Препоръка 01/2019 относно проекта на списък на Европейския надзорен орган по защита на данните във връзка с операциите по обработване, за които се изисква оценка на въздействието върху защитата на данните (член 39, параграф 4 от Регламент (ЕС) 2018/1725)

Прието на 10 юли 2019 г.

Съдържание

Европейският комитет по защита на данните,

като взе предвид член 70, параграф 1, буква д) от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (наричан по-нататък „ОРЗД“),

като взе предвид член 39, параграф 4 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (наричан по-нататък „Регламент 2018/1725“),

като взе предвид член 12 и член 22 от своя Правилник за дейността от 25 май 2018 г.,
преработен на 23 ноември 2018 г.,

като има предвид, че:

(1) Основната роля на Комитета е да осигурява съгласуваност при прилагането на Регламент 2016/679 (наричан по-нататък „ОРЗД“) в цялото Европейско икономическо пространство. Съгласно член 70, параграф 1, буква д) от ОРЗД, за тази цел, Комитетът разглежда по искане на някой от своите членове всеки въпрос, отнасящ се до прилагането на Регламента, и издава насоки, препоръки и най-добри практики за насърчаване на съгласуваното прилагане на същия. Член 39, параграф 6 от Регламент 2018/1725 предвижда, че преди приемането на списъка на операциите по обработване, за които се изисква оценка на въздействието върху защитата на данните съгласно член 39, параграф 4 от Регламент 2018/1725, Европейският надзорен орган по защита на данните отправя искане до ЕКЗД да разгледа, проекта на този списък в съответствие с член 70, параграф 1, буква д) от ОРЗД.. Това задължение се прилага, доколкото списъкът се отнася до операции по обработване от администратор по смисъла на член 3, точка 8 от Регламент 2018/1725, действащ съвместно с един или повече администратори, различни от институции и органи на Съюза. Поради това, целта на настоящата препоръка е да бъде съгласувана с подхода, възприет преди това към проектите на списъци на надзорните органи (наричани по-нататък „НО“). Комитетът се стреми да постигне съгласуваност на първо място, като изисква от НО да включат в списъците си някои видове обработване, на второ място, като изисква от тях да премахнат някои критерии, за които Комитетът не счита непременно, че създават високи рискове за субектите на данни, и накрая, като изисква от тях да използват някои критерии по хармонизиран начин.

(4) Съгласно член 39, параграф 1 от Регламент 2018/1725 извършването на ОВЗД е задължително за администратора само, когато съществува вероятност обработването „да породи висок риск за правата и свободите на физическите лица“. В член 39, параграф 3 от Регламент 2018/1725 са посочени примери на случаи, които може да породят висок риск. Това е неизчерпателен списък, който съответства на формулировката на член 35, параграф 3 от ОРЗД. В Насоките относно оценката на въздействието върху защитата на данни[1], одобрени от ЕКЗД[2], Работната група за

[1] РГ29, Насоки относно оценката на въздействието върху защитата на данни и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679 (WP 248 rev. 01).
[2] ЕКЗД, Endorsement 1/2018.

защита на личните данни по член 29 изясни критериите, които могат да помогнат да се установи кога за операциите по обработване се изисква ОВЗД. В насоките, с номер РД248 на Работната група за защита на личните данни по член 29 се посочва, че в повечето случаи администраторът на данни може да счете, че за обработване, което отговаря на два критерия, ще се изисква извършване на ОВЗД; в някои случаи обаче администраторът на данни може да счете, че ще се изисква ОВЗД за обработване, отговарящо само на един от тези критерии.

(5) Списъците, изготвяни от Европейския надзорен орган по защита на данните, спомагат за постигането на същата цел — да се установят операциите по обработване, за които съществува вероятност да породят висок риск, и операциите по обработване, за които поради наличието на такава вероятност се изисква извършването на ОВЗД. В този смисъл, критериите, разработени в насоките на работната група за защита на личните данни по член 29, остават релевантни.

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

1 КРАТКО ИЗЛОЖЕНИЕ НА ФАКТИТЕ

1. В приложение на член 39, параграф 4 от Регламент 2018/1725 Европейският надзорен орган по защита на данните представи своя проект на списък пред ЕКЗД на 18 март 2019 г. и представи преразгледана версия на 21 юни 2019 г.

2. Документът, представен от Европейския надзорен орган по защита на данните съдържа и част, свързана с член 39, параграф 5 от Регламент 2018/1725. В преработения проект на документа изрично се уточнява, че включеният в него списък по член 39, параграф 5 се прилага само за ситуации, в които институции или органи на Съюза са съвместни или единствени администратори. По-специално, проектът за списък по член 39, параграф 5 обхваща операциите, свързани с обработване от страна на институциите и органите на Съюза за целите на вътрешното им управление, извършвано без участието на администратори, различни от институциите и органите на Съюза.

3. Поради това, ЕКЗД констатира, че тази втора част на документа не попада в приложното поле на член 39, параграф 6 от Регламент 2018/1725. Тази разпоредба предвижда, че задължението да се поиска препоръка от ЕКЗД се прилага само спрямо онези елементи, които се отнасят до операции по обработване, при които администраторът съгласно Регламент 2018/1725 действа съвместно с един или повече администратори, които не са институции или органи на Съюза. Поради това, ЕКЗД няма да коментира тази част от проекта на документа.

2 ОЦЕНКА

2.1 Общи доводи на ЕКЗД във връзка с представения списък

4. Списъкът, представен на ЕКЗД, се тълкува като допълнително уточняване на член 39, параграф 1 от Регламент 2018/1725, който се ползва с предимство във всички случаи. Затова списъкът не следва да се счита за изчерпателен.

5. Комитетът взема под внимание член 39, параграф 10 от Регламент 2018/1725, който предвижда, че не се изисква ОВЗД, ако конкретната операция или набор от операции по обработване имат правно основание в правен акт, приет въз основа на Договорите, и когато оценката на

въздействието върху защитата на данните вече е била извършена като част от общата оценка на въздействието, предшестваща приемането на този правен акт. В този случай параграфи 1—6 от член 39 не се прилагат, освен ако във въпросния правен акт не е предвидено друго.

6. В настоящата препоръка по принцип не се разглеждат елементите, представени от Европейския надзорен орган по защита на данните, за които е счетено, че излизат извън приложното поле на член 39, параграф 6 от Регламент 2018/1725. Това се отнася до елементи, които не засягат обработката на данни, при която администраторът действа съвместно с един или повече администратори, които не са институции или органи на Съюза. Въпреки това, тъй като Европейският надзорен орган по защита на данните реши да приеме един списък за двата вида операции по обработване, настоящата препоръка де факто се прилага за двете категории дейности по обработване на данни.

7. Препоръката има за цел да осигури съответствие с основните операции по обработване, които Комитетът поиска да бъдат добавени от всички надзорни органи към техните списъци, ако те все още не са били добавени.

8. Това означава, че за ограничен брой операции по обработване, които ще бъдат определени по хармонизиран начин, Комитетът препоръчва на Европейския надзорен орган по защита на данните да изисква извършването на ОВЗД.

9. Когато в настоящата препоръка не се коментират някои от елементите от представения списък за ОВЗД, това означава, че Комитетът не изисква от Европейския надзорен орган по защита на данните да предприема по-нататъшни действия.

10. Накрая Комитетът припомня, че прозрачността е от основно значение за администраторите на данни и за лицата, обработващи данни. С цел елементите в списъка да бъдат по-ясни, Комитетът препоръчва в списъците да се добави изрично препращане за всеки вид обработване към критериите, определени в насоките, с оглед подобряване на прозрачността.

2.2 Анализ на проекта на списък

11. Като взема предвид, че:

а) съгласно член 39, параграф 1 от Регламент 2018/1725 се изисква извършване на ОВЗД, когато съществува вероятност дейността по обработването да породи висок риск за правата и свободите на физическите лица; както и

б) член 39, параграф 3 от Регламент 2018/1725 съдържа неизчерпателен списък на видовете обработване, за които се изисква ОВЗД,

Комитетът отправя следните препоръки:

Чувствителни данни

12. В проекта за списък като критерий са посочени „чувствителни данни“, както следва — „Чувствителни данни: данни, разкриващи етнически или расов произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, генетични данни, биометрични данни за уникално идентифициране на физическото лице, данни, свързани със здравето, сексуалния живот или сексуалната ориентация, наказателни присъди или

престъпления и свързани с тях мерки за сигурност, или които по друг начин се считат за чувствителни.“

13. Въпреки че текстът е много подобен на насоките за ОВЗД, съдържащи се в работния документ на Работната група по чл.29 WP248rev.01, одобрен от ЕКЗД, съществува значителна разлика. Докато в проекта за списък се използва формулировката „или които по друг начин се считат за чувствителни“, в насоките се говори за „данни от изключително лично естество“.

14. Комитетът отбелязва, че в нито един от членовете на ОРЗД не се използва терминът „чувствителни данни“, въпреки че той се споменава в 2 съображения; за този термин се счита, че указва единствено категориите данни, изброени в членове 9 и 10 от ОРЗД. За да се избегне объркване, Комитетът препоръчва на Европейския надзорен орган по защита на данните да измени формулировката „или които по друг начин се считат за чувствителни“ и да използва точната формулировка на насоките за ОВЗД.

Широкомащабно обработване

15. Комитетът отбелязва, че Европейският надзорен орган по защита на данните се позовава на вътрешен телефонен указател на институция на ЕС като контрапример за широкомащабно обработване. Без да се засяга това, дали ОВЗД е действително необходима, не е ясно защо телефонен указател на институция на ЕС сам по себе си не попада в обхвата на понятието за широкомащабно обработване, особено след като той по принцип може да включва лични данни на голям брой лица. ЕКЗД припомня освен това, че понятието „широкомащабен“ се отнася и за дела от съответното население, както е определен в насоките относно длъжностните лица по защита на данните („ДЛЗД“), приети през декември 2016 г., преразгледани на 5 април 2017 г. и одобрени от ЕКЗД. Комитетът препоръчва използването на различен пример.

Набори от данни, съчетани или комбинирани от различни операции по обработване на данни

16. Комитетът отбелязва, че примерът, използван за операциите по обработване, които включват набори от данни, съчетани или комбинирани от различни операции по обработване на данни, може да повдигне съмнения относно законосъобразността му съгласно Регламент 2018/1725, предвид начина, по който е описан. Въпреки че Комитетът не е в състояние да оцени тази законосъобразност и не разполага с компетенциите за това, той предлага, с цел постигане на по-голяма яснота, да се използва различен пример.

Уязвими субекти на данни

17. Комитетът отбелязва, че Европейският надзорен орган по защита на данните използва в решението си като контрапример служителите на институциите на ЕС *в съпоставка със* стандартните процедури, предвидени в Правилника за длъжностните лица. Комитетът припомня, че служителите са посочени като уязвими субекти на данни в насоките за ОВЗД, съдържащи се в документ WP248rev.01, одобрен от ЕКЗД. Въпреки че може да се спори дали дисбалансът на силите между работодател и нает лице е по-малък в контекста на „стандартните процедури“, предвидени в съответните разпоредби на Правилника, не може да се счита, че това винаги е така, особено когато наетите лица не оказват значително влияние върху съдържанието на посочените правила. Освен това не е ясно кои процедури

могат да се смятат за нестандартни, в който случай потенциално би било необходимо да се извърши ОВЗД, като това може да доведе до значително объркване. Поради тези причини Комитетът препоръчва Европейският надзорен орган по защита на данните да замени дадения контрапример с друг.

3 ЗАКЛЮЧЕНИЕ

18. Комитетът приканва Европейския надзорен орган по защита на данните да направи следните промени в своя списък:

- Относно чувствителните данни: Комитетът препоръчва на Европейския надзорен орган по защита на данните да измени своя списък като промени формулировката „или които по друг начин се считат за чувствителни“ и използва точната формулировка от насоките за ОВЗД;
- по отношение на широкомащабното обработване на данни: Комитетът препоръчва на Европейския надзорен орган по защита на данните да измени своя списък, като използва различен контрапример;
- по отношение на наборите от данни, съчетани или комбинирани от различни операции по обработване на данни: Комитетът препоръчва на Европейския надзорен орган по защита на данните да измени своя списък, като използва различен пример;
- по отношение на уязвимите субекти на данни: Комитетът препоръчва на Европейския надзорен орган по защита на данните да измени своя списък, като използва различен контрапример.

За Европейския комитет по защита на данните,

Председател

(Андреа Йелинек)