

Шенгенска информационна система от второ поколение (ШИС II)
Ръководство за упражняване на правото на достъп
(Резюме)

Лица, чиито лични данни се събират, съхраняват или обработват по друг начин в Шенгенската информационна система от второ поколение (наричана по-нататък „ШИС II“), имат права на достъп, поправка на неточни данни и заличаване на незаконно съхранявани данни (1). В настоящото ръководство са описани начините за упражняване на тези права.

I. Въведение в Шенгенската информационна система от второ поколение (ШИС II)

ШИС II е широкомащабна информационна система, създадена като компенсаторна мярка на премахването на проверките по вътрешните граници и имаща за цел да гарантира високо ниво на сигурност в пространството на свобода, сигурност и правосъдие на Европейския съюз, включително поддържане на обществената сигурност и обществения ред, както и запазване на сигурността на териториите на държавите членки. ШИС II се прилага във всички държави - членки на ЕС, с изключение на Кипър, Хърватия и Ирландия (2), и в четири асоциирани държави: Исландия, Норвегия, Швейцария и Лихтенщайн.

ШИС II е информационна система, която дава възможност на националните правоприлагащи, съдебни и административни органи да изпълняват специфични задачи, като обменят съответни данни. Европейските агенции ЕВРОПОЛ и ЕВРОЮСТ също имат достъп, макар и ограничен, до тази система.

Категории на обработваната информация

В ШИС II централно място заемат две широки категории информация под формата на сигнали, на първо място, за *лица* - които са издирвани с цел задържане, изчезнали, търсени за помощ в съдебно производство, за скрит или специален контрол, или граждани на трети държави, подлежащи на отказ за влизане или пребиваване в шенгенското пространство, и, на второ място, за *вещи* - като МПС, документи за пътуване, кредитни карти, за конфискуване или използване като доказателство в наказателно производство, или за скрит или специален контрол.

Правно основание

В зависимост от вида на сигнала ШИС II се регламентира или от Регламент (ЕО) № 1987/2006 на Европейския парламент и на Съвета от 20 декември 2006 г. за създаването, функционирането и използването на Шенгенска информационна система от второ поколение във връзка със сигнални процедури, попадащи в обхвата на дял IV от Договора за създаване на Европейската общност - бивш първи стълб (наричан по-нататък „Регламент за ШИС II“), или от Решение 2007/533/ПВР на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение, когато се отнася до процедури, попадащи в обхвата на дял VI от Договора за създаване на Европейската общност - бивш трети стълб (наричано по-нататък „Решение за ШИС II“).

Категории на обработваните лични данни

Когато сигналът се отнася до лице, информацията трябва винаги да включва име, фамилия и всякакви псевдоними, пол, позоваване на решението, предизвикало подаването

на сигнала, и мярката, която следва да се предприеме. Ако има такава, сигналът може да съдържа и информация като всякакви специфични, обективни, физически характеристики, които не подлежат на промяна; място и дата на раждане; снимки; дактилоскопични отпечатъци; националност(и); дали въпросното лице е въоръжено, склонно към насилие или беглец; причина за сигнала; орган, подаващ сигнала; връзки с други сигнали, въведени в ШИС II в съответствие с член 37 от Регламента за ШИС II или член 52 от Решението за ШИС II.

Архитектура на системата

ШИС II се състои от: 1) централна система („централна ШИС II“); 2) национална система („N.SIS II“) във всяка държава членка, която се свързва с централната ШИС II; и 3) комуникационна инфраструктура между централната система и националните системи, образувайки кодирана виртуална мрежа, предназначена за данни на ШИС II и обмен на данни между органите, отговарящи за обмена на всяка допълнителна информация (бюра SIRENE) (3).

II. Права, предоставени на физически лица, чиито данни се обработват в ШИС II

В съответствие с принципите на защита на данните, на всички физически лица, чиито данни се обработват в ШИС II, се предоставят специални права от Регламента за ШИС II и Решението за ШИС II (4), които са разгледани по-долу. Всеки, който упражнява което и да е от тези права, може да се обърне към компетентните органи в държава по свой избор, в която функционира ШИС II. Тази опция е възможна, тъй като всички национални бази данни (N.SIS II) са идентични с базата данни на централната система (5). Следователно тези права могат да се упражнят във всяка държава, която работи с ШИС II, независимо от държавата членка, подала сигнала.

Когато дадено лице упражнява правото си на достъп, поправка на неточни данни и заличаване на незаконно съхранявани данни, отговорите на компетентните органи трябва да бъдат дадени в точно определен срок. По този начин лицето ще бъде информирано във възможно най-кратък срок и във всички случаи не по-късно от 60 дни от датата, на която е поискало достъп, или по-скоро, ако националното законодателство предвижда това (6). Лицето ще бъде информирано и за последващите действия, предприети за упражняване на неговите права за поправка или заличаване, във възможно най-кратък срок, но във всички случаи не по-късно от три месеца от датата, на която е поискало поправка или заличаване, или по-скоро, ако националното законодателство предвижда това (7).

Право на достъп

Правото на достъп дава възможност на всекиго, който поиска това, да узнае свързаната с него или нея информация, съхранявана в досие с данни, както е посочено в националното законодателство. Това е основен принцип на защитата на лични данни, което дава възможност на субектите на данни да упражняват контрол върху личните данни, съхранявани от трети страни. Това право е изрично предвидено в член 41 от Регламента за ШИС II и в член 58 от Решението за ШИС II.

Правото на достъп се упражнява в съответствие със законодателството на държавата членка, в която е отправено искането. Процедурите са различни в отделните държави, както и правата за съобщаване на данните на заявителя. Когато дадена държава членка получи искане за достъп до сигнал, който не е подаден от самата нея, тази държава трябва да уведоми подалата го държава за своето становище относно възможността за разкриване на

данните на заявителя (8). Информацията не се съобщава на субекта на данни, ако това е крайно необходимо за изпълнение на правната задача, свързана със сигнала, или с цел да се защитят правата и свободите на други хора.

Понастоящем има два вида системи, регламентиращи правото на достъп до данни, обработени от правоприлагащите органи, и следователно приложими и към данните на ШИС. В някои държави членки правото на достъп е пряко, а в други – непряко.

В случай на **пряк достъп** съответното лице подава заявление направо до органите, обработващи данните (полиция, жандармерия, митници и пр.). Ако националното законодателство допуска това, на заявителя може да бъде изпратена свързаната с него информация.

В случай на **непряк** достъп лицето изпраща искането си за достъп на националния орган за защита на данните на държавата, до която искането е подадено. Органът за защита на данните извършва необходимите проверки за разглеждане на искането и отговаря на заявителя.

Право на поправка или заличаване на данни

Правото на достъп се допълва от правото за разрешаване на поправка на личните данни, когато те са фактически неточни или непълни, и правото да се поиска тяхното заличаване, ако са били незаконно съхранявани (член 41, параграф 5 от Регламента за ШИС II и член 58, параграф 5 от Решението за ШИС II).

Съгласно шенгенската правна рамка само държавата, която подава сигнал в ШИС II, може да го промени или заличи (вж. член 34, параграф 2 от Регламента за ШИС II и член 49, параграф 2 от Решението за ШИС II). Ако искането е подадено в държава членка, която не е подала сигнала, компетентните органи на съответните държави членки си сътрудничат при разглеждане на случая, като обменят информация и извършват необходимите проверки. Заявителят следва да посочи основанията за своето искане за поправка или заличаване на данните и да събере всяка значима информация в негова подкрепа.

Средства за правна защита: правото да се подаде жалба до органа за защита на данните или да се заведе иск за съдебно производство

Член 43 от Регламента за ШИС II и член 59 от Решението за ШИС II осигуряват средствата за правна защита, с които разполагат физическите лица, когато искането им не е било удовлетворено. Всяко лице може да заведе иск пред съдилищата или пред компетентния орган по законодателството на всяка държава членка за получаване на достъп, поправка, заличаване или получаване на информация, или за получаване на компенсация във връзка със сигнал, свързан с него.

В случаите, когато трябва да разглеждат жалба с трансграничен елемент, националните органи за защита на данните следва да си сътрудничат помежду си с оглед да се гарантират правата на субектите на данни.

III. Процедура за упражняване на правото на достъп до информация в ШИС II – валидна за Република България

1. Същност на правото (пряко, косвено, смесено)

Всяко лице има право на достъп до неговите лични данни, събрани без неговото знание и обработвани в информационните фондове на Министерството на вътрешните работи (МВР) или ШИС, като депозира молба за достъп до националното Бюро СИРЕНЕ, обособено като звено в Дирекция „Международно оперативно сътрудничество“ на МВР.

2. Данни за контакт на органа, в който се депозират молбите за достъп

Министерство на вътрешните работи на Република България
София, 1000
ул. „Шести септември“ №29
Тел.: +359 2 982 5000 – централно управление
Уеб сайт: <http://www.mvr.bg/contactus.htm>

3. Формални изисквания по отношение на молбата: необходима информация и документи – възможни разходи (изрично се упоменава, когато упражняването на тези права е безплатно)

Лицата могат да упражнят това право чрез депозирането на писмена молба (подадена лично или чрез изрично упълномощени лица с нотариално заверено пълномощно) до администратора на лични данни (в този случай – Министерството на вътрешните работи).

Молбата би могла да бъде депозирана и по електронната поща, следвайки установената с Закона за електронния документ и електронния подпис процедура.

Министърът на вътрешните работи трябва да издаде решение в рамките на 14-дневен срок от получаването на молбата за достъп. При поискване, копие на обработените лични данни на лицето може да бъде предоставено на хартия.

Не е предвидена такса за депозирането на молба за достъп до данни в ШИС.

4. Данни за контакт на националния орган за защита на личните данни и възможната му роля

Комисия за защита на личните данни
София, 1592
бул. „Проф. Цветан Лазаров“ №2
Кол център – Тел.: + 359 2 9153 518
Деловодство – Тел.: +359 2 9153 515; + 359 2 9153 519
Факс: + 359 2 9153 525
Електронна поща: kzld@cpdp.bg
Уеб сайт: www.cdpd.bg

Всяко лице има правото да поиска от КЗЛД да извърши проверка на данните в Шенгенската информационна система, отнасящи се за него, както и да получи информация за тяхното използване. Ако данните са въведени от друга държава-членка, КЗЛД ще извърши проверката в тясно сътрудничество с надзорния орган на тази държава-членка.

В случай, че администраторът на лични данни (Министърът на вътрешните работи) не уважи молбата за достъп на физическото лице и ако то счита, че има нарушение на Закона за защита на личните данни при обработването на личните му данни (напр. възпрепятстване на упражняването на правата на физическото лице), лицето може да подаде жалба до КЗЛД (за да инициира административното производство). Ако физическото лице не подаде жалба до КЗЛД, то може да обжалва решението (за отказа за достъп и предоставяне на информация или възпрепятстването на упражняването на правото на изтриване, коригиране и блокиране) пред съда. Комисията за защита на личните данни разглежда жалбата и приема решение, което, след влизането си в сила, е обвързващо за администратора на лични данни. Ако предмет на жалбата е бил отказ за достъп, с решението си КЗЛД може да задължи администратора на лични данни да предостави достъп и да даде инструкции за това.

Когато се установи нарушение, свързано с обработването на лични данни, КЗЛД може да наложи административно наказание на администратора на лични данни – глоба или имуществена санкция.

5. Очакван резултат на молбите за достъп. Съдържание на информацията (прилагат се специфичните крайни срокове, установени в съответната държава)

В Закона за Министерството на вътрешните работи е предвидено, че всяко физическо лице има правото да изиска достъп до неговите лични данни, събрани без негово съгласие и обработвани в информационните фондове на МВР. Администраторът на лични данни издава решение в рамките на 14-дневен срок от получаването на молбата за достъп. На физическото лице се предоставя хартиено копие на неговите лични данни, които са били обект на обработване, в случай на проявено желание. Структурите на МВР могат частично или изцяло да откажат предоставянето на данни, когато:

- това може да застраши националната сигурност или обществения ред;
- за защита на класифицирана информация или държавна тайна;
- източниците на информация или методите и средствата за нейното събиране могат да бъдат разкрити;
- предоставянето на данните на физическото лице би могло да дерогира упражняването на законово регламентирани правомощия на МВР;
- ако информацията е въведена в ШИС от друга държава, която не разрешава нейното предоставяне.

Физическите лица биват уведомявани писмено за правното основание на отказа. Ако уведомлението не е изпратено в законоустановените срокове, това се счита за отказ. Съгласно чл. 161 от Закона за Министерството на вътрешните работи, отказът е предмет на административно обжалване по Административнопроцесуалния кодекс.

6. Препратки към приложимото национално законодателство

- Закон за Министерството на вътрешните работи - обн. ДВ. бр.53 от 27 Юни 2014 г., последно допълнение от ДВ. бр. 61 от 11 август 2015 г.
- Наредба № 8121з-465 от 26 август 2014 г. за организацията и функционирането на Националната Шенгенска информационна система на Република България (Обн., ДВ, бр. 74 от 2014 г.)
- Закон за защита на личните данни - обн. ДВ. бр.1 от 4 Януари 2002г., последно изм. и доп. ДВ. бр.15 от 15 Февруари 2013г.

7. Език

Молбите за достъп до лични данни, обработвани в Шенгенската информационна система, трябва да бъдат изготвени на български език.

(1) Тези права са предоставени в съответствие с член 41 от Регламент (ЕО) № 1987/2006 от 20 декември 2006 г. за създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II) и член 58 от Решение 2007/533/ПВР на Съвета от 12 юни 2007 г. относно създаването, функционирането и използването на Шенгенска информационна система от второ поколение (ШИС II).

(2) Информацията е от юли 2015 г. Въпреки че използват ШИС, България и Румъния имат все още вътрешни граници. Обединеното кралство има достъп до ШИС с изключение на сигнали, които се използват за недопускане на шенгенска територия.

(3) Данните на ШИС II се въвеждат, актуализират, заличават и търсят посредством различните национални системи. Централната система, която изпълнява технически надзор и административни функции, е разположена в Страсбург (Франция). Тя предоставя услугите за въвеждането и обработването на данните в ШИС II. Резервна централна система, способна да осигури всички функции на главната централна система в случай на повреда на тази система, е разположена недалеч от Залцбург (Австрия). Всяка държава членка отговаря за изграждането, функционирането и поддържането на своята собствена национална система и за свързването ѝ с централната система. Тя определя орган, национална служба за ШИС II (служба N.SIS II), която има основна отговорност за съответния национален проект на ШИС II. Този орган отговаря за безпрепятственото функциониране и сигурността на своята национална система.

(4) Вж. по-специално член 41 от Регламента за ШИС II и член 58 от Решението за ШИС II.

(5) Вж. член 4, параграф 1, буква б) от Регламента и Решението за ШИС II.

(6) Вж. член 41, параграф 6 от Регламента за ШИС II и член 58, параграф 6 от Решението за ШИС II.

(7) Вж. член 41, параграф 7 от Регламента за ШИС II и член 58, параграф 7 от Решението за ШИС II.

(8) Вж. член 41, параграф 3 от Регламента за ШИС II и член 58, параграф 3 от Решението за ШИС II.