Препоръки 2/2021 относно правното основание за съхранението на данни за кредитна карта единствено с цел улесняване на по-нататъшни онлайн трансакции

Приети на 19 май 2021 г.

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 (по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство и по-конкретно приложение XI и протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.,

като взе предвид членове 12 и 22 от своя Правилник за дейността,

ПРИЕ СЛЕДНИТЕ ПРЕПОРЪКИ:

1. Цифровата икономика и електронната търговия продължиха да се развиват и при пандемията от COVID-19. Аналогично нараснаха рисковете при използване на данни за кредитни карти онлайн. Както е посочено в Насоките на Работната група по член 29 относно оценката на въздействието върху защитата на данни, нарушенията, свързани с данни за кредитни карти, *„очевидно биха довели до сериозно въздействие върху ежедневието на субекта на данни*“, тъй като финансовите данни могат да бъдат използвани за *„измами при плащания*“[1].

2. Поради тази причина е много важно администраторите на данни да въведат подходящите гаранции за субектите на данни и да им осигурят контрол върху собствените им лични данни, за да се намали рискът от незаконно обработване и да се насърчи доверие в цифровата среда. Европейският комитет по защита на данните счита, че това доверие е жизненоважно за устойчивия растеж на цифровата икономика.

3. За тази цел предназначението на настоящите препоръки е да се насърчи хармонизирано прилагане на правилата за защита на данните по отношение на обработването на данни за кредитни карти в рамките на Европейското икономическо пространство (ЕИП) и да се гарантира еднородна защита на правата на физическите лица при пълно зачитане на основните принципи за защита на данните, както се изисква от ОРЗД.

4. По-специално, в настоящите препоръки се разглежда съхранението на данни за кредитни карти от онлайн доставчици на стоки и услуги с единствената и конкретна цел да се улеснят по-нататъшни покупки от страна на субектите на данни[2]. В тях е обхванато положението, при което физическо лице купува продукт или плаща за услуга посредством уебсайт или

[1] РАБОТНА ГРУПА ПО ЧЛЕН 29 ЗА ЗАЩИТА НА ЛИЦАТА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ – Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679.

[2] Следва да се отбележи, че в препоръките не са обхванати платежните институции, които осъществяват дейност в онлайн магазини, нито публичните органи. Не е обхванато и съхранението на данни за кредитна карта за каквито и да е други цели, например спазване на правно задължение или създаване на повтарящо се плащане в случай на договор с автоматично подновяване или абонамент за дългосрочна услуга (например- договор, в който се предвижда доставката на определена стока всеки месец, или абонамент за услуга за поточно предаване на музика или филми).

приложение и по принцип предоставя данните на кредитната си карта в специален формуляр, за да извърши тази единична трансакция.

5. Както при всяко обработване, администраторът на данни трябва да има валидно правно основание съгласно член 6 от ОРЗД, за да съхранява тези данни. В това отношение следва да се отбележи, че няколко от посочените в член 6 от ОРЗД правни основания не биха били приложими в тази ситуация и трябва да бъдат изключени. Съхранението на данни за кредитна карта след трансакция с цел д се улеснят по-нататъшни покупки не може да се счита за необходимо за спазването на законово задължение (член 6, параграф 1, буква в) от ОРЗД), нито за да бъдат защитени жизненоважните интереси на физическо лице (член 6, параграф 1, буква г) от ОРЗД). За подходящо правно основание не може да се счита и изпълнението на задача от обществен интерес или упражняването на официални правомощия, които са предоставени на администратора (член 6, параграф 1, буква д) от ОРЗД).

6. Освен това, съхранението на данни за кредитна карта след плащането за стоки или услуги не е само по себе си необходимо за изпълнението на договор (член 6, параграф 1, буква б) от ОРЗД). Като се има предвид, че първоначално обработването на данните, свързани с кредитната карта, която е използвана от клиента за плащане, е необходимо за изпълнението на договора, при което се задейства член 6, параграф 1, буква б) от ОРЗД, съхранението на тези данни е полезно единствено с цел улесняване на потенциална следваща трансакция и на продажбите. Такава цел не може да се счита за строго необходима за изпълнението на договора за предоставяне на стоката или услугата, за която субектът на данните вече е платил[3].

7. По отношение на обработване, необходимо за целите на легитимните интереси на администратора или на трета страна[4], Европейският комитет по защита на данните отбелязва, че за да може администраторът да се позове на член 6, параграф 1, буква е) от ОРЗД, трябва да бъдат изпълнени трите условия, предвидени в този член[5]. Това правно основание изисква, на първо място, идентифициране и квалифициране на легитимен интерес, преследван от администратора или от трета страна. Интересът на администратора или третата страна може да бъде по-широк от целта на обработването и трябва да бъде възникнал и все още съществуващ към момента на обработването[6].

8. Свързаното с легитимните интереси правно основание изисква, на второ място, необходимост от обработване на лични данни за целите на преследвания легитимен

[3] Вж. също така документа на Европейския комитет по защита на данните „Насоки 2/2019 относно обработката на лични данни съгласно член 6, параграф 1, буква б) от ОРЗД при предоставянето на онлайн услуги на субектите на данни“, по-специално на стр. 10.

[4] Вж. становището на Работната група по член 29 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО, което е в процес на преразглеждане от Европейския комитет по защита на данните (вж. Работната програма на Европейския комитет по защита на данните за 2021/2022 г., приета на 16 март 2021 г.).

[5] Вж. Решение на Съда на ЕС от 4 май 2017 г. по дело C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde срещу Rīgas pašvaldības SIA „Rīgas satiksme“, ECLI:EU:C:2017:336, точка 28.

[6] Вж. Решение на Съда на ЕС от 11 декември 2019 г. по дело C-708/18, ТК срещу Asociaţia de Proprietari bloc M5A-ScaraA, ECLI:EU:C:2019:1064, точка 44.

интерес. При това положение, дори и администраторът да има легитимен интерес, както е посочено по-горе, не е очевидно, че съхранението на данни за кредитна карта с цел улесняване на бъдещи покупки е необходимо за преследване на този интерес. Всъщност, действителното извършване на друга покупка зависи от избора на потребителя и не се определя от възможността да я реализира „с едно натискане“.

9. Накрая, третото условие изисква да се извърши проверка на баланса: легитимният интерес на администратора или третата страна трябва да бъде претеглен спрямо интересите или основните права и свободи на субекта на данните, включително неговите права на защита на данните и неприкосновеност на личния живот. Тази проверка изисква да се вземат под внимание конкретните обстоятелства на обработването[7]. Съществен компонент при оценката на баланса е потенциалното въздействие на обработването на данни върху правата и свободите на физическите лица[8]. Това въздействие може да зависи от естеството на данните, конкретния начин на обработване и достъпа на трети страни до тези данни. По отношение на критерия, свързан с естеството на данните, следва да се отбележи, че финансовите данни са определени от Работната група по член 29 като данни от изключително лично естество, тъй като нарушенията във връзка с тях очевидно биха довели до сериозно въздействие върху ежедневието на субекта на данни[9]. Следователно, независимо от задължението на администратора на данни да прилага подходящи технически или организационни мерки, за да гарантира подходящо ниво на сигурност на данните за кредитни карти, съгласно член 5, параграф 1, буква е) от ОРЗД и факта, че тези данни може да бъдат съхранявани за други цели, тяхното обработване с цел улесняване на по-нататъшни покупки може да е свързано с повишен риск от нарушаване на сигурността, тъй като предполага обработване в други системи. Друг важен елемент на проверката, който би могъл да се вземе под внимание при оценката на въздействието на обработването върху субекта на данните, са основателните очаквания, които лицата имат в зависимост от взаимоотношенията с администратора на данни, същността и целта на събирането на лични данни[10]. При все това изглежда, че към момента на покупката при предоставяне на данни за извършване на плащане с кредитна карта, физическото лице няма основателни очаквания тази информация да бъде съхранявана за период, по-дълъг от необходимото за плащане на стоките или услугите, които купува в момента. Следователно, в тази ситуация, основните права и свободи на лицето, обект на защита на данни, вероятно имат предимство пред интереса на администратора на данните.

10. Тези аспекти водят до заключението, че съгласието (член 6, параграф 1, буква а) от ОРЗД) изглежда е единственото подходящо правно основание за законосъобразност на

[7] Вж. Решение на Съда на ЕС от 24 ноември 2011 г. по дела C-468/10 и C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) и Federación de Comercio Electrónico y Marketing Directo (FECEMD) срещу Administración del Estado, ECLI:EU:C:2011:777, точки 47 и 48; Решение на Съда на ЕС от 19 октомври 2016 г. по дело C-582/14, Patrick Breyer срещу Bundesrepublik Deutschland, ECLI:EU:C:2016:779, точка 62.

[8] Вж. горепосоченото Решение на Съда на ЕС от 24 ноември 2011 г., точка 44; горепосоченото Решение на Съда на ЕС от 11 декември 2019 г., точка 56.

[9] РАБОТНА ГРУПА ПО ЧЛЕН 29 ЗА ЗАЩИТА НА ЛИЦАТА ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ — Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679.

[10] Вж. съображение 47 от ОРЗД.

гореописаното обработване. В действителност, преди да се съхранят данните за кредитната карта следва да се получи изричното съгласие на субекта на данни, като се вземат предвид рисковете за сигурността, възможността на физическото лице да упражнява контрол върху тях и да взема активно решения за използването на данните за кредитната му карта. Това съгласие ще даде възможност на администратора на данните да докаже желанието на лицето да улесни по-нататъшните си покупки чрез конкретния уебсайт или приложение, което не може да бъде доказано само чрез извършването на една или няколко изолирани трансакции.

11. Не може да има презумпция за съгласие, то трябва да бъде свободно, конкретно, информирано и недвусмислено[11]. То трябва да бъде дадено чрез ясно утвърдително действие и следва да бъде поискано по лесен за потребителя начин, като например чрез поле за отметка, в което избора не може да бъде попълнен предварително[12], директно във формуляра, който се използва за събирането на данни. Това конкретно съгласие трябва да бъде разграничено от съгласието, което се дава за общите условия за услуги или продажби, и не следва да бъде условие за завършване на трансакцията.

12. Съгласно член 7, параграф 3 от ОРЗД субектът на данни има правото да оттегли по всяко време съгласието си за съхранение на данните за кредитната му карта за целите на улесняването на по-нататъшни покупки. Оттеглянето трябва да е свободно, опростено и толкова лесно за субекта на данните, колкото е било и даването на съгласието. То трябва да води до действително заличаване на данните за кредитната карта, съхранени от администратора на данни с единствената цел да се улесняват по-нататъшни покупки.

За Европейския комитет по защита на данните

Председател

(Andrea Jelinek)

[11] Вж. документа на Европейския комитет по защита на данните „Насоки 5/2020 относно съгласието в съответствие с Регламент 2016/679“.
[12] *Пак там*.