Насоки 6/2020 относно взаимодействието между Втората директива за платежните услуги и ОРЗД

Версия 2.0

Приети на 15 декември 2020 г.

История на версиите

Версия 2.0	15 декември 2020 г.	Приемане на Насоките след обществена консултация
Версия 1.0	17 юли 2020 г.	Приемане на Насоките за подлагане на обществена консултация

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 Споразумението за ЕИП, и по-специално приложение XI и протокол 37 към него, както са изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.[1],

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

като има предвид, че:

(1) В Общия регламент относно защитата на данните е предвиден съгласуван набор от правила относно обработването на лични данни в целия ЕС.

(2) С Втората директива за платежните услуги (Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 23 декември 2015 г., наричана по-нататък (ДПУ2) е отменена Директива 2007/64/ЕО и са предвидени нови правила, за да се осигури правна яснота за потребителите, търговците и дружествата в рамките на платежната верига, както и да се осъвремени правната уредба за пазара на платежни услуги[2]. Държавите членки трябваше да транспонират ДПУ2 в своето национално право преди 13 януари 2018 г.

(3) Важна характеристика на ДПУ2 е въвеждането на правна уредба за нови услуги по иницииране на плащане и услуги по предоставяне на информация за сметка. Чрез Директивата се позволява на тези доставчици на нови платежни услуги да получат достъп до платежни сметки на субекти на данни с цел предоставяне на посочените услуги.

(4) Що се отнася до защитата на данните, в съответствие с член 94, параграф 1 от ДПУ2 обработването на лични данни, включително предоставянето на информация относно обработването на данни за целите на ДПУ2, се извършва в съответствие с ОРЗД[3] и с Регламент (ЕС) 2018/1725.

(5) В съображение 89 от ДПУ2 е посочено, че когато за целите на Директивата се обработват лични данни, следва да се определи точната цел, да се посочи съответното правно основание, да се спазват приложимите изисквания за сигурност, установени с ОРЗД, както и да се зачитат принципите на необходимост, пропорционалност, ограничаване в рамките на целта и да се спазва пропорционален срок за запазване на данните. Принципите за защита на данните на етапа на проектирането и по подразбиране следва да са заложени във всички системи за обработване на данни, които се разработват и използват в рамките на ДПУ2[4].

[1] Посочването на „държави членки“ в настоящия документ следва да се разбира като посочване на „държавите — членки на ЕИП“.
[2] Съображение 6 от ДПУ2.
[3] Тъй като ДПУ2 предхожда ОРЗД, в нея все още се прави позоваване на Директива 95/46/ЕО. В член 94 от ОРЗД е посочено, че позоваванията на отменената Директива 95/46/ЕО се тълкуват като позовавания на ОРЗД.
[4] Съображение 89 от ДПУ2.

(6) В съображение 93 от ДПУ2 е посочено, че доставчиците на услуги по иницииране на плащане и доставчиците на услуги по предоставяне на информация за сметка, от една страна, и доставчикът на платежни услуги, обслужващ сметка, от друга страна, следва да спазват необходимите изисквания за защита на данните и изисквания за сигурност, предвидени или посочени в тази директива или включени в регулаторните технически стандарти.

ПРИЕ СЛЕДНИТЕ НАСОКИ:

1. ВЪВЕДЕНИЕ

1. С Втората директива за платежните услуги (наричана по-нататък ДПУ2) са въведени редица новости в областта на платежните услуги. Въпреки че благодарение на нея се създават нови възможности за потребителите и се подобрява прозрачността в тази област, прилагането на ДПУ2 повдига определени въпроси и пораждат опасения, свързани с необходимостта субектите на данни да запазят пълен контрол върху своите лични данни. Общият регламент относно защитата на данните (наричан по-нататък ОРЗД) се прилага за обработването на лични данни, включително дейностите по обработване, извършвани във връзка с предлагането на платежните услуги съгласно определението в ДПУ2[5]. Съответно администраторите, които извършват дейност в областта, обхваната от ДПУ2, трябва винаги да гарантират съответствие с изискванията на ОРЗД, включително принципите за защита на данните, определени в член 5 от ОРЗД, както и съответните разпоредби на Директивата за правото на неприкосновеност на личния живот и електронни комуникации[6]. Въпреки че ДПУ2[7] и регулаторните технически стандарти за задълбоченото установяване на идентичността на клиента и общите, и сигурни отворени стандарти на комуникация (наричани по-нататък РТС[8]) съдържат определени разпоредби, свързани със защитата и сигурността на данните, възникна несигурност относно тълкуването на тези разпоредби, както и относно взаимодействието между общата уредба за защита на данните и ДПУ2.

2. На 5 юли 2018 г. Европейският комитет по защита на данните (ЕКЗД) публикува писмо относно ДПУ2, в което представи разяснения по въпроси за защитата на личните данни във връзка с ДПУ2, по-специално относно обработването на лични данни на недоговарящи страни (т.нар. „данни на пасивната страна“) от страна на доставчици на услуги по предоставяне на информация за сметка (наричани по-нататък ДУПИС) и доставчици на услуги по иницииране на плащане (наричани по-нататък ДУИП), процедурите, свързани с даването и оттеглянето на съгласие, РТС и сътрудничеството между доставчиците на платежни услуги, обслужващи сметка (наричани по-нататък ДПУОС), във връзка с мерките за сигурност. От

[5] Член 1, параграф 1 от ОРЗД.

[6] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37—47).

[7] Член 94 от ДПУ2 и т.н.

[8] Делегиран регламент (ЕС) 2018/389 на Комисията от 27 ноември 2017 г. за допълнение на Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти за задълбоченото установяване на идентичността на клиента и общите и сигурни отворени стандарти на комуникация (текст от значение за ЕИП) (C(2017) 7782; ОВ L 69, 13.3.2018 г., стр. 23—43), на разположение на адрес https://eur-lex.europa.eu/legal-content/bg/TXT/PDF/?uri=CELEX:32018R0389&from=EN.

друга страна, подготвителната работа по настоящите насоки включваше събирането на мнения от заинтересованите страни както в писмена форма, така и на проява с участието на заинтересовани страни, за да бъдат установени най-неотложните предизвикателства.

3. Настоящите насоки имат за цел даването на допълнителни указания относно аспектите на защитата на данните в контекста на ДПУ2, по-специално относно връзката между съответните разпоредби на ОРЗД и ДПУ2. Основният акцент на настоящите насоки е върху обработването на лични данни от страна на ДУПИС и на ДУИП. Поради това в настоящия документ са разгледани условията за предоставяне на достъп до информация за платежна сметка от страна на ДПУОС и за обработването на лични данни от страна на ДУИП и ДУПИС, включително изискванията и гаранциите във връзка с обработването на лични данни от страна на ДУИП и ДУПИС за цели, различни от първоначалните, за които са събрани данните, особено когато такива са събрани във връзка с предоставянето на услуга по предоставяне на информация за сметка[9]. В настоящия документ също така са разгледани различните понятия за изрично съгласие в съответствие с ДПУ2 и ОРЗД, обработването на „данни на мълчалива страна“, обработването на специални категории лични данни от страна на ДУИП и ДУПИС, прилагането на основните принципи за защита на данните, описани в ОРЗД, включително свеждането на данните до минимум, прозрачността, отчетността и мерките за сигурност. В ДПУ2 са включени многофункционалните задължения в областите, *inter alia*, на потребителското и конкурентното право. Съображенията, свързани с тези области на правото, са извън обхвата на настоящите насоки.

4. За да се улесни четенето на насоките, по-долу са предоставени основните определения, използвани в настоящия документ.

1.1 Определения

„Доставчик на услуги по предоставяне на информация за сметка“ (ДУПИС) означава доставчик на онлайн услуга, при която се предоставя обобщена информация за една или повече платежни сметки, държани от ползвателя на платежни услуги при друг доставчик на платежни услуги, или при повече от един доставчик на платежни услуги;

„доставчик на платежни услуги, обслужващ сметка“ (ДПУОС) означава доставчик на платежни услуги, предлагащ и поддържащ платежни сметки за даден платец*;*

„свеждане на данните до минимум“ е принцип на защита на данните, съгласно който личните данни следва да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват;

„платец“ означава физическо или юридическо лице, което е титуляр на платежна сметка и разрешава изпълнението на платежно нареждане по тази сметка или, когато липсва платежна сметка, физическо или юридическо лице, което дава платежно нареждане;

„получател“ означава физическо или юридическо лице, определено за краен получател на средствата, които са предмет на платежна операция*;*

„платежна сметка“ означава сметка, водена на името на един или повече ползватели на платежни услуги и използвана за изпълнението на платежни операции;

[9] Услугата по предоставяне на информация за сметка е онлайн услуга, при която се предоставя обобщена информация за една или повече платежни сметки, държани от ползвателя на платежните услуги или при друг доставчик на тези услуги, или при повече от един доставчик на платежни услуги.

„доставчик на услуги по иницииране на плащане“ (ДУИП) означава доставчик на услуга по иницииране на плащане, при която се инициира платежно нареждане по искане на ползвателя на платежни услуги по отношение на платежна сметка, държана при друг доставчик на платежни услуги;

„доставчик на платежни услуги“ означава орган по член 1, параграф 1 от ДПУ2[10] или физическо, или юридическо лице, което се ползва от освобождаване по член 32 или 33 от ДПУ2;

„ползвател на платежни услуги“ означава физическо или юридическо лице, което се ползва от платежна услуга в качеството си на платец или на получател, или и в двете качества;

„лични данни“ означава всякаква информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социалната идентичност на това физическо лице;

„защита на данните на етапа на проектирането“ означава технически и организационни мерки, заложени в продукт или услуга, които са разработени с оглед на ефективното прилагане на принципите на защита на данните и интегриране на необходимите гаранции в процеса на обработване, за да се спазят изискванията на ОРЗД и да се осигури защита на правата на субектите на данни;

„защита на данните по подразбиране“ означава прилагане на подходящи технически и организационни мерки във връзка с продукт или услуга, с които се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването;

„регулаторни технически стандарти“ (РТС) се отнася до Делегиран регламент (ЕС) 2018/389 на Комисията от 27 ноември 2017 г. за допълнение на Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти за задълбоченото

[10] Член 1, параграф 1 от ДПУ2 гласи, че с ДПУ2 се установяват правилата, в съответствие с които държавите членки могат да направят разграничение между следните шест категории *доставчици на платежни услуги*:
а) кредитните институции съгласно определението в член 4, параграф 1, точка 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета (1), включително техните клонове по смисъла на член 4, параграф 1, точка 17 от същия регламент, когато тези клонове са разположени на територията на Съюза, независимо дали главното управление на тези клонове е в Съюза или — в съответствие с член 47 от Директива 2013/36/ЕС и националното право — извън Съюза;
б) институциите за електронни пари по смисъла на член 2, точка 1 от Директива 2009/110/ЕО, включително — в съответствие с член 8 от същата директива и с националното право — техните клонове, когато тези клонове са разположени в Съюза, а главното им управление е извън Съюза, доколкото предоставяните от тези клонове платежни услуги са свързани с издаването на електронни пари;
в) пощенските джиро институции, които съгласно националното право имат право да предоставят платежни услуги;
г) платежните институции;
д) ЕЦБ и националните централни банки, когато не действат в качеството си на органи на паричната политика или на други публични органи;
е) държавите членки или техните регионални или местни органи, когато не действат в качеството си на публични органи.

установяване на идентичността на клиента и общите и сигурни отворени стандарти на комуникация;

„доставчик трета страна“ (ДТС) означава както ДУИП, така и ДУПИС.

1.2 Услуги съгласно ДПУ2

5. С ДПУ2 се въвеждат два нови вида (доставчици на) платежни услуги: ДУИП и ДУПИС. В приложение I към ДПУ2 са изброени осемте платежни услуги, които са обхванати от ДПУ2.

6. ДУИП предоставят услуги по иницииране на плащане, при които се издава платежно нареждане по искане на ползвателя на платежни услуги по отношение на платежна сметка на ползвател, съхранявана при друг доставчик на платежни услуги[11]. ДУИП може да се обърне с искане към ДПУОС (обикновено това е банка) и да започне платежна операция от името на ползвателя на платежни услуги. Ползвателят (на платежни услуги) може да бъде физическо лице (субект на данни) или юридическо лице.

7. ДУПИС предлагат онлайн услуги за предоставяне на обобщена информация за една или повече платежни сметки, съхранявани от ползвателя на платежните услуги или при друг доставчик на платежни услуги, или при повече от един доставчик на платежни услуги[12]. Съгласно съображение 28 от ДПУ2 ползвателят на платежни услуги има възможност да получи незабавно цялостна представа за финансовото си положение във всеки един момент.

8. Когато става въпрос за услуги по предоставяне на информация за сметка, биха могли да се предлагат няколко различни вида услуги, като акцентът е върху различни характеристики и цели. Някои доставчици например могат да предлагат на ползвателите услуги като планиране на бюджета и наблюдение на плащанията. Обработването на лични данни в контекста на тези услуги попада в обхвата на ДПУ2. Услугите, които са свързани с оценка на кредитоспособността на ползвателя на платежни услуги, или одиторски услуги, извършвани въз основа на събиране на информация чрез услуга по предоставяне на информация за сметка, попадат извън обхвата на ДПУ2 и съответно са обхванати от ОРЗД. Освен това сметки, различни от платежни сметки (например спестовни, инвестиционни), също не попадат в обхвата на ДПУ2.Най-общо, ОРЗД е приложимата правна уредба за обработването на лични данни.

Пример 1:

HappyPayments е дружество, което предлага онлайн услуга, състояща се в предоставянето на информация за една или повече платежни сметки чрез мобилно приложение с цел осигуряване на финансов надзор (услуга по предоставяне на информация за сметка). Чрез тази услуга ползвателят на платежни услуги може да следи, с един поглед, последните операции и салдото по две или повече платежни сметки в различни банки. Чрез нея по желание на ползвателя на платежни услуги се предлага също така категоризация на плащанията и постъпленията по различни типове (заплата, свободно време, енергия, ипотечен кредит и др.), като по този начин на ползвателя на платежни услуги се оказва помощ с финансовото планиране. С това приложение HappyPayments предлага също така услуга по иницииране на плащане директно от определена платежна сметка или определени платежни сметки на ползвателите (услуга по иницииране на плащане).

[11] Член 4, точка 15 от ДПУ2.
[12] Член 4, точка 16 от ДПУ2.

9. Предлагането на такива услуги е урегулирано с ДПУ2, където са регламентирани законовите условия, при които ДУИП и ДУПИС могат да имат достъп до платежните сметки, за да предоставят услуга на ползвателя на платежни услуги.

10. В член 66, параграф 1 и член 67, параграф 1 от ДПУ2 е определено, че ползвателят на платежни услуги има право на достъп и право на използване на платежни услуги и услуги по предоставяне на информация за сметка. Това означава, че ползвателят на платежни услуги следва да запази пълна свобода от отношение на упражняването на това право и не може да бъде принуждаван да се възползва от това право.

11. Достъпът до платежни сметки и използването на информацията за платежна сметка са регламентирани отчасти в членове 66 и 67 от ДПУ2, в които се съдържат гаранции във връзка със защитата на (личните) данни. В член 66, параграф 3, буква е) от ДПУ2 е посочено, че ДУИП не изисква от ползвателя на платежни услуги никакви други данни освен необходимите за предоставяне на услугата по иницииране на плащане, а в член 66, параграф 3, буква ж) от ДПУ2 е предвидено, че ДУИП не използват, не осъществяват достъп до данни нито съхраняват такива данни за цели, различни от изпълнението на услугата по иницииране на плащане, която изрично е поискана от ползвателя на платежни услуги. Освен това в член 67, параграф 2, буква г) от ДПУ2 достъпът на ДУПИС е ограничен само до информация от определени платежни сметки и свързаните с тях платежни операции, а в член 67, параграф 2, буква е) от ДПУ2 е предвидено, че ДУПИС не използва, не осъществява достъп до данни, нито съхранява такива данни за цели, различни от изпълнението на услугата по предоставяне на информация за сметка, която ползвателят на платежни услуги изрично е поискал, в съответствие с правилата за защита на данните. В последната разпоредба се подчертава, че във връзка с услугите по предоставяне на информация за сметка, лични данни могат да се събират единствено за конкретни, изрично указани и легитимни цели. Следователно, ДУПИС следва изрично да посочва в договора, за какви конкретни цели ще бъдат обработвани личните данни относно сметката в контекста на предлаганата от него услуга по предоставяне на информация за сметка. Договорът следва да бъде законосъобразен, съставен добросъвестно и прозрачно съгласно член 5 от ОРЗД и също така да съответства на останалите нормативни актове в областта на защитата на потребителите.

12. В зависимост от конкретните обстоятелства доставчиците на платежни услуги биха могли да изпълняват ролята на администратор или на обработващ лични данни съгласно ОРЗД. В контекста на настоящите насоки „администратори“ са онези доставчици на платежни услуги, които самостоятелно или съвместно с други определят целите и средствата за обработването на лични данни. Допълнителни указания по този въпрос могат да бъдат намерени в Насоки 7/2020 на ЕКЗД относно концепциите за администратор и обработващ лични данни съгласно ОРЗД.

2 ЗАКОННИ ОСНОВАНИЯ И ПО-НАТАТЪШНО ОБРАБОТВАНЕ СЪГЛАСНО ДПУ2

2.1 Законни основания за обработване

13. Съгласно ОРЗД администраторите трябва да имат правно основание, за да обработват лични данни. Разпоредбата на член 6, параграф 1 от ОРЗД съставлява изчерпателен и ограничителен списък на шест правни основания за обработване на лични данни съгласно същия регламент[13]. Администраторът определя подходящото правно основание и гарантира, че всички условия за това правно основание са спазени. Определянето на това кое основание е валидно и най-подходящо в конкретна ситуация зависи от обстоятелствата, при които се извършва обработването, включително целта на обработването и отношението между администратора и субекта на данни.

2.2 Член 6, параграф 1, буква б) от ОРЗД (обработването е необходимо за изпълнението на договор)

14. Платежните услуги се предоставят на договорна основа между ползвателя на платежни услуги и доставчика на платежни услуги. Както е посочено в съображение 87 от ДПУ2, „*настоящата директива следва да се отнася само за договорни задължения и отговорности между ползвателя на платежни услуги и доставчика на платежни услуги*“. По отношение на ОРЗД основното правно основание за обработването на лични данни за целите на предоставянето на платежни услуги е член 6, параграф 1, буква б) от ОРЗД, където се посочва, че обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данни преди сключването на договор.

15. Определения на платежните услуги съгласно ДПУ2 са дадени в приложение I към ДПУ2. Предоставянето на тези услуги, както са определени в ДПУ2, е необходимо изискване за сключването на договор, по който страните имат достъп до данни за платежни сметки на ползвателя на платежни услуги. Тези доставчици на платежни услуги трябва също така да

[13] Съгласно член 6 обработването е законосъобразно само ако и доколкото е приложимо поне едно от следните условия:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на правно задължение, което се прилага спрямо администратора;

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

е) обработването е необходимо за целите на законните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

бъдат лицензирани оператори. По отношение на услугите по иницииране на плащане и услугите по предоставяне на информация за сметка съгласно ДПУ2 в договорите може да се съдържат клаузи, с които се налагат условия и за допълнителни услуги, които не попадат в обхвата на ДПУ2. В *Насоки 2/2019 на ЕКЗД относно обработката на лични данни съгласно член 6, параграф 1, буква б) от Общия регламент относно защита на данните при предоставянето на онлайн услуги на субектите на данни* ясно се посочва, че администраторите трябва да преценяват какъв вид обработване на лични данни е обективно необходимо за изпълнението на договора. В тези насоки се изтъква, че обосновката на необходимостта зависи от характера на услугата, гледните точки и очакванията на страните по договора, обосновката на договора и неговите основни елементи.

16. В Насоки 2/2019 на ЕКЗД също така се пояснява, че съгласно член 7, параграф 4 от ОРЗД се прави разграничение между дейностите по обработване, необходими за изпълнението на даден договор, и клаузите, съгласно които предоставянето на услугата зависи от определени дейности по обработване, които всъщност не са необходими за изпълнението на договора. Изразът „необходими за изпълнението“ очевидно изисква нещо повече от договорно условие[14]. Администраторът следва да е в състояние да демонстрира, че основният предмет на конкретния договор със субекта на данни не може реално да бъде изпълнен, ако не се извърши въпросното конкретно обработване на лични данни. Позоваването или споменаването в договора на обработване на лични данни само по себе си не е достатъчно, за да се счита, че въпросното обработване попада в обхвата на член 6, параграф 1, буква б) от ОРЗД.

17. В член 5, параграф 1, буква б) от ОРЗД е заложен принципът на ограничаване в рамките на целта, според който се изисква личните данни да се събират за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, несъвместим с тези цели. При преценката дали член 6, параграф 1, буква б) е подходящо правно основание за онлайн (платежна) услуга трябва да се вземе предвид конкретната цел или предназначение на услугата[15]. Целите на обработването трябва да бъдат ясно посочени и съобщени на субекта на данни в съответствие със задълженията на администратора за ограничаване в рамките на целта и за прозрачност. Оценката на това, което е „необходимо“, включва комбинирана, основана на факти оценка на обработването „за преследваната цел и за това дали тя представлява по-малко вмешателство в сравнение с други възможности за постигане на същата цел“. Член 6, параграф 1, буква б) не обхваща обработване, което е полезно, но не е обективно необходимо за изпълнението на договорните услуги или за предприемане на съответните стъпки преди сключване на договора по искане на субекта на данни, дори и това да е необходимо за другите бизнес цели на администратора[16].

18. В Насоки 2/2019 на ЕКЗД ясно е посочено, че чрез договорите не може изкуствено да се разширяват категориите лични данни или видовете операции по обработване, които администраторът трябва да извърши за изпълнението на договора по смисъла на член 6, параграф 1, буква б)[17]. В тези насоки са разгледани също така случаи, при които могат да възникнат ситуации тип „приемате или отказвате“ за субектите на данни, които може да се

[14] Насоки 2/2019 относно обработката на лични данни съгласно член 6, параграф 1, буква б) от Общия регламент относно защита на данните при предоставянето на онлайн услуги на субектите на данни, ЕКЗД, точка 8.
[15] Пак там.
[16] Пак там, стр. 9.
[17] Пак там, стр. 11.

интересуват от само една от услугите. Това може да се случи, когато администраторът желае да обедини в пакет няколко отделни услуги или елементи на услуга с различни основни цели, характеристики или обосновка. Когато договорът се състои от няколко отделни услуги или елементи на услуга, които на практика могат да бъдат изпълнени независимо едни от други, приложимостта на член 6, параграф 1, буква б) следва да бъде оценена като се вземе предвид всяка от тези услуги поотделно и се прецени това, което е обективно необходимо за изпълнението на всяка една от отделните услуги, които субектът на данни активно е поискал или за които се е регистрирал[18].

19. В съответствие с горепосочените насоки администраторите трябва да преценят какво е обективно необходимо за изпълнението на договора. Когато администраторите не могат да докажат, че обработването на личните данни във връзка с платежна сметка е обективно необходимо за предоставянето на всяка от тези услуги поотделно, член 6, параграф 1, буква б) от ОРЗД не е валидно правно основание за обработване. В тези случаи администраторът следва да потърси друго правно основание за обработване.

2.3 Предотвратяване на измами

20. Член 94, параграф 1 от ДПУ2 гласи, че държавите членки разрешават обработването на лични данни от платежни системи и доставчици на платежни услуги, когато това е необходимо за осигуряване на предотвратяването, разследването и разкриването на измами при плащания. Обработването на лични данни, строго необходимо за целите на предотвратяването на измами, би могло да представлява законен интерес на съответния доставчик на платежни услуги, при условие че пред тези интереси нямат преимущество интересите или основните права и свободи на субекта на данни[19]. Дейностите по обработване за целите на предотвратяването на измами следва да се основават на внимателна оценка на всеки отделен случай от страна на администратора в съответствие с принципа на отчетност. Освен това за целите на предотвратяването на измами администраторите може също така да бъдат обект на специфични правни задължения, които налагат обработването на лични данни.

2.4 По-нататъшно обработване (ДУПИС и ДУИП)

21. В член 6, параграф 4 от ОРЗД са определени условията за обработване на лични данни за цели, различни от онези, за които са били събрани личните данни. По-конкретно такова по-нататъшно обработване може да се извършва, когато то се основава на правото на Съюза или на държава членка, която представлява необходима и пропорционална мярка в едно демократично общество за гарантиране на целите по член 23, параграф 1, когато субектът на данни е дал своето съгласие или когато обработването за други цели, различни от онези, за които са били събрани личните данни, е съвместимо с първоначалната цел.

22. Следва внимателно да се вземат предвид член 66, параграф 3, буква ж) и член 67, параграф 2, буква е) от ДПУ2. Както е споменато по-горе, в член 66, параграф 3, буква ж) от ДПУ2 се посочва, че ДУИП не използва, не осъществява достъп до данни нито съхранява такива данни за цели, различни от изпълнението на услугата по иницииране на плащане, която ползвателят на платежни услуги изрично е поискал. В член 67, параграф 2, буква е) от ДПУ2 се посочва, че ДУПИС не използва, не осъществява достъп до данни нито съхранява такива данни за цели, различни от изпълнението на услугата по предоставяне на информация за

[18] Пак там, стр. 12.
[19] Съображение 47 от ОРЗД.

сметка, която ползвателят на платежни услуги изрично е поискал, в съответствие с правилата за защита на данните.

23. Следователно разпоредбите на член 66, параграф 3, буква ж) и член 67, параграф 2, буква е) от ДПУ2 значително ограничават възможностите за обработване за други цели, което означава, че обработването за друга цел не е позволено, освен ако субектът на данни е дал съгласие в съответствие с член 6, параграф 1, буква а) от ОРЗД или обработването е предвидено в правото на Съюза или на държава членка, което се прилага спрямо администратора, съгласно член 6, параграф 4 от ОРЗД. Когато обработването за цели, различни от онези, за които са били събрани личните данни, не се основава на съгласието на субекта на данни или на правото на Съюза или на държава членка, ограниченията, установени в член 66, параграф 3, буква ж) и в член 67, параграф 2, буква е) от ДПУ2 ясно показват, че всяка друга цел не е съвместима с целта, за която първоначално са събрани личните данни. Проверката за съвместимост по член 6, параграф 4 от ОРЗД не може да доведе до определяне на правно основание за обработване.

24. Чрез член 6, параграф 4 от ОРЗД се дава възможност за по-нататъшно обработване въз основа на правото на Съюза или на държава членка. Така например, всички ДУИП и ДУПИС са задължени субекти съгласно член 3, параграф 2, буква а) от Директива (ЕС) 2015/849 на Европейския парламент и на Съвета от 20 май 2015 г. за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма (Директива относно борбата с изпирането на пари и финансирането на тероризма). Следователно тези задължени субекти са длъжни да прилагат мерките за комплексна проверка на клиента, както е уточнено в посочената директива. Съответно личните данни, обработвани във връзка с услуга в обхвата на ДПУ2, се обработват по-нататък въз основа на поне едно правно задължение, вменено на доставчика на услуги[20].

25. Както е споменато в параграф 20, в член 6, параграф 4 от ОРЗД се посочва, че обработването за цели, различни от онези, за които са били събрани личните данни, може да се основава на съгласието на субекта на данните, ако са изпълнени всички условия за съгласие по ОРЗД. Както е изложено по-горе, администраторът трябва да докаже, че субектът на данни е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него (съображение 42 от ОРЗД).

2.5 Законни основания за предоставяне на достъп до сметката (ДПУОС)

26. Както е споменато в точка 10, ползвателите на платежни услуги могат да упражняват правото си да използват услуги по иницииране на плащане и услуги по предоставяне на информация за сметка. Задълженията, наложени на държавите членки с член 66, параграф 1 и член 67, параграф 1 от ДПУ2, следва да се приложат в националното законодателство с оглед да се гарантира действителното упражняване на правото на ползвателя на платежни услуги да се ползва от гореспоменатите платежни услуги. Действителното упражняване на такива права не би било възможно, ако не съществува паралелно задължение на ДПУОС — обикновено банка, да предоставя на доставчика на платежни услуги достъп до сметката, при условие че доставчикът е удовлетворил всички изисквания за получаване на достъп до сметката на ползвателя на платежни услуги. В допълнение в член 66, параграф 5 и член 67, параграф 4 от ДПУ2 ясно е определено, че предоставянето на услуги по иницииране на плащане и на услуги

[20] Следва да се обърне внимание, че задълбоченият анализ на въпроса дали Директивата относно борбата с изпирането на пари и финансирането на тероризма отговаря на стандарта на член 6, параграф 4 от ОРЗД попада извън обхвата на настоящия документ.

по предоставяне на информация за сметка не трябва да е обусловено от съществуването на договорно правоотношение между ДУИП/ДУПИС и ДПУОС.

27. Обработването на лични данни от ДПУОС, състоящо се в предоставянето на достъп до личните данни, поискани от ДУИП и ДУПИС с цел да предоставят своята платежна услуга на ползвателя на платежни услуги, се основава на правно задължение. За да бъдат постигнати целите на ДПУ2, ДПУОС трябва да предоставят личните данни за целите на услугите на ДУИП и ДУПИС, което е необходимо условие, за да могат ДУИП и ДУПИС да предоставят своите услуги и по този начин да гарантират упражняване на правата, предвидени в член 66, параграф 1 и член 67, параграф 1 от ДПУ2. Следователно приложимото правно основание в този случай е член 6, параграф 1, буква в) от ОРЗД.

28. Тъй като в ОРЗД е уточнено, че обработването въз основа на правно задължение следва да бъде ясно установено в правото на Съюза или на държава членка (вж. член 6, параграф 3 от ОРЗД), задължението на ДПУОС да предоставят достъп следва да произтича от националното законодателство, което се транспонира ДПУ2.

3 ИЗРИЧНО СЪГЛАСИЕ

3.1 Съгласие в съответствие с ОРЗД

29. В съответствие с ОРЗД съгласието служи като едно от шестте правни основания за законосъобразност на обработването на лични данни. В член 4, точка 11 от ОРЗД съгласието е определено като „всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени“. Тези четири условия — съгласието да бъде свободно изразено, конкретно, информирано и недвусмислено — са от съществено значение за неговата валидност. Съгласно Насоки 5/2020 на ЕКЗД относно съгласието в съответствие с Регламент 2016/679, съгласието може да бъде подходящо правно основание само ако на субекта на данни са предложени контрол и възможност за реален избор по отношение на приемането или отхвърлянето на предлаганите условия, или отхвърлянето им, без това да доведе до вредни последици за него. Когато иска съгласие, администраторът е длъжен да прецени дали то ще отговаря на всички изисквания за получаване на валидно съгласие. Ако е получено в пълно съответствие с ОРЗД, съгласието представлява инструмент, чрез който субектът на данни може да контролира това дали неговите лични данни ще бъдат или няма да бъдат обработвани. В противен случай контролът от страна на субекта на данни става илюзорен, а съгласието ще бъде невалидно правно основание за обработването, което от своя страна ще направи дейността по обработването незаконосъобразна[21].

30. ОРЗД съдържа също така допълнителни гаранции в член 7, в който е предвидено, че администраторът на данни трябва да може да докаже, че към момента на обработването е имало валидно съгласие. Също така искането за съгласие трябва да се представя по начин, който ясно да го отличава от другите въпроси, в разбираема и лесно достъпна форма, като се използва ясен и прост език. Освен това субектът на данни трябва да бъде информиран за правото да оттегли съгласието си по всяко време също толкова лесно, колкото го е дал.

31. В съответствие с член 9 от ОРЗД съгласието е едно от изключенията от общата забрана за обработване на специални категории лични данни. В такива случаи обаче съгласието на субекта на данни трябва да бъде „изрично“[22].

32. В съответствие с Насоки 5/2020 на ЕКЗД относно съгласието в съответствие с Регламент 2016/679 изричното съгласие се отнася до начина, по който е изразено съгласието от субекта на данни. Това означава, че субектът на данни трябва да направи изрично изявление, указващо съгласие, за конкретна цел или конкретни цели на обработването. Ясен начин да се гарантира, че съгласието е изрично, би било изричното потвърждаване на съгласието в писмена декларация. Когато е подходящо, администраторът може да се увери, че писмената декларация е подписана от субекта на данни, за да бъде предотвратено в бъдеще всяко възможно съмнение, както и потенциалната липса на доказателства.

33. При никакви обстоятелства заключение за дадено съгласие не може да се извлече от потенциално двусмислени изявления или действия. Администраторът трябва също така да

[21] Насоки 5/2020 относно съгласието в съответствие с Регламент 2016/679, ЕКЗД, точка 3.

[22] Вж. също Становище 15/2011 относно понятието „съгласие“ (WP 187), стр. 6—8, и/или Становище 6/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО (WP 217), стр. 9, 10, 13 и 14.

има предвид, че съгласието не може да се получава чрез същото действие, с което се приема договор или се приемат общите условия за дадена услуга.

3.2 Съгласие в съответствие с ДПУ2

34. Европейският комитет по защита на данните отбелязва, че правната уредба относно изричното съгласие е сложна, тъй като както ДПУ2, така и ОРЗД включват понятието „изрично съгласие“. Това води до въпроса дали „изричното съгласие“, посочено в член 94, параграф 2 от ДПУ2, следва да се тълкува по същия начин като изричното съгласие в съответствие с ОРЗД.

3.2.1 Изрично съгласие в съответствие с член 94, параграф 2 от ДПУ2

35. В ДПУ2 са включени редица различни специални правила относно обработването на лични данни, по-конкретно в член 94, параграф 1 от ДПУ2, в който е определено, че обработването на лични данни за целите на ДПУ2 трябва да съответства на законодателството на ЕС в областта на защитата на данните. Освен това в член 94, параграф 2 от ДПУ2 е посочено, че доставчиците на платежни услуги осъществяват достъп до личните данни, необходими за предоставяне на техните платежни услуги, и ги обработват и запазват само с изричното съгласие на ползвателя на платежни услуги. В съответствие с член 33, параграф 2 от ДПУ2 това изискване за изрично съгласие на ползвателя на платежни услуги не се прилага за ДУПИС. В член 67, параграф 2, буква а) от ДПУ2 обаче все пак се предвижда изрично съгласие за ДУПИС, за да предоставят услугата.

36. Както беше посочено по-горе, списъкът с правни основания за обработването съгласно ОРЗД е изчерпателен. Както беше посочено в точка 14, правното основание за обработване на лични данни за предоставянето на платежни услуги по принцип е член 6, параграф 1, буква б) от ОРЗД, където се посочва, че обработването е необходимо за изпълнението на договор, по който субектът на данни е страна, или за предприемане на стъпки по искане на субекта на данни преди сключването на договор. От това следва, че член 94, параграф 2 от ДПУ2 не може да се счита за допълнително правно основание за обработването на лични данни. ЕКЗД счита, че с оглед на гореизложеното настоящата точка следва да се тълкува, от една страна, в съответствие с приложимата правна уредба в областта на защитата на данните, а от друга страна, по начин, чрез който да се запази полезното ѝ действие. Поради това изричното съгласие в съответствие с член 94, параграф 2 от ДПУ2 следва да се счита за допълнително изискване с договорен характер[23] по отношение на достъпа до лични данни и последващото им обработване и съхраняване с цел предоставяне на платежни услуги и следователно не е същото като (изричното) съгласие в съответствие с ОРЗД.

37. „Изричното съгласие“, посочено в член 94, параграф 2 от ДПУ2, е договорно съгласие. Това означава, че член 94, параграф 2 от ДПУ2 следва да се тълкува в смисъл, че при сключването на договор с доставчик на платежни услуги съгласно ДПУ2 субектите на данни трябва да са напълно запознати с конкретните категории лични данни, които ще бъдат обработвани. Освен това те трябва да са запознати с конкретната цел (платежна услуга), за която ще бъдат обработвани техните лични данни, и трябва да дадат изричното си съгласие относно тези клаузи. Такива клаузи следва да се отличават ясно от другите въпроси, които се разглеждат в договора, и трябва да бъдат изрично приети от субекта на данни.

[23] Писмо на Европейския комитет по защита на данните относно ДПУ2, 5 юли 2018 г., стр. 4.

38. В основата на понятието „изрично съгласие“ по член 94, параграф 2 от ДПУ2 стои получаването на достъп до лични данни за последващо обработване и съхраняване на тези данни с цел предоставяне на платежни услуги. Това означава, че доставчикът на платежни услуги[24] все още не обработва личните данни, но му е необходим достъп до личните данни, които са били обработвани под ръководството на друг администратор. Ако ползвател на платежни услуги сключи договор например с доставчик на услуги по иницииране на плащане, този доставчик трябва да получи достъп до личните данни на ползвателя на платежни услуги, които се обработват под ръководството на доставчика на платежни услуги, обслужващ сметката. Целта на изричното съгласие по член 94, параграф 2 от ДПУ2 е да се даде разрешение за получаване на достъп до тези лични данни, за да може да се обработват и да се съхраняват личните данни, които са необходими за целите на предоставянето на платежната услуга. Ако субектът на данни даде изричното си съгласие, доставчикът на платежни услуги, обслужващ сметката, е длъжен да предостави достъп до посочените лични данни.

39. Въпреки че съгласието, предвидено в член 94, параграф 2 от ДПУ2, не е правно основание за обработването на лични данни, това съгласие се отнася по-конкретно за личните данни и защитата на данните, и с него на ползвателя на платежни услуги се гарантира прозрачност и известна степен на контрол[25]. Макар че в ДПУ2 не са уточнени материалноправните условия за съгласието, предвидено в член 94, параграф 2 от ДПУ2, както е посочено по-горе, то следва да се разбира в съответствие с приложимата правна уредба в областта на защитата на данните и по начин, по който да се запази полезното му действие.

40. По отношение на информацията, която трябва да бъде предоставяна от администраторите, и изискването за прозрачност в Насоките на Работната група по член 29 относно прозрачността е уточнено, че „*основен въпрос във връзка с принципа на прозрачност, очертан в тези разпоредби, е това, че субектите на данни следва да са в състояние предварително да определят какви са обхватът и последствията от обработването и че те не трябва да бъдат изненадани по-късно от начините, по които са били използвани личните им данни*“[26].

41. Освен това, както се изисква съгласно принципа на ограничаване в рамките на целта, личните данни трябва да бъдат събирани за конкретни, изрично указани и легитимни цели (член 5, параграф 1, буква б) от ОРЗД). Когато личните данни се събират за повече от една цел, „*администраторите следва да избягват да определят само една широка цел, за да обосновят различни допълнителни дейности по обработване, които всъщност имат само далечна връзка с действителната първоначална цел*“[27]. ЕКЗД е подчертал, най-вече в контекста на договорите за онлайн услуги, риска от включване в договорите на общи условия за обработване и е заявил, че целта на събирането трябва да бъде ясно и точно посочена: тя трябва да съдържа достатъчно подробности, за да се определи какъв вид обработване е включено и не е включено в рамките на конкретната цел, както и да

[24] Това се прилага за услуги 1—7 от приложение I към ДПУ2.

[25] Член 94, параграф 2 от ДПУ2 спада към глава 4 „Защита на данните“.

[26] Работна група по член 29, Насоки относно прозрачността съгласно Регламент 2016/679, точка 10 (приети на 11 април 2018 г.), одобрени от ЕКЗД.

[27] Становище 3/2013 на работната група по член 29 относно принципа на ограничаване в рамките на целта (РД 203), стр. 16.

съществува възможност за оценка на съответствието със закона и за прилагането на гаранции за защита на данните[28].

42. Когато въпросът за целите се разглежда в контекста на допълнителното изискване за изрично съгласие в съответствие с член 94, параграф 2 от ДПУ2, това предполага, че администраторите трябва да предоставят на субектите на данни конкретна и изрична информация относно определените от администратора специфични цели, за които е получен достъп до техните лични данни и за които личните им данни се обработват и запазват. В съответствие с член 94, параграф 2 от ДПУ2 субектите на данни трябва изрично да приемат тези специфични цели.

43. Освен това, както е посочено по-горе в точка 10, ЕКЗД подчертава, че ползвателят на платежни услуги трябва да може да избира дали да използва услугата и не може да бъде принуден да я използва. Следователно съгласието по член 94, параграф 2 от ДПУ2 също трябва да бъде свободно изразено съгласие.

3.3 Заключение

44. Изричното съгласие в съответствие с ДПУ2 е различно от (изричното) съгласие в съответствие с ОРЗД. Изричното съгласие по член 94, параграф 2 от ДПУ2 е допълнително изискване с договорен характер. Когато доставчик на платежни услуги има нужда от достъп до лични данни за предоставянето на платежна услуга, е необходимо изричното съгласие на ползвателя на платежни услуги в съответствие с член 94, параграф 2 от ДПУ2.

[28] Насоки 2/2019 относно обработката на лични данни съгласно член 6, параграф 1, буква б) от Общия регламент относно защита на данните при предоставянето на онлайн услуги на субектите на данни, точка 16 (версия от обществената консултация) и Становище 3/2013 на Работната група по член 29 относно ограничаването в рамките на целта (РД 203), стр. 15—16.

4 ОБРАБОТВАНЕ НА ДАННИ НА ПАСИВНА СТРАНА

4.1 Данни на пасивната страна

45. Обработването на така наречените „данни на пасивната страна“ е въпрос във връзка със защитата на данните, който е нужно внимателно да бъде разгледан. В настоящия документ данни на пасивната страна означава лични данни относно субект на данни, който не е ползвател на конкретен доставчик на платежни услуги, но чиито лични данни се обработват от този конкретен доставчик на платежни услуги за целите на изпълнението на договор между доставчика и ползвателя на платежни услуги. Такъв например е случаят, когато ползвател на платежни услуги — субект на данни А, използва услугите на даден ДУПИС, а субект на данни Б е извършил поредица от платежни операции по платежната сметка на субект на данни А. В този случай субект на данни Б се счита за „пасивна страна“, а личните данни (като например номер на сметката на субекта на данни Б и паричните суми по тези операции), отнасящи се до субект на данни Б, се считат за „данни на пасивната страна“.

4.2 Законен интерес на администратора на лични данни

46. В член 5, параграф 1, буква б) от ОРЗД е предвидено изискване личните данни да се събират единствено за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, несъвместим с тези цели. Освен това в ОРЗД е заложено изискване всяко обработване на лични данни да бъде както необходимо, така и пропорционално и в съответствие с принципите за защита на данните, като например принципите за ограничение на целите и на свеждане на данните до минимум.

47. Съгласно ОРЗД обработването на данни на пасивната страна е позволено, когато то е необходимо за целите на законните интереси на администратора или на трета страна (член 6, параграф 1, буква е) от ОРЗД). Такова обработване обаче може да се извършва само при условие че пред законните интереси на администратора нямат „преимущество [...] интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни“.

48. Следователно законосъобразно основание за обработване на данни на пасивната страна от страна на ДУИП и ДУПИС — при предоставянето на платежни услуги по ДПУ2 — може да бъде законният интерес на администратора или на трета страна да изпълнява договора с ползвателя на платежни услуги. Необходимостта да се обработват лични данни на пасивната страна е ограничена и се определя от разумните очаквания на тези субекти на данни. По отношение на предоставянето на платежни услуги, които са обхванати от ДПУ2, трябва да бъдат установени ефективни и подходящи мерки, за да се гарантира, че интересите или основните права и свободи на мълчаливите страни не се пренебрегват и че разумните очаквания на тези субекти на данни относно обработването на личните им данни се зачитат. Администраторът (ДУПИС или ДУИП) трябва да установи необходимите гаранции във връзка с обработването, за да защити правата на субектите на данни. Това включва технически мерки, за да се гарантира, че данните на пасивната страна не се обработват за цели, различни от целите, за които са били първоначално събрани от ДУИП и ДУПИС. Ако е практически осъществимо, трябва да се прилагат също криптиране или други техники за постигане на подходящо равнище на сигурност и свеждане на данните до минимум.

4.3 По-нататъшно обработване на личните данни на пасивната страна

49. Както е посочено в параграф 29, личните данни, обработвани във връзка с платежна услуга, регламентирана с ДПУ2, могат да бъдат обработвани по-нататък въз основа на правни

задължения, вменени на доставчика на услуги. Тези правни задължения могат да се отнасят до лични данни на пасивната страна.

50. Що се отнася до по-нататъшното обработване на данни на пасивната страна въз основа на законен интерес, ЕКЗД счита, че те не могат да се използват за цели, различни от целите, за които са били събрани, освен на основание, заложено в правото на ЕС или на държава членка. Получаването на съгласието на пасивната страна не е осъществимо по законен път, тъй като за да се получи такова съгласие, трябва да се събират или обработват лични данни на пасивната страна, за което не може да бъде намерено правно основание по член 6 от ОРЗД. Чрез проверката за съвместимост по член 6, параграф 4 от ОРЗД не може също така да се изведе основание за обработване за други цели (напр. дейности по директен маркетинг). Правата и свободите на тези пасивни страни на данни няма да бъдат зачетени, ако новият администратор на данни използва личните данни за други цели, като се вземе предвид причината, поради която са били събрани личните данни, и по-специално отсъствието на всякакви отношения със субектите на данни, които са пасивни страни[29]; отсъствието на каквато и да било връзка между всяка друга цел и целта, за която първоначално са били събрани личните данни (т.е. фактът, че доставчиците на платежни услуги се нуждаят от данните на пасивната страна само за да изпълнят договор с другата договаряща страна); естеството на съответните лични данни[30], обстоятелството, че субектите на данни не са в състояние разумно да очакват по-нататъшно обработване или дори да са наясно кой администратор може да обработва техните лични данни и като се вземат предвид законовите ограничения за обработването, посочени в член 66, параграф 3, буква ж) и член 67, параграф 2, буква е) от ДПУ2.

[29] В съображение 87 от ДПУ2 се посочва, че ДПУ2 се отнася само до „договорни задължения и отговорности между ползвателя на платежни услуги и доставчика на платежни услуги“. Следователно данните на пасивната страна не попадат в обхвата на ДПУ2.

[30] Особено внимание следва да се обърне при обработването на финансови лични данни, тъй като съгласно Насоките относно оценката на въздействието върху защитата на данни (ОВЗД) може да се счита, че при такова обработване нараства възможният риск за правата и свободите на физическите лица.

5 ОБРАБОТВАНЕ НА СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ СЪГЛАСНО ДПУ2

5.1 Специални категории лични данни

51. Съгласно член 9, параграф 1 от ОРЗД се забранява обработването на „лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице“.

52. Следва да се подчертае, че в някои държави членки електронните плащания вече са повсеместни и много хора ги предпочитат в хода на ежедневните си операции пред паричните плащания. Същевременно чрез финансовите операции може да се разкрие чувствителна информация относно отделен субект на данни, включително информация, свързана със специални категории лични данни. Така например, в зависимост от подробните данни, свързани с операцията, политическите възгледи и религиозните убеждения може да бъдат разкрити чрез дарения, направени за политически партии или организации, църкви или енории. Членството в синдикални организации може да бъде разкрито чрез събирането на годишна такса за членство от банковата сметка на дадено лице. Данните за здравословното състояние може да бъдат събрани чрез анализ на платежни документи за заплатени медицински разходи от страна на субекта на данни на медицински специалист (например психиатър). И накрая, с информацията относно определени покупки може да се разкрие информация относно сексуалния живот или сексуалната ориентация на лицето. Както е видно от тези примери, дори единични операции могат да съдържат специални категории лични данни. Освен това при услугите по предоставяне на информация за сметка може да се използва профилиране съгласно определението в член 4, параграф 4 от ОРЗД. Както вече е посочено в Насоките на Работната група по член 29 относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент (ЕС) 2016/679, одобрени от ЕКЗД, „профилирането може да създаде специални категории данни, като ги изведе по дедуктивен път от данни, които сами по себе си не представляват специални категории данни, но се превръщат в такива, когато бъдат съчетани с други данни“[31]. Това означава, че чрез сумите по финансовите операции могат да се разкрият различни видове модели на поведение, което може да включва специални категории лични данни. Следователно има значителни шансове доставчик на услуги, обработващ информация относно финансовите операции на субекти на данни, да обработва и специални категории лични данни.

53. По отношение на понятието „чувствителни данни за плащанията“ ЕКЗД отбелязва следното: определението за чувствителни данни за плащанията в ДПУ2 се различава значително от начина, по който понятието „чувствителни данни“ се използва широко в ОРЗД и на (законодателството в областта на) защитата на данните. Докато в ДПУ2 „чувствителни данни за плащанията“ са определени като „данни, включително персонализирани идентификационни данни за сигурност, които могат да бъдат използвани за извършването на

[31] Насоки на Работната група по член 29 относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент (ЕС) 2016/679, РД 251 ред.01, стр. 17.

измама“, в ОРЗД е подчертана необходимостта от специфична защита на специални категории лични данни, които съгласно член 9 от ОРЗД по своето естество са особено чувствителни от гледна точка на основните права и свободи, като например специални категории лични данни[32]. Във връзка с това се препоръчва поне да се определи кои видове лични данни ще бъдат обработвани и да им се направи точна категоризация. Най-вероятно ще е необходима оценка на въздействието върху защитата на данните (ОВЗД) в съответствие с член 35 от ОРЗД, която ще спомогне за въпросното определяне. Повече указания относно ОВЗД могат да бъдат намерени в Насоките на Работната група по член 29 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, одобрени от ЕКЗД.

5.2 Възможни дерогации

54. Забраната, предвидена в член 9 от ОРЗД, не е абсолютна. По-специално, като се има предвид, че дерогациите в член 9, параграф 2, букви б)—е) и з)—й) от ОРЗД явно не са приложими за обработването на лични данни в контекста на ДПУ2, може да се разгледат следните две дерогации в член 9, параграф 2 от ОРЗД:

а) забраната не се прилага, ако субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели (член 9, параграф 2, буква а) от ОРЗД);

б) забраната не се прилага, ако обработването е необходимо по причини от важен обществен интерес на основание на правото на Съюза или на държава членка, която е пропорционална на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данни (член 9, параграф 2, буква ж) от ОРЗД).

55. Следва да се изтъкне, че списъкът с дерогации, предвиден в член 9, параграф 2 от ОРЗД, е изчерпателен. Доставчикът на услуги следва да признае възможността в обработваните лични данни за целите на предоставянето на някоя от услугите, попадащи в приложното поле на ДПУ2, да са включени специални категории данни. Тъй като забраната, предвидена в член 9, параграф 1 от ОРЗД, е приложима за тези доставчици на услуги, те трябва да гарантират, че едно от изключенията по член 9, параграф 2 от ОРЗД е приложимо за тях. Следва да се подчертае, че когато доставчикът на услуги не може да докаже, че е изпълнена една от дерогациите, предвидената в член 9, параграф 1 забрана е приложима.

5.3 Важен обществен интерес

56. В рамките на платежните услуги може да се обработват специални категории лични данни по причини от важен обществен интерес, но само когато са изпълнени всички условия, предвидени в член 9, параграф 2, буква ж) от ОРЗД. Това означава, че обработването на специални категории лични данни трябва да бъде разгледано в специална дерогация от член 9, параграф 1 от ОРЗД в правото на Съюза или на държава членка. В тази разпоредба ще трябва да бъде разгледана пропорционалността на преследваната от обработването цел и да се съдържат подходящи и конкретни мерки за защита на основните права и интересите на субектите на данни. Също така в тази разпоредба съгласно правото на Съюза или на държава членка ще трябва да се зачита същността на правото на защита на данните. И

[32] В съображение 10 от ОРЗД например специалните категории лични данни са наречени „чувствителни данни“.

накрая, трябва да се докаже също, че обработването на специални категории данни е необходимо по причини от важен обществен интерес, включително интереси от системно значение. Само когато всички тези условия са изцяло изпълнени, тази дерогация може да стане приложима за определени видове платежни услуги.

5.4 Изрично съгласие

57. В случаите, когато дерогацията от член 9, параграф 2, буква ж) от ОРЗД не се прилага, получаването на изрично съгласие в съответствие с условията за валидно съгласие, предвидени в ОРЗД, изглежда остава единствената възможна законна дерогация за обработване на специални категории лични данни от страна на ДТС. В Насоки 5/2020 на ЕКЗД относно съгласието в съответствие с Регламент 2016/679[33] е посочено, че: „[в] член 9, параграф 2 „необходимо за изпълнението на договор“ не се признава за изключение от общата забрана за обработване на специални категории данни. Ето защо администраторите и държавите членки, които разглеждат тази ситуация, следва да се запознаят със специалните изключения в член 9, параграф 2, букви б)—й)“. Когато доставчиците на услуги се осланят на разпоредбата на член 9, параграф 2, буква а) от ОРЗД, те трябва да се уверят, че са получили изрично съгласие, преди да започнат обработването. Изричното съгласие, предвидено в член 9, параграф 2, буква а) от ОРЗД, трябва да отговаря на всички изисквания на ОРЗД.

5.5 Липса на подходяща дерогация

58. Както беше посочено по-горе, когато доставчикът на услуги не може да докаже, че е изпълнена една от дерогациите, се прилага забраната в член 9, параграф 1. В този случай може да бъдат въведени технически мерки, за да се предотврати обработването на специални категории лични данни, например чрез предотвратяване на обработването на определени извадки от данни. Във връзка с това доставчиците на платежни услуги може да проучат техническите възможности за изключване на специалните категории лични данни и да позволят избирателен достъп, като по този начин ще се предотврати обработването от страна на ДТС на специални категории лични данни, свързани с пасивни страни.

[33] Насоки 5/2020 относно съгласието в съответствие с Регламент 2016/679, ЕКЗД, точка 99.

6 СВЕЖДАНЕ НА ДАННИТЕ ДО МИНИМУМ, СИГУРНОСТ, ПРОЗРАЧНОСТ, ОТЧЕТНОСТ И ПРОФИЛИРАНЕ

6.1 Свеждане на данните до минимум и защита на данните на етапа на проектирането и по подразбиране

59. Принципът на свеждане на данните до минимум е залегнал в член 5, параграф 1), буква в) от ОРЗД: „личните данни са […] подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват“. По същество съгласно принципа на свеждане на данните до минимум администраторите следва да не обработват повече лични данни, отколкото е необходимо, за да постигнат съответната конкретна цел. Както беше изтъкнато в глава 2, обемът и видът лични данни, необходими за предоставянето на платежната услуга, се определят от обективната и разбираема и за двете страни цел на договора[34]. Свеждането на данните до минимум е приложимо за всяко обработване (т.е. всяко събиране или осъществяване на достъп и искане на лични данни). В Насоки 4/2019 относно член 25- Защитата на данните на етапа на проектирането и по подразбиране (ЗДЕПП) на ЕКЗД е посочено, че „обработващите лични данни и доставчиците на технологии също са признати като ключови фактори за ЗДЕПП, те трябва да са наясно, че администраторите са задължени да обработват лични данни само със системи и технологии, които имат вградена защита на данните“[35].

60. Член 25 от ОРЗД съдържа задължения за прилагане на защитата на данните на етапа на проектирането и по подразбиране. Тези задължения са от особено значение за принципа на свеждане на данните до минимум. В този член е определено, че администраторът въвежда както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на данните и интегрирането на необходимите гаранции в процеса на обработване, за да се спазят изискванията на ОРЗД и да се осигури защита на правата на субектите на данни. Администраторът въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, срока на съхраняването им и тяхната достъпност. Тези мерки може да включват криптиране, псевдонимизация и други технически мерки.

61. Когато се прилага задължението по член 25 от ОРЗД, елементите, които трябва да бъдат взети предвид, са достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица. Допълнителни разяснения относно това задължения са предоставени в цитираните по-горе Насоки № 4/2019 относно член 25- Защита на данните на етапа на проектирането и по подразбиране.

[34] Насоки 2/2019 относно обработката на лични данни съгласно член 6, параграф 1, буква б) от Общия регламент относно защита на данните при предоставянето на онлайн услуги на субектите на данни, ЕКЗД, точка 32.

[35] Насоки 4/2019 относно член 25- Защитата на данните на етапа на проектирането и по подразбиране, стр. 29.

6.2 Мерки за свеждане на данните до минимум

62. За да предостави поисканите услуги, доставчикът трета страна, който има достъп до данни за платежна сметка, трябва да вземе предвид също така принципа на свеждане на данните до минимум и трябва да събира само лични данни, които са необходими за конкретната платежна услуга, поискана от ползвателя на платежни услуги. По принцип достъпът до лични данни следва да бъде ограничен до необходимото за предоставянето на платежни услуги. Както беше посочено в глава 2, съгласно ДПУ2 се изисква ДПУОС да предоставят информация за ползвателя на платежни услуги по искане на ползвателя на платежни услуги, когато той иска да използва услуга по иницииране на плащане или услуга по предоставяне на информация за сметка.

63. Когато за предоставянето на договора не са необходими всички данни за платежна сметка, преди данните да бъдат събрани, ДУПИС следва да направи подбор на съответните категории данни. Така например, категориите данни, които може да не са необходими, може да включват самоличността на пасивната страна и характеристиките на операцията. Също така, освен ако не се изисква съгласно правото на държава членка или на Съюза, предоставянето на международния номер на банковата сметка (IBAN номер) на пасивната страна може да не е необходимо.

64. Във връзка с това възможното прилагане на технически мерки, които дават възможност или подкрепят ДТС да спазват задължението си за осъществяване на достъп и извличане само на личните данни, необходими за предоставянето на услугите си, може да се считат за съответстващи на член 24, параграф 2 от ОРЗД, тъй като са част от прилагането на подходящи политики за защита на данните от страна на администратора. В това отношение ЕКЗД препоръчва използването на цифрови инструменти, за да се помогне на ДУПИС да спазват задължението си да събират само лични данни, които са необходими за целите, за които тези данни се обработват. Ако например на доставчик на услуга не са му необходими характеристиките на дадена операция (посочени в полето за описание на записите на операциите), за да предоставя услугата си, ДТС могат да използват цифров инструмент за подбор като средство да изключат това поле от общите операции на ДТС по обработване.

Пример 2:

HappyPayments, нашият доставчик на услуги по предоставяне на информация за сметка от пример 1, иска да гарантира, че обработва само личните данните за платежна сметка, от които неговите ползватели се интересуват. Стремежът към достъп до повече данни за платежна сметка не е необходим за предоставянето на услугата. Поради това той позволява на ползвателите да избират конкретните видове информация, от която се интересуват.

Ползвател А желае да получи общ преглед на плащанията си за последните два месеца. Съответно той иска за своите две банкови сметки, държани при два различни ДПУОС, информацията за всички операции през последните два месеца, сумата по операцията, датата на изпълнение и името на получателя и поставя отметка в съответните полета в потребителския интерфейс на HappyPayments.

След това HappyPayments започва да иска от съответните ДПУОС само информацията, която отговаря на полетата, зададени от ползвател А, и само за последния двумесечен период. Дружеството не е поискало информацията например за „съобщаването“ на операцията по превод или дори IBAN номера, тъй като ползвател А не е поискал тази информация.

За да позволят на HappyPayments да изпълни задълженията си за свеждане на данните до минимум, ДПУОС позволяват на дружеството да поиска данни за конкретни полета за редица дати.

65. Във връзка с това следва да се отбележи също, че съгласно ДПУ2 ДПУОС могат да осигуряват достъп само до информация за платежна сметка. Няма правно основание съгласно ДПУ2 за осигуряване на достъп по отношение на лични данни, съдържащи се в други сметки, например спестовни сметки, сметки по ипотечен заем или инвестиционни сметки. Съответно съгласно ДПУ2 трябва да се приложат технически мерки, за да се гарантира, че достъпът е ограничен до необходимата информация за платежната сметка.

66. Освен да събира възможно най-малко данни, доставчикът също така трябва да приложи ограничени срокове на съхраняване. Доставчикът на услуги не следва да съхранява лични данни за период, по-дълъг от необходимото във връзка с целите, за които ползвателят на платежни услуги е поискал данните.

67. Ако съгласно договора между субекта на данни и ДУПИС се изисква предаване на лични данни до трети страни, тогава могат да бъдат предадени единствено тези данни, които са необходими за изпълнението на договора. Субектите на данни следва също така да бъдат специално осведомени за предаването и за личните данни, които ще бъдат предадени на тази трета страна.

6.3 Сигурност

68. ЕКЗД вече е изтъкнал, че нарушенията, свързани с финансовите лични данни, *„очевидно биха довели до сериозно въздействие върху ежедневието на субекта на данни“* и е посочил като пример рисковете от измами при плащания[36].

69. Когато нарушение, свързано с данни, включва финансови данни, субектът на данни може да бъде изложен на значителен риск. В зависимост от изтеклата информация субектите на данни може да бъдат изложени на риск от кражба на самоличността, кражба на средства от техните сметки или други активи. Освен това е възможно разкриването на данни за операцията да бъде свързано със значителни рискове за неприкосновеността на личния живот, тъй като данните за операцията може да съдържат сведения за всички аспекти на личния живот на субекта на данни. Същевременно финансовите данни очевидно са ценни за престъпниците и следователно са привлекателна цел.

70. Като администратори, доставчиците на платежни услуги са задължени да предприемат подходящи мерки, за да защитят личните данни на субектите на данни (член 24, параграф 1 от ОРЗД). Колкото по-големи са рисковете, свързани с дейността по обработване, извършвана от администратора, толкова по-високи са стандартите за сигурност, които трябва да бъдат прилагани. Тъй като обработването на финансови данни е свързано с различни сериозни рискове, мерките за сигурност следва да бъдат със съответната степен на строгост.

71. Доставчиците на услуги следва да се придържат към високи стандарти, включително механизми за задълбочено установяване на идентичността на клиента и високи стандарти за сигурност на техническите средства[37]. Други процедури, като проверката на това дали

[36] Насоките на Работната група по член 29 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, РД 248 ред.01 — одобрени от ЕКЗД.
[37] Вж. РТС.

обработващите лични данни спазват стандартите за сигурност и прилагането на процедури за възпрепятстване на непозволен достъп, също са важни.

6.4 Прозрачност и отчетност

72. Прозрачността и отчетността са два основни принципа на ОРЗД.

73. По отношение на прозрачността (член 5, параграф 1, буква а) от ОРЗД) в член 12 от ОРЗД е уточнено, че администраторът предприема необходимите мерки за предоставяне на всякаква информация по членове 13 и 14 от ОРЗД. Освен това съгласно посочения член се изисква информацията или комуникацията относно обработването на лични данни да бъде кратка, прозрачна, разбираема и лесно достъпна. Информация трябва да бъде на ясен и прост език и да се предоставя писмено „или по друг начин, включително, когато е целесъобразно, с електронни средства“. В Насоките на Работната група по член 29 относно прозрачността съгласно Регламент 2016/679, одобрени от ЕКЗД, се дават конкретни указания за спазване на принципа на прозрачност в цифрова среда.

74. В съответствие с цитираните по-горе Насоки относно прозрачността съгласно Регламент 2016/679 член 11 от ОРЗД следва да се тълкува като начин за прилагане на действително свеждане до минимум на данните, без да се възпрепятства упражняването на правата от страна на субектите на данни, както и в смисъл, че трябва да се осигури възможност за упражняването на тези права с помощта на допълнителна информация, предоставена от субекта на данни. Може да има случаи, в които администраторът обработва лични данни, при които не се изисква идентифициране на субекта на данни (например с псевдонимизирани данни). В такива случаи също може да е приложим член 11, параграф 1, тъй като той гласи, че администраторът не е задължен да поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данни с единствената цел да бъде спазен ОРЗД.

75. По отношение на услугите съгласно ДПУ2 член 13 от ОРЗД е приложим за личните данни, събирани от субекта на данни, а член 14 е приложим, когато от субекта на данни не са получени личните данни.

76. По-специално, субектът на данни трябва да бъде уведомен за периода, за който личните данни ще бъдат съхранявани, или ако това не е възможно, за използваните критерии за определяне на този период, и когато е приложимо, за законните интереси на администратора или на евентуална трета страна. Когато обработването се извършва въз основа на съгласие в съответствие с член 6, параграф 1, буква а) от ОРЗД или изрично съгласие в съответствие с член 9, параграф 2, буква а) от ОРЗД, субектът на данни трябва да бъде уведомен за съществуването на право на оттегляне на съгласието по всяко време.

77. Администраторът предоставя информацията на субекта на данни, като се отчитат конкретните обстоятелства, при които личните данни се обработват. Ако личните данни трябва да се използват за връзка със субекта на данни[38], какъвто най-вероятно ще бъде случаят с ДУПИС, информацията трябва да бъде предоставена най-късно при осъществяване на първия контакт с този субект на данни. Ако личните данни трябва да се разкрият пред друг получател, информацията трябва да бъде предоставена най-късно при разкриването на личните данни за първи път.

[38] Член 14, параграф 3, буква б) от ОРЗД.

78. По отношение на платежните онлайн услуги в цитираните по-горе насоки е изяснено, че администраторите на данни могат да следват многопластов подход, като изберат да прилагат комбинация от методи за осигуряване на прозрачност. По-специално се препоръчва да се използват многопластови декларации/съобщения за поверителност с препратки към различните категории информация, които трябва да бъдат предоставени на субекта на данните, вместо цялата информация да се показва в едно съобщение на екрана, за да се избегне информационна умора, като същевременно се гарантира ефективността на информацията.

79. В цитираните по-горе насоки също така е изяснено, че администраторите може да изберат да използват допълнителни инструменти, за да предоставят информация на отделния субект на данни, например информационни табла относно поверителността. Информационното табло относно поверителността е място, където субектите на данни могат да преглеждат „информация относно поверителността“ и да управляват своите предпочитания, свързани с поверителността, като разрешават или забраняват използването на своите данни по определени начини от въпросния администратор[39]. С помощта на информационното табло относно поверителността може да се осигури общ преглед на ДТС, които са получили изричното съгласие на субектите на данни, и може да се предложи информация относно естеството и обема на личните данни, до които ДТС са осъществили достъп. По принцип чрез общия преглед ДПУОС може да предложи на ползвателя възможността да оттегли конкретното изрично съгласие в съответствие с ДПУ2[40], което би довело до отказ на достъп до неговите платежни сметки на един или повече ДТС. Ползвателят може също така да поиска от ДПУОС да откаже достъп до неговата платежна сметка или неговите платежни сметки на един или повече конкретни ДТС[41], тъй като ползвателят има правото да (не) използва услуга по предоставяне на информация за сметка. Ако информационните табла относно поверителността се използват, за да се даде или да се оттегли изрично съгласие, те следва да бъдат разработени и прилагани законосъобразно и по-специално да предотвратяват създаването на пречки пред правото на ДТС да предоставят услуги в съответствие с ДПУ2. В тази връзка и в съответствие с приложимите разпоредби съгласно ДПУ2 ДТС има възможност отново да получи изрично съгласие от ползвателя, след като това съгласие е било оттеглено.

80. Съгласно принципа на отчетност се изисква администраторът да определи подходящи технически и организационни мерки, за да гарантира и да може да докаже, че обработването се извършва в съответствие с ОРЗД, по-специално с основните принципи за защита на данните, предвидени в член 5, параграф 1. При определянето на тези мерки следва да се вземат предвид естеството, обхватът, контекстът и целите на обработването и

[39] Съгласно Насоките на Работната група по член 29 относно прозрачността съгласно Регламент 2016/679, одобрени от ЕКЗД, информационните табла относно поверителността са особено полезни, когато субектите на данни използват една и съща услуга на много различни устройства, тъй като те им дават достъп до техните лични данни и контрол върху тях, независимо от това как използват услугата. Даването на възможност на субектите на данни да регулират ръчно своите настройки за поверителност чрез информационно табло относно поверителността може също така да улесни персонализирането на декларацията/съобщението за поверителност, като се отразяват само видовете обработване, които се прилагат за този конкретен субект на данните.

[40] Вж. например „изричното съгласие“, посочено в член 67, параграф 2, буква а) от ДПУ2.

[41] Вж. също становището ЕВА/ОР/2020/10, точка 45.

рисковете за правата и свободите на физическите лица и те трябва да се преразглеждат и при необходимост да се актуализират[42].

6.5 Профилиране

81. Обработването на лични данни от страна на доставчиците на платежни услуги може да включва „профилиране“ съгласно член 4, параграф 4 от ОРЗД. Така например, ДУПИС биха могли да разчитат на автоматизирано обработване на лични данни, за да извършват оценка на определени лични аспекти, свързани с дадено физическо лице. В зависимост от спецификите на услугата, може да се оценява личното финансово състояние на даден субект на данни. Услугите по предоставяне на информация за сметка, които се предоставят по искане на ползвателите, може да включват задълбочена оценка на личните данни за платежната сметка.

82. По отношение на субекта на данни администраторът също така трябва да действа в съответствие с принципа на прозрачност относно наличието на автоматизирано вземане на решения, включително профилиране. В такива случаи администраторът трябва да предостави съществена информация относно използваната логика, както и относно значението и предвидените последствия от това обработване за субекта на данни (член 13, параграф 2, буква е) и член 14, параграф 2, буква ж) и съображение 60)[43]. По сходен начин, съгласно член 15 от ОРЗД субектът на данни има право да поиска и да получи информация от администратора относно наличието на автоматизирано вземане на решения, включително относно профилирането, използваната логика, както и значението и последствията за субекта на данни, и при определени обстоятелства има право да възрази срещу „профилирането“, независимо дали се извършва изцяло автоматизирано вземане на индивидуални решения, основано на профилиране[44].

83. Освен това от значение в този контекст е и предвиденото в член 22 от ОРЗД право на субекта на данни да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данни или по подобен начин го засяга в значителна степен. Тази норма също така включва, при определени обстоятелства, необходимостта администраторите на данни да прилагат подходящи мерки за защита на правата и свободите и законните интереси на субекта на данни, като например конкретна информация за физическото лице, правото на човешка намеса при вземането на решения и правото да изрази гледната си точка и да оспори решението. Както е посочено и в съображение 71 от ОРЗД, това означава, наред с другото, че лицето има право да не бъде обект на решение, като например автоматичен отказ на онлайн искания за кредит, без човешка намеса[45].

84. Автоматизираното вземане на решения, включително профилирането, което включва специални категории лични данни, е позволено само при изпълнение на следните кумулативни условия на член 22, параграф 4 от ОРЗД:

- да е налице приложимо изключение по член 22, параграф 2; както и

[42] Член 5, параграф 2 и член 24 от ОРЗД.
[43] Насоки относно прозрачността съгласно Регламент 2016/679, РД 260 ред.01, одобрени от ЕКЗД.
[44] Насоки на Работната група по член 29 относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент (ЕС) 2016/679, РД 251 ред.01.
[45] Съображение 71 от ОРЗД.

- да се прилага член 9, параграф 2, буква а) или буква ж) от ОРЗД. И в двата горепосочени случая администраторът трябва да въведе подходящи мерки за защита на правата и свободите, както и на законните интереси на субекта на данните[46].

85. Изискванията за по-нататъшно обработване, посочени в тези насоки, също трябва да бъдат спазвани. Разясненията и указанията относно автоматизираното вземане на индивидуални решения и профилирането, предоставени в Насоките на Работната група по член 29 относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент (ЕС) 2016/679, одобрени от ЕКЗД, са напълно приложими по отношение на платежните услуги и съответно следва да бъдат надлежно вземани предвид.

За Европейския комитет по защита на данните,

Председател

(Andrea Jelinek)

[46] Насоки на Работната група по член 29 относно автоматизираното вземане на индивидуални решения и профилирането за целите на Регламент (ЕС) 2016/679, РД 251 ред.01, стр. 28.