Съвет на
Европейския съюз

Брюксел, 25 януари 2021 г.
(OR. en)

5534/21

Междуинституционално досие:
2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
До:	Делегациите
№ предх. док.:	14250/20
Относно:	Решение за изпълнение на Съвета за отправяне на препоръка за отстраняване на недостатъците, установени при оценката от 2019 г. на прилагането от **Словакия** на достиженията на правото от Шенген в областта на **защитата на данните**

Приложено на делегациите се изпраща Решението за изпълнение на Съвета за отправяне на препоръка за отстраняване на недостатъците, установени при оценката от 2019 г. на прилагането от Словакия на достиженията на правото от Шенген в областта на защитата на данните, прието чрез писмена процедура на 21 януари 2021 г.

В съответствие с член 15, параграф 3 от Регламент (ЕС) № 1053/2013 на Съвета от 7 октомври 2013 г. тази препоръка ще бъде изпратена на Европейския парламент и на националните парламенти.

Решение за изпълнение на Съвета за отправяне на

ПРЕПОРЪКА

за отстраняване на недостатъците, установени при оценката от 2019 г. на прилагането от Словакия на достиженията на правото от Шенген в областта на защитата на данните

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) № 1053/2013 на Съвета от 7 октомври 2013 г. за създаването на механизъм за оценка и наблюдение с цел проверка на прилагането на достиженията на правото от Шенген и за отмяна на решението на изпълнителния комитет от 16 септември 1998 г. за създаване на Постоянен комитет за оценка и прилагане на Шенгенското споразумение[1], и по-специално член 15 от него,

като взе предвид предложението на Европейската комисия,

като има предвид, че:

(1) Целта на настоящото решение е да се препоръчат корективни действия на Словашката република за отстраняване на недостатъците, установени по време на извършената през 2019 г. оценка по Шенген в областта на защитата на данните. След извършването на оценката, с Решение за изпълнение C(2020) 8160 на Комисията беше приет доклад, в който се съдържат направените констатации и оценки и се посочват най-добрите практики и недостатъците, установени по време на оценката.

[1] ОВ L 295, 6.11.2013 г., стр. 27.

(2) От последната извършена през 2012 г. оценка по Шенген насам Органът за защита на данните (ОЗД) редовно провежда надзорни дейности по ШИС II в съответствие с годишно планиране, както и че е разработена концепция за проверките по ШИС II за следващите четири години; че ОЗД е извършил значителен брой проверки по ВИС в консулствата; усилията на ОЗД и Министерството на вътрешните работи (МВР) за предоставяне на информация на субектите на данни под формата на електронни и печатни материали; версиите на различни езици на информацията по свързаните с Шенген теми на уебсайта на ОЗД и в листовките; че ОЗД предоставя образци на исканията на субектите на данни във връзка с ШИС и ВИС; че бюрото SIRENE предоставя отговори на исканията не само на словашки, но и на английски език; че словашките органи информират субектите на данни, ако в ШИС II не се съхраняват данни за тях; много активният контрол на записите във ВИС и ШИС II от страна на отдела за инспекция на Бюрото за инспекция към МВР; много активната роля на двамата служители от отдела за сигурност на Министерството на външните работи и европейските въпроси (МВнРЕВ), който се занимава с въпросите, свързани със защитата на данните; че МВнРЕВ предоставя обучение по защита на данните на своя персонал, по-специално преди временно командироване за изпълнение на консулски задачи, както и че отделът за сигурност (в качеството си на длъжностно лице по защита на данните) предоставя такова обучение; че предвидената процедурна и физическа сигурност за защита на данните в ШИС II е на високо равнище; много активната роля на длъжностното лице по защита на данните и на заместник-длъжностното лице по защита на данните от отдела за защита на данните на звеното за инспекция на Бюрото за инспекция към МВР, включително относно насоките и контрола на записите във връзка с ШИС II; че МВР предоставя обучение по защита на данните за всички крайни ползватели на Н.ШИС II.

(3) Като се има предвид колко важно е да се спазват достиженията на правото от Шенген относно защитата на данните във връзка с ВИС, следва да се даде приоритет на изпълнението на препоръки 7 и 24.

(4) Настоящото решение следва да се предаде на Европейския парламент и на парламентите на държавите членки. Съгласно член 16, параграф 1 от Регламент (ЕС) № 1053/2013 в срок от три месеца след приемането на решението Словашката република следва да изготви план за действие, съдържащ всички препоръки за отстраняване на посочените в доклада за оценка недостатъци, и да представи този план за действие на Комисията и на Съвета,

ПРЕПОРЪЧВА:

Словашката република:

Орган за защита на данните

1. да гарантира, че с оглед подобряване на работата и ефективността на ОЗД бюджетът и персоналът на ОЗД следва да бъдат допълнително увеличени;

2. да гарантира, че частта от общия държавен бюджет, предвидена за ОЗД, следва да бъде ясно видима, за да се гарантира, че ОЗД разполага с отделен публичен годишен бюджет;

3. да гарантира, че в рамките на бюджетната процедура Държавният съвет следва да бъде информиран за позицията на ОЗД относно неговите бюджетни нужди и проведените между ОЗД и Министерството на финансите (МФ) обсъждания относно бюджета;

4. да предприеме мерки, така че МФ да не може да установява връзка между бюджета и размера на глобите, които трябва да бъдат събрани от ОЗД, тъй като това може да окаже въздействие върху естеството и приоритизирането на работата на ОЗД и по този начин да засегне неговата независимост. Следва да се гарантира, че бюджетът на ОЗД не може да бъде намаляван в рамките на календарната година, в случай че ОЗД не е събрал изцяло очакваните глоби;

5. да гарантира, че на ОЗД ще бъдат възложени всички задачи и правомощия, предвидени за органите за защита на данните съгласно членове 57 и 58 от Общия регламент относно защитата на данните;

6. да гарантира, че в допълнение към редовните надзорни дейности, извършвани в службата Н.ШИС и бюрото SIRENE, ОЗД упражнява надзор върху повече органи крайни ползватели, които имат достъп до ШИС II;

7. да гарантира, че надзорните дейности на ОЗД във връзка с ВИС включват инспекция на централния визов орган (ЦВО) по отношение на обработването на данни в Н.ВИС. Тъй като крайният срок за първия одит на националната визова система беше октомври 2015 г., ОЗД следва да проведе тази все още липсваща част от одита във възможно най-кратък срок;

8. да гарантира, че ОЗД проверява редовно и външните изпълнители;

Права на субектите на данни

9. да намери подходящ начин, по който ОЗД, МВР и МВнРЕВ да информират субектите на данни относно потенциалните рискове, които крие предаването на копия на лични карти и чувствителна информация чрез отворен интернет. МВР и МВнРЕВ се приканват да обмислят възможността да предложат на субектите на данни защитен канал за електронно предаване на такива документи;

10. да гарантира, че 60-дневният срок за отговор по исканията на субектите на данни във връзка с ШИС II, предвиден в член 41, параграф 6 от Регламента за ШИС II и в член 58, параграф 6 от Решението за ШИС II, се спазва докато не започнат да се прилагат изцяло (най-късно до 28 декември 2021 г.) новите достижения на правото в областта на ШИС[1], където има препратки към крайния срок за отговор по исканията на субектите на данни, предвиден в ОРЗД (30 дни с възможност за удължаване с още два месеца, когато е необходимо);

11. да обмисли възможността за предоставяне на част от отпечатаната информация (листовки/знаци и т.н.) за субектите на данни в помещенията на полицейските участъци, както и да я направи видима и лесно достъпна;

12. да обмисли възможността за предоставяне например на неофициална версия на английски език на решенията на ОЗД по жалби относно искания на субекти на данни във връзка с ШИС II; това би помогнало на субектите на данни да разберат по-добре решението и по този начин би засилило правата на субектите на данни;

13. да гарантира, че информацията относно правата на субектите на данни във връзка с ВИС на уебсайта на МВнРЕВ е по-лесна за намиране; уебсайтът следва също така да предоставя образци за упражняването на правата на субектите на данни във връзка с ВИС;

---

[1] Регламент (ЕС) 2018/1862 на Европейския парламент и на Съвета от 28 ноември 2018 г. за създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на полицейското сътрудничество и съдебното сътрудничество по наказателноправни въпроси, за изменение и отмяна на Решение 2007/533/ПВР на Съвета и за отмяна на Регламент (ЕО) № 1986/2006 на Европейския парламент и на Съвета и Решение 2010/261/ЕС на Комисията, ОВ L 312, 7.12.2018 г., стр. 56 (вж. по-специално членове 66 – 71); Регламент (ЕС) 2018/1861 на Европейския парламент и на Съвета от 28 ноември 2018 г. за създаването, функционирането и използването на Шенгенската информационна система (ШИС) в областта на граничните проверки, за изменение на Конвенцията за прилагане на Споразумението от Шенген и за изменение и отмяна на Регламент (ЕО) № 1987/2006, ОВ L 312, 7.12.2018 г., стр. 14 (вж. по-специално членове 51—57).

14. да гарантира, че формулярът за кандидатстване за издаване на виза съдържа ясна информация за различните органи, които обработват лични данни като част от националната визова система. По-специално следва да бъде поместена информация, че МВнРЕВ е администраторът на данни;

15. да предостави на субектите на данни във връзка с ВИС физическа информация (листовки/знаци и т.н.) на летищата и в другите зони за граничен контрол и да я направи видима и лесно достъпна;

16. да гарантира, че отговорите до субектите на данни във връзка с лични данни във ВИС предоставят информация относно възможността за обжалване на отговора пред ОЗД и компетентния съд;

17. да предприеме необходимите мерки за изясняване на отговорностите на МВнРЕВ и ЦВО по разглеждането на исканията на субектите на данни във връзка с ВИС и да изготви вътрешни или методологически насоки и за двата субекта; тази информация следва да бъде на разположение на субектите на данни;

Визова информационна система

18. да предприеме необходимите мерки за повишаване на равнището на сигурност за достъп до държавната среда, и по-специално до националните приложения за визи в МВнРЕВ и МВР (ЦВО), по-специално чрез достъп до националните визови бази данни посредством многофакторна технология;

19. да вземе необходимите мерки за подобряване на физическата и организационната сигурност в центъра за данни Н.ВИС на МВнРЕВ, по-специално по отношение на следните аспекти:

   – осигуряване на дневник на посетителите на входа на центъра за данни за служители по ИКТ, посетители или доставчици, достъпът на които следва да бъде ограничен;

   – инсталиране на система за гасене на пожари с газ (аргонит);

   – инсталиране на система за откриване на водни течове;

   – осигуряване на обезпрашен и подреден под;

   – заключване на защитната стена на сървърите на ЕС;

20. да ускори процедурата по създаване на нов център за данни Н.ВИС на друго място и преместването на центъра за данни;

21. да обмисли възможността за промяна на местния срок на съхраняване на файловете със записи на Н.ВИС в дипломатическите и консулските мисии чрез определяне на времеви период, а не на размер мегабайти;

22. да обмисли възможността за използване на системи за автоматична проверка на записите в МВнРЕВ;

23. да предприеме необходимите мерки, така че дипломатическите мисии или МВнРЕВ редовно да инспектират външните изпълнители;

24. да предприеме необходимите мерки за предоставяне на обучение по защита на данните за местните консулски служители по по-систематичен и еднакъв начин;

25. да гарантира, че при електронното заявление за издаване на виза се изисква същата информация като при заявлението за издаване на виза на хартиен носител (както е посочено в приложение I към Визовия кодекс на ЕС[1]);

Шенгенска информационна система II

26. да предприеме необходимите мерки за повишаване на равнището на сигурност за достъп до Н.ШИС II, по-специално чрез многофакторна автентикация и използване единствено на https връзки за достъп до Н.ШИС II;

27. да гарантира, че МВР уведомява ОЗД за всяко нарушение на сигурността на данните, което има вероятност да доведе до риск за правата и свободите на физическите лица. Освен това МВР следва да създаде регистър за нарушенията на сигурността на личните данни;

---

[1] Регламент (ЕО) № 810/2009 на Европейския парламент и на Съвета от 13 юли 2009 г. за създаване на Визов кодекс на Общността (Визов кодекс); ОВ L 243, 15.9.2009 г., стр. 1.

Обществена осведоменост

28. да обмисли възможността за поставяне на листовките за ОЗД на разположение на субектите на данни и на по-достъпни места, като например полицейските участъци, зоните за граничен контрол и помещенията на консулствата;

29. да обмисли възможността за предоставяне на достъп до презентациите, семинарите и общодостъпните мероприятия на ОЗД за широката общественост, и по-специално за субектите на данни, тъй като те са заинтересовани от информацията относно ШИС II и ВИС.

Съставено в Брюксел на […] година.

За Съвета

Председател