rita VAITKEVICIENE г-жа Neringa KAKTAVICIUTE- MICKIENE</p>

<p>ЛЮКСЕМБУРГ ЧЛЕНОВЕ г-н Georges WIVENES г-н Pierre WEIMERSKIRCH</p> <p>ЗАМЕСТИК-ЧЛЕН г-н Thierry LALLEMANG</p>	<p>МАЛТА ЗАМЕСТИК-ЧЛЕН г-н David CAUCHI</p>
<p>НИДЕРЛАНДИЯ ЧЛЕНОВЕ г-н Jacob KOHNSTAMM г-жа Jannette BEUVING</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Laetitia KRONER</p>	<p>НОРВЕГИЯ ЧЛЕНОВЕ г-н George APENES г-жа Guro SLETTE MARK</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Astrid FLESLAND</p>
<p>ПОЛША ЧЛЕН г-н Michał SERZYCKI</p> <p>ЗАМЕСТИК-ЧЛЕН г-н Piotr DROBEK</p>	<p>ПОРТУГАЛИЯ ЧЛЕНОВЕ г-н Luis BARROSO г-жа Isabel CERQUEIRA DA CRUZ</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Clara VIEIRA CARDOSO GUERRA</p>
<p>СЛОВАШКА РЕПУБЛИКА ЧЛЕН г-н Peter LIESKOVSKY</p> <p>ЗАМЕСТИК-ЧЛЕН г-н Tomáš MIČO</p>	<p>СЛОВЕНИЯ ЧЛЕНОВЕ г-жа Alenka JERSE г-жа Natasa PIRC MUSAR</p> <p>ЗАМЕСТИК-ЧЛЕН г-н Marijan EONE</p>
<p>ИСПАНИЯ ЧЛЕН г-н Rafael GARCIA GOZALO</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Marta AGUIRRE CALZADA</p>	<p>ШВЕЦИЯ ЧЛЕН г-жа Elizabeth WALLIN</p> <p>ЗАМЕСТИК-ЧЛЕН г-жа Birgitta ABJORNSSON</p>
<p>ШВЕЙЦАРИЯ ЧЛЕНОВЕ г-н Bruno BAERISWYL г-н Jean-Philippe WALTER</p>	

8. НАБЛЮДАТЕЛИ В ОБЩИЯ КОНТРОЛЕН ОРГАН ЗА ШЕНГЕН

БЪЛГАРИЯ г-н Veselin TSELKOV г-н Valentin ENEV	КИПЪР г-жа Goulla FRANGO г-жа Louiza MARKIDOU
ИРЛАНДИЯ г-н Billy HAWKES г-жа A. GARDNER г-жа A. McCABE	ЛИХТЕНЩАЙН г-н Philipp MITTELBERGER
РУМЪНИЯ г-жа Georgeta BASARABESCU г-жа Nicoleta RUSU г-жа Simona SANDRU г-жа Alina SAVOI г-н George GRIGORE	ОБЕДИНЕНО КРАЛСТВО г-н David Smith г-жа Jane DAWSON