Комисия за Защита на Личните Данни

ИНФОРМАЦИОНЕН БЮЛЕТИН

Брой 1 (106), януари 2024 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода ноември и декември 2023 г.)

КЗЛД ПРИЕ МЕТОДИЧЕСКИ УКАЗАНИЯ ОТНОСНО ПОДАВАНЕТО НА НЕОБХОДИМАТА СТАТИСТИЧЕСКА ИНФОРМАЦИЯ ПО ЗАКОНА ЗА ЗАЩИТА НА ЛИЦАТА, ПОДАВАЩИ СИГНАЛИ ИЛИ ПУБЛИЧНО ОПОВЕСТЯВАЩИ ИНФОРМАЦИЯ ЗА НАРУШЕНИЯ

На свое редовно заседание от 13.12.23 г. КЗЛД прие **Методически указания № 2 относно подаването към Комисията за защита на личните данни на необходимата статистическа информация по Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения**.

В качеството ѝ на централен орган за външно подаване на сигнали по ЗЗЛПСПОИН, КЗЛД има редица задължения, сред които са даване на методически указания на задължените субекти по чл. 12 от ЗЗЛПСПОИН, поддържане на регистър на сигналите, анализиране и обобщаване на практиката по работата с тях, както и предаване на Европейската комисия на необходимите статистически данни. Ежегодно предоставяната на Европейската комисия информация следва да съдържа за броя на постъпилите сигнали, броя на извършените проверки и резултатите от тях, както и отчет за финансовите постъпления от събраните глоби и имуществени санкции и оценка при установени финансови щети.

На 27 юли 2023 година КЗЛД прие **Наредба № 1 от 27 юли 2023 г. за воденето на регистъра на сигналите по чл. 18 от Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения и за препращане на вътрешни сигнали към Комисията за защита на личните данни**. В нея са разписани детайлно общите положения, съдържанието на регистъра и реда за неговото водене, сроковете и условията за съхраняването на сигналите, възможността за осъществяване на достъп до регистъра, както и случаите, в които сигналите се препращат до КЗЛД.

Приетите на 13.12.2023 г. Методически указания № 2 имат за цел да:

• **Подпомагат дейността на задължените субекти по ЗЗЛПСПОИН**, в т.ч. и на определените от тях служители/звена, отговарящи за разглеждането на сигнали, при предоставянето на КЗЛД на статистическа информация.

• **Установят единни правила и критерии** при отчитането и обобщаването на статистическата информация.

• **Не допускат противоречива практика при подаването на статистическа информация и установят контрола, упражняван от КЗЛД** при прилагането на нормативната уредба за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения.

Съгласно **Методически указания № 2** статистическата информация следва да бъде предоставена до 31 януари 2024 г. Поради забавяне на пускането в експлоатация на електронния отчетен модул, който КЗЛД разработва специално за тази цел, на задължените субекти ще бъде предоставен подходящ допълнителен срок за подаване на информацията. Алтернативните начини за подаване на статистиката (*т. 7 и 8 съгласно методическите указания*) могат да се ползват от 01.01.2024 г.

КЗЛД обръща внимание на задължените субекти по чл. 12, ал. 1 от ЗЗЛПСПОИН, че те **не следва да подават** статистическа информация към Комисията, **ако при тях не са постъпвали сигнали** през отчетния период.

КЗЛД ОРГАНИЗИРА СЕМИНАРИ ВЪВ ВРЪЗКА С АНГАЖИМЕНТИТЕ СИ ПО ПРИСЪЕДИНЯВАНЕ НА РЕПУБЛИКА БЪЛГАРИЯ КЪМ ОИСР И ПО ПРИЛАГАНЕТО НА ЗЗЛПСПОИН

В периода от 20-ти до 22-ри ноември 2023 г. КЗЛД организира и проведе паралелно три семинара, чиито фокуси бяха в областите на *изпълнение на Националната пътна карта с дейности по сътрудничеството с ОИСР и прилагане на Закона за зашита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (ЗЗЛПСПОИН)".*

Присъединяването на Република България към Организацията за икономическо сътрудничество и развитие (ОИСР) е задача от национален приоритет. В семинара, проведен под наслов *„Изпълнение на Националната пътна карта с дейности по сътрудничеството с ОИСР – добри практики"* участваха представители на водещи и партниращи институции от пътната карта за присъединяване на Република България към ОИСР. Целта на семинара бе да събере на едно място представители на водещите и партниращите институции по отделните комитети, в които участват и представители на КЗЛД, за да обменят опит и добри практики в досегашния им опит в дейностите по сътрудничеството с ОИСР. Представен бе опитът на Комитетите по цифрова икономика, по публично управление, по регулаторна политика и по здравеопазване. Натрупаният опит в подготовката на самооценките, съдържащи синтезирана информация за законодателството, политиките и практиките по отделните правни инструменти на ОИСР, проведените първи технически мисии от страна на представители на Организацията, ще послужат за разработването на общи стъпки, които българските институции могат да следват в процеса по присъединяването към ОИСР. На семинара бе предложен и обсъден първи проект на Наръчник с добри практики за осъществяване на действия по присъединяване на Република България към ОИСР. Участниците в обсъжданията се обединиха около структурата и общите теми, които Наръчникът – като незадължителен документ, следва да съдържа, за да бъде от полза за представителите на държавните институции.

Под наслов „Цифрово бъдеще за Европа", специализираната администрация на КЗЛД обсъди въпроси, свързани с аспекти на присъединяването на Република България към ОИСР. Представени и дискутирани бяха решения, становища, резултатите от проверки на КЗЛД, както и казуси от Информационната система на вътрешния пазар, свързани защитата на личните данни в среда на дигитализация и нови технологии решения.

В семинара, посветен на прилагането на ЗЗЛПСПОИН участваха представители на КЗЛД и на органи с компетентност по чл. 20 по ЗЗЛПСПОИН. Този закон определя КЗЛД като Централен орган за външно подаване на сигнали и за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. Комисията координира и контролира дейностите по разглеждане на сигнали от страна на органите по чл. 20, към които КЗЛД препраща по компетентност постъпилите при нея сигнали. За целите на изпълнението на закона КЗЛД има ангажимент да организира най-малко веднъж годишно среща с органите по чл. 20 от закона, на която да се анализира дейността по работа със сигналите. В съответствие с това изискване, на семинара бяха поканени представители на органите по чл. 20 от ЗЗЛПСПОИН с цел обсъждане прилагането на закона и осъществяване на междуинституционално взаимодействие. Обсъдени бяха въпроси, свързани с разглеждане и проверка на сигнали за нарушения по чл. 3 от ЗЗЛПСПОИН - материална компетентност на органите по чл. 20, отчитане на специалното секторно законодателство, прилагане на коригиращите мерки, предоставяне на информация от компетентните органи с оглед изготвянето на доклад, който ще се изпраща ежегодно на Европейската комисия. Специално внимание бе отделено на сферите на взаимодействие между КЗЛД и Комисията за противодействие на корупцията, както и взаимодействието и осигуряването на мерки за подкрепа на лицата по чл. 5 от ЗЗЛПСПОИН, които се предоставят от КЗЛД и от Националното бюро за правна помощ.

КЗЛД ОБЯВИ КОНКУРС ПО СЛУЧАЙ ПРЕДСТОЯЩОТО ОТБЕЛЯЗВАНЕ НА ДЕНЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

По повод наближаващия Ден за защита на личните данни КЗЛД обяви конкурс със следните теми: „**Визия за медийно присъствие на КЗЛД**” и „**Визия за електронен информационен бюлетин на КЗЛД**”.

В наши дни електронната среда е най-достъпният във всяко отношение начин за реализиране на всяка комуникационна политика. Тя е безспорен фаворит за отправяне на послания към всички видове целеви групи и за формиране на обществените нагласи и мнения. В условията на огромна лавина от всякаква информация, **институционалните издания са надежден и достоверен източник на проверена информация** „от първа ръка”. Едновременно с това е важно както съдържанието, което е основната цел, така и оформлението като средство за привличане на внимание и интерес към съдържанието.

Приканваме участниците в нашия конкурс да споделят идеи за това какво трябва да бъде медийното присъствие на Комисията под формата на уебсайт, участие в социални медии, издаване на периодичен информационен бюлетин за дейността на Комисията и други.

До участие в конкурса се допускат всички желаещи без ограничения. Всеки участник може да работи по една от двете теми, както и да участва и с двете. Форматът на участие е по избор: всичко, с което считате, че може да изразите своите идеи - презентация, текст, илюстративни материали.

Обем на текстови материал – до 10 страници по БДС – 30 реда с 60 знака на ред, шрифт Times New Roman с големина на буквите 12 и разредка 1,5, като използваните фигури и графики не се включват в общия обем. Обем на презентация – до 20 слайда.

Материалите следва да бъдат изпращани на електронна поща **concours@cpdp.bg**.

Срокът за изпращане на материалите е 01.03.2024 г.

Предвидената награда за победителя в конкурса е предложение за работа в КЗЛД в областта на изграждане на медийно присъствие на институцията. Важно е да се знае, че **излъчването на победител не е задължително.** Награда ще се предложи само в случай, че някой от участниците ни впечатли с визия, която отговаря на нашите изисквания.

КЗЛД ПУБЛИКУВА ЕКСПОЗЕТА ПО ТЕМИ, РАЗРАБОТЕНИ ОТ ФИНАЛИСТИТЕ НА МИНАЛОГОДИШНИЯ СТУДЕНТСКИ КОНКУРС

През 2023 г. съвместно с Кариерния център на Юридическия факултет на СУ „Св. Климент Охридски“, КЗЛД проведе конкурс за студентско есе на тема „**Особености в защитата на личните данни в електронна среда – научените уроци след две години пандемия**“. Конкурсът бе обявен през януари по случай Деня за защита на личните данни, отбелязван всяка година в редица държави по света. Целта на провеждането на тези конкурси е приобщаване на младите хора към търсенето на решения на предизвикателствата пред защитата на личните данни в контекста на дигитализацията и глобализацията, обхващащи всички сфери на живота. В първия етап участниците писаха есе на по обявената тема, а до втория етап бяха допуснати двама кандидати. Всеки от тях защити своите идеи пред конкурсната комисия с предварително създадени презентация и изложение.

Двамата финалисти получиха грамоти и възможност за осъществяване на едномесечен платен стаж в Комисията за защита на личните данни. Като част от реализирания стаж те подготвиха експозета по теми от областта на защита на личните данни, като в настоящия брой на информационния бюлетин ги публикуваме в цялост в последния раздел на настоящия бюлетин.

ЕКЗД ПУБЛИКУВА СПЕШНО РЕШЕНИЕ СЪС ЗАДЪЛЖИТЕЛЕН ХАРАКТЕР ОТНОСНО META

На 27 октомври 2023 г. Европейският комитет по защита на данните прие **спешно решение със задължителен характер, поискано от Норвежкия орган по защита на данните, за нареждане на окончателни мерки по отношение на Meta Platforms Ireland Ltd.** В резултат на това, на 10 ноември 2023 г. Ирландският орган по защита на данните прие окончателно решение за налагане на забрана на Meta Ireland Limited (Meta IE) за обработване въз основа на договор и легитимен интерес на лични данни за целите на поведенческата реклама. Спешното решение със задължителен характер на ЕКЗД последва искане от Норвежкия орган за защита на данните да бъдат разпоредени окончателни мерки по този въпрос, които биха имали ефект в цялото Европейско икономическо пространство.

Председателят на Комитета Ану Талус заявява: „След внимателно обмисляне, ЕКЗД сметна за необходимо да даде указания на Ирландския орган да наложи забрана за обработване, адресирана до Meta IE, в цялото ЕИП. Още през декември 2022 г. обвързващите решения на Комитета изясниха, че

договорът не е подходящо правно основание за обработване на лични данни, извършвано от Meta за поведенческа реклама. В допълнение, от Ирландския орган бе установено, че Meta не е демонстрирала съответствие с разпорежданията, наложени в края на миналата година. Това е довело до използването на процедура по спешност (чл. 66 от ОРЗД) - дерогация от обичайната процедура за сътрудничество, която може да се използва само при изключителни обстоятелства.

Според чл. 66 от ОРЗД, при извънредни обстоятелства, когато засегнат орган по защита на данните прецени, че е налице спешна необходимост да се действа, за да се защитят правата и свободите на субектите на данни на неговата територия, той може да приеме незабавно временни мерки, които имат правно действие на негова територия за максимум три месеца. Тези мерки се приемат чрез дерогация от механизма за съгласуваност на ОРЗД (чл. 63 от ОРЗД) или механизма за обслужване на едно гише (чл. 60 от ОРЗД). Този инструмент е създаден така, че органите винаги да са в състояние да защитават правата и свободите на лицата в съответната държава членка, при всякакви обстоятелства. Органът по защита на данните, който издава такива временни мерки, трябва да съобщи тези мерки и причините за приемането им без неоправдано забавяне на другите засегнати органи, Европейския комитет по защита на данните и Европейската комисия. Ако органът, който е предприел такива временни мерки, счита, че окончателните мерки трябва да бъдат приети спешно, той може да поиска от ЕКЗД спешно становище или спешно решение със задължителен характер, като предостави причините за спешната необходимост от приемане на окончателни мерки.

На 14 юли 2023 г. Норвежкият орган по защита на данните прие решение за налагане на временна забрана по чл. 66 (1) от ОРЗД относно Meta IE и Facebook Norway AS („Facebook Норвегия“) по отношение на обработването на лични данни на норвежки субекти на данни за поведенческа реклама, разчитаща на правни основания на договор или легитимен интерес. Тази забрана беше ограничена по време и географски обхват: тя беше валидна за три месеца и се прилагаше само в Норвегия. На 26 септември 2023 г. Норвежкият надзорен орган изпрати искане до ЕКЗД за спешно решение със задължителен характер за нареждане на приемането на окончателни мерки, приложими за потребителите във всички държави от ЕИП.

След анализ на досието ЕКЗД достигна до извода, че има продължаващи нарушения на ОРЗД и е налице спешна необходимост от действия в светлината на рисковете за правата и свободите на субектите на данни.

Въз основа на представените доказателства ЕКЗД установи, че е налице продължаващо нарушение на чл. 6 (1) ОРЗД поради неподходящо използване за целите на поведенческа реклама на правните основания на договор и легитимен интерес при обработването на лични данни, събирани от Meta IE. Освен това ЕКЗД установи, че е налице и продължаващо нарушение на задължението на Meta да спазва решенията на надзорните органи, най-вече окончателните решения на Ирландския надзорен орган от декември 2022 г.

Що се отнася до наличието на спешност, ЕКЗД стигна до заключението, че редовните механизми за сътрудничество не могат да бъдат приложени по техния обичаен начин и че спешната необходимост от разпореждане на окончателни мерки е ясна в светлината на рисковете от сериозни и непоправими вреди, причинени на субектите на данни без приемането на крайни мерки.

Комитетът реши, че **окончателните мерки трябва да бъдат приети от Ирландския надзорен орган** и счете за подходящо, пропорционално и необходимо да го инструктира да наложи забрана за обработване на лични данни, адресирана до Meta IE за обработка на лични данни, събрани в продуктите на Meta, за целите на поведенческата реклама въз основа на договор и легитимен интерес. Това спешно решение със задължителен характер беше изпратено до Ирландския и Норвежкия надзорни органи, както и до всички други засегнати надзорни органи. **Ирландският надзорен орган прие окончателното си решение на 10 ноември 2023 г.**

ЕКЗД ПРЕДОСТАВИ ЯСНОТА ОТНОСНО ТЕХНИКИТЕ ЗА ПРОСЛЕДЯВАНЕ, ОБХВАНАТИ ОТ ДИРЕКТИВАТА ЗА НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ И ЕЛЕКТРОННИТЕ КОМУНИКАЦИИ

На 14 ноември 2023 г. Европейският комитет по защита на данните прие **Насоки относно техническия обхват на чл. 5 (3) от Директивата за правото на неприкосновеност на личния живот и електронни комуникации**. Насоките имат за цел да изяснят кои технически операции, по-специално нови и нововъзникващи техники за проследяване, са обхванати от директивата, и да осигурят по-голяма правна сигурност на администраторите на данни и лицата.

Председателят на EDPB Ану Талус заявява: „*Не е тайна, че проследяването на дейностите на потребителите онлайн може сериозно да навреди на поверителността на хората. Неяснотите относно приложното поле на чл. 5, параграф 3 от Директивата за ePrivacy и появата на нови техники, в допълнение към или като алтернатива на традиционните бисквитки, доведоха до нови рискове за поверителността. Тези насоки разглеждат решения, като проследяване на връзки и пиксели, локална обработка и уникални идентификатори, за да се гарантира, че не се заобикалят задълженията за съгласие, посочени в горепосочения член.*“

За да се изясни обхватът, насоките анализират ключови понятия като „информация“, „терминално оборудване на абонат или потребител“, „електронна съобщителна мрежа“, „получаване на достъп“ и „ съхранена информация/съхранение“. Насоките също така включват набор от случаи на практическа употреба, включващи общи техники за проследяване.

Насоките разглеждат само обхвата на прилагане на чл. 5(3) от Директива за неприкосновеността на личния живот и електронните комуникации. Те не разглеждат как трябва да се получава съгласието или изключенията.

Насоките са представени за обществено обсъждане до 18 януари 2024 г

КООРДИНАЦИОННАТА ГРУПА ЗА НАДЗОР НА ЕВРОДАК ОБСЪДИ ДОСТЪПА НА ПРАВООХРАНИТЕЛНИТЕ ОРГАНИ ДО ОБРАБОТВАНИ ОТ СИСТЕМАТА ДАННИ

На 28 ноември 2023 г. се проведе заседание на Координационната група за надзор на системата Евродак. Участваха 32 представители на органите по защита на данните на държавите-членки на Европейския съюз и Европейското икономическо пространство, както и Европейския надзорен орган по защита на данните, подпомагани от представители на Секретариата на Групата.

Координационната група за надзор на Евродак („Eurodac SCG“) е създадена с Регламент (ЕО) № 603/2013, с цел осигуряване на координиран надзор в областта на защитата на личните данни в информационната система Евродак - компютърна система, която управлява централна информационна база данни за дактилоскопични отпечатъци, както и електронните средства за предаване на информация между държавите-членки и централната система. Целта на тази система е най-вече да спомага за определянето на компетентната държава-членка за разглеждането на дадена молба за убежище съгласно Регламент (ЕС) № 604/2013 (Дъблин III) и да ускори идентификацията на индивидите, да улесни избора на държава-членка, която да приеме кандидатите, и да осигури

избягване на възможността за многократно подаване на молба за убежище в различни страни от един и същи кандидат.

Един от основните обсъдени на заседанието въпроси бе по отношение на достъпа на правоохранителните органи до данните, обработвани в Евродак. Представен бе проект на въпросник, който може да се ползва от надзорните органи при осъществяване на надзорните им дейности. Съгласно Глава VI от действащия Регламент за Евродак се предвижда процедура, позволяваща за целите на правоприлагането да се извършва сравняване на пръстови отпечатъци с тези, съдържащи се в Евродак. Въпреки това, поради правото на неприкосновеност на личния живот, правоприлагащите органи имат право да използват Евродак за сравнения само когато има разумни основания, че това ще им помогне значително при предотвратяването, разкриването или разследването на тероризъм или друго тежко престъпление, и само в краен случай, след като първо са извършени други проверки.

Бъдещият регламент за Евродак предвижда разширяване на достъпа на правоприлагащите органи до системата. В писмо, изпратено до Европейския парламент, Групата изразява загриженост относно няколко бъдещи промени и подчертава, че достъпът до данни за целите на правоприлагането трябва да се предоставя по изключение и да подлежи на строги условия с оглед на естеството и предназначението на системата.

Що се отнася до действителната практика, последните доклади на eu-LISA (Агенцията на Европейския съюз за оперативното управление на широкомащабни информационни системи) относно годишната статистика на Евродак показват като цяло ниски нива на достъп от страна на правоприлагащите органи. Броят на исканията обаче се е увеличил значително през последните години.

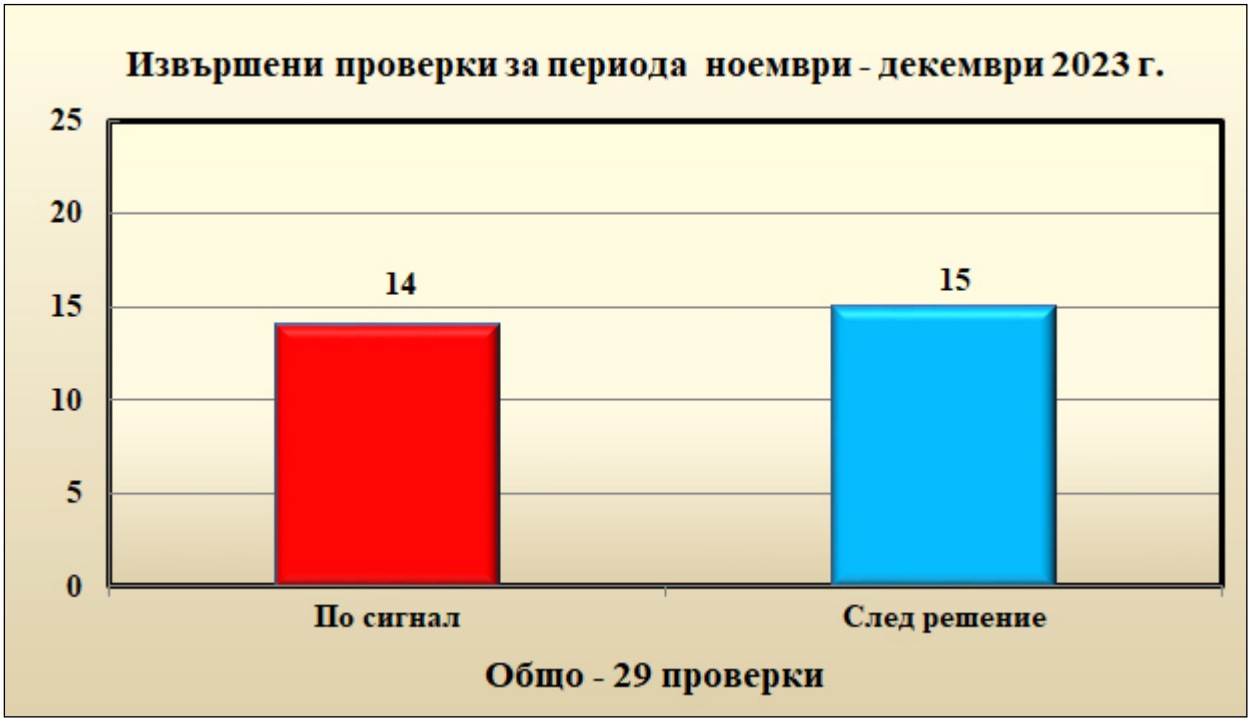
В този контекст работната програма на Координационната група по надзор на Евродак за периода 2022-2024 г. включва въпросът за достъпа на правоприлагащите органи до системата. Оценката на текущото използване на тази процедура изглежда особено интересна, за да хвърли светлина върху статистическите данни и от гледна точка на бъдещите промени, засягащи системата Евродак.

Като допълнение към вече приетия общ план за инспекция и механизми за докладване, Групата предложи изготвянето на контролен списък за наблюдение, специално посветен на достъпа на правоприлагащите органи до данните на Евродак. Контролният списък е структуриран на основата на регламента за Евродак, за да се изолират съответните задължения и да се подчертаят различните стъпки от процедурата за достъп. В резултат на това контролният списък изброява елементи, които могат да бъдат проверени в хронологичен ред на всяка стъпка от процедурата за достъп до данните в Евродак от правоприлагащите органи. Всяко задължение, съдържащо се в регламента, е отразено. Той също така включва по-общ раздел за мерките за сигурност и предлага да се поставят под въпрос елементи от контекста, за да се улесни оценката. Структурата на въпросника предполага неговото допълване.

Eurodac SCG

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА НОЕМВРИ-ДЕКЕМВРИ 2023 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета, през месеците ноември и декември 2023 г. са извършени общо 29 проверки – 14 след постъпили в КЗЛД сигнали и 15 след решение на КЗЛД.



Разгледани са 58 искания, включително различни запитвания по актуални въпроси, относно защита на физическите лица във връзка с обработването на лични данни. По подадените сигнали, за изясняване на факти и обстоятелства са изисквани становища от съответните администратори на лични данни във връзка с твърденията за нарушения на законодателството в областта за защита на личните данни. На всички податели са изпратени съответните отговори за предприетите действия и резултати, а когато е необходимо са изпращани и на съответните органи или институции, за отношение по компетентност.

Във връзка с констатации, че с определени операции по обработване на лични данни са нарушени разпоредби на регламента, за отчетния период КЗЛД е упражнила корективни правомощия по чл. 58, § 2 от Регламент (ЕС) 2016/679, като на съответните администратори на лични данни са издадени 7 разпореждания, отправено е 1 предупреждение и е наложена 1 имуществена санкция/глоба.

РЕШЕНИЯ ПО ЖАЛБИ

КЗЛД публикува в своя бюлетин и на институционалния си сайт решения по жалби, с цел **да се осигури прозрачност за обществеността относно практиката** на Комисията при разглеждането на жалби на граждани. За постигането на тази цел не е необходимо публикуване на всички решения на КЗЛД по жалби, а отразяване произнасянето на Комисията по различни казуси. Всички публикувани решения на КЗЛД са с анонимизирани лични данни на физическите лица и голяма част от имената на юридическите лица.

РЕШЕНИЕ
№ ППН-01-556 /2022/
София, 06.11.2023 г.

Комисията за защита на личните данни в състав: председател – Венцислав Караджов и членове – Цанко Цолов, Мария Матева, Веселин Целков, на редовно заседание, проведено на 19.07.2023 г., на основание чл. 10, ал. 1 от Закона за защита на личните данни, чл. 57, § 1, б. „е" от Регламент 2016/679 и чл. 40, ал. 1 от Правилника за дейността на КЗЛД и на нейната администрация /ПДКЗЛДНА/ разгледа по основателност жалба № ППН-01-556/31.08.2022 г.

Комисията за защита на личните данни е сезирана с горепосочената жалба с твърдения за злоупотреба с личните данни на г-жа М.Й. от „К.Г." ЕООД. Дружеството е подало информация за наличие на сключен трудов договор за длъжност „готвач" в стопанисван от същото ресторант без знанието и съгласието на субекта на данни. Жалбоподателката изразява притесненията си от процесното обработване, посочва, че не желае да се асоциира с ресторанта и разчита на контрол от страна на КЗЛД.

Въз основа на чл. 26 от АПК и чл. 38, ал. 2 от ЗЗЛД страните са уведомени за образуваното административно производство, като са им указани процесуалните права съобразно реда на АПК, по който се развива производството /ППН-01-556#1/24.10.2022/.

Отговор от „К.Г." ЕООД на поредни запитвания /ППН-01-556#4/2022, ППН-01-556#5/2022, ППН-01-556#8/2023/ не е постъпил в 7-дневния срок, определен от КЗЛД.

Въз основа на изискана информация от НАП относно данни за сключен трудов договор с г-жа М.Й. /ППН-01-556#2/24.10.2022, ППН-01-556#6/18.01.2023/, са представени отговори /ППН-01-556#3/31.10.2022 г. и № ППН-01-556#7/2023 г./, както следва: в системата на НАП има данни за регистрирано уведомление по чл. 62, ал. 5 от Кодекса на труда /„КТ"/ от „К.Г." ЕООД за сключен трудов договор на 21.07.2022 г. с жалбоподателката, както и за уведомление по чл. 62, ал. 5 от КТ за прекратяване на договора, считано от 17.08.2022 г.

Жалбата е разгледана по редовност и допустимост по реда на чл. 38, ал. 1 от ПДКЗЛДНА, като са конституирани следните страни: М.Й. – жалбоподател, „К.Г." ЕООД – ответник.

Страните са редовно уведомени за насроченото за 19.07.2023 г. заседание за разглеждане на жалбата по същество /уведомление ППН-01-556#13/19.06.2023 и ППН-01-556#14/19.06.2023/.

Въз основа на допълнителни запитвания до НАП /ППН-01-556#15/19.06.2023 и ППН-01-556#18/07.07.2023/, постъпва отговор /ППН-01-556#16/05.07.2023/ с данни за адрес за кореспонденция по чл. 8 от ДОПК с дружеството „К.Г." ЕООД.

Повторно са изискани информация и доказателства от ответника /ППН-01-556#12/12.05.2023,

ППН-01-556#17/05.07.2023, ППН-01-556#19/10.07.2023/, като съобщенията са се върнали „непотърсени” или отговор не е постъпил в указания от Комисията срок.

С протокол /ППН-01-556#20/11.07.2023/ е приобщена към административната преписка информация от значение за прилагането на чл. 10г от ЗЗЛД, като е установено, че администраторът е „малко” предприятие по смисъла на чл. 3, ал. 2 от Закона за малките и средни предприятия.

Постъпва отговор ППН-01-556#24(22)/19.07.2023 г. от ответника, с който се представя незаверено копие от следните документи:

- трудов договор , длъжностна характеристика за длъжността „готвач”, декларации по Кодекса на труда, заповед за прекратяване на трудовото правоотношение, всичките неподписани от жалбоподателката М.Й.;

- документ, адресиран до ИА „Главна Инспекция по труда”, дирекция ИТ – Б., представляващ обяснение на управителя на „К.Г.” ЕООД, неподписано сведение от помощник барман, протоколи за неявяване на работа на г-жа М.Й., подписани от лица, сочени за служители на „К.Г.” ЕООД;

- справка за приети и отхвърлени уведомления по чл. 62, ал. 5 от КТ относно сключен трудов договор за длъжността „готвач”; справка за уведомление по чл. 62, ал. 5 от КТ за прекратяване на трудовото правоотношение.

При така установеното от фактическа страна, от правна страна жалбата се явява допустима и основателна.

Комисията е независим надзорен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Регламент 2016/679 и ЗЗЛД.

Жалбата попада в законоустановената компетентност на КЗЛД съобразно чл. 6, ал. 1 от ЗЗЛД, като не са налице изключенията, визирани в чл. 2, § 2 от Регламента.

Предмет на жалбата е твърдение за обработване на лични данни в противоречие с Регламента от администратора „К.Г.” ЕООД чрез съвкупност от дейности като събиране, съхранение, употреба и разпространение на лични данни към приходната администрация. Нарушението се установява безспорно въз основа на представените доказателства от НАП и от администратора на лични данни.

От доказателствата, постъпили с отговор ППН-01-556#24(22)/19.07.2023 г. на „К.Г.” ЕООД е видно, че жалбоподателката не е положила подпис върху трудов договор или друг документ, свързан с възникването на твърдяното трудово правоотношение. Независимо от това, данните ѝ са използвани за целите на регистриране на трудов договор в приходната администрация, след което са предприети действия по неговото прекратяване.

Личните данни, предмет на незаконосъобразно обработване, са данните от личната карта на лицето, като по-конкретно предмет на разпространение са данните, необходими за изпращането на уведомления към НАП – три имена и ЕГН /арг. от чл. 5, т. 2 от Наредба № 5 от 29 декември 2002 г. за съдържанието и реда за изпращане на уведомлението по чл. 62, ал. 5 от Кодекса на труда – „Наредбата”/.

Жалбата е съобразена с изискванията за редовност на чл. 29 от АПК, чл. 38а от ЗЗЛД и чл. 28, ал. 1 от ПДКЗЛДНА. Комисията за защита на личните данни е сезирана с писмено искане, съдържащо данни за жалбоподателя, естество на искането, дата на узнаване на нарушението, лице, срещу което се подава жалбата, дата и подпис.

Жалбата е процесуално допустима на основание чл. 27, ал. 2 от АПК, а именно:

- няма влязъл в сила административен акт със същия предмет и страни;

- няма висящо административно производство със същия предмет, пред същия орган и с участието на същата страна, независимо дали е във фазата на издаване или оспорване;

- няма въпрос от компетентност на друг орган, когато актът не може да бъде издаден без предварителното решаване на този въпрос;

- страните в производството имат дееспособност, съответно процесуална правоспособност;

- заявителят има правен интерес от подаване на жалбата – защита на свое основно право за защита на данните.

Жалбата е подадена в срока за сезиране на Комисията по чл. 27, ал. 2, т. 6 от АПК във вр. с чл. 38, ал. 1 от ЗЗЛД.

Разгледана по същество, жалбата се явява основателна.

Администраторът не е доказал съответствие на дейностите по сключване и регистриране на трудовия договор в НАП с разпоредбите на Регламента и на ЗЗЛД.

Не е представено писмено заявление за постъпване на работа, носещо подписа на жалбоподателката г-жа М.Й., не са представени предварителен или окончателен договор, сключен със субекта на данни, следователно администраторът не е доказал в хода на настоящото административно производство, че се е сдобил правомерно с личните данни на жалбоподателката, нито че ги е използвал законосъобразно за целите на регистриране и прекратяване на трудов договор със същата.

Законосъобразността на процесното обработване изисква наличието на сключен писмен трудов договор със служителя, едва след което следва да се изпрати уведомление до приходната администрация, като според приложимата законова и подзаконова нормативна уредба тези действия се извършват преди постъпване на работа на служителя /на основание чл. 62, ал. 3 от КТ уведомлението до НАП се изпраща в тридневен срок от сключването или изменението на трудовия договор, както и в седемдневен срок от неговото прекратяване/. Работодателят следва да изпълни задължението си по чл. 63, ал. 1 от КТ, а именно: да предостави на работника или служителя преди постъпването му на работа екземпляр от сключения трудов договор, подписан от двете страни, както и копие от уведомлението по чл. 62, ал. 3, заверено от съответната териториална дирекция на Националната агенция за приходите. Същото не е доказано да е изпълнено, като администраторът не представя нито доказателства за двустранно подписан сключен трудов договор, нито такива за връчено копие от горепосоченото уведомление /напротив – представен е набор от документи, никой от които не носи подписа на субекта на данни, а представените писмени сведения на служителите, адресирани до Инспекцията по труда, не представляват доказателствено средство по смисъла на чл. 39, ал. 1 от АПК, доколкото е налице специален закон /Кодекса на труда/, който предписва писмена форма за доказване и за действителност на трудовия договор.

Дори и да бяха спазени горецитираните разпоредби, то в случай на неявяване на работника или служителя на работа, трудовото правоотношение се смята невъзникнало /по арг. от 63, ал. 3, изр. 2 от КТ/, в който случай работодателят е длъжен да изпрати до НАП уведомление за заличаване в тридневен срок по реда на чл. 7, т. 1 от Наредбата, а не уведомление за прекратяване на трудовия договор. За да бъде прекратено едно правоотношение, е необходимо на първо време същото да съществува. Доколкото в настоящия случай трудово правоотношение не е възникнало, администраторът неправилно е приложил разпоредбата на чл. 3, ал. 1, т. 2 от Наредбата, като е подал уведомление за прекратяване, а не за заличаване.

Горепосочените обстоятелства водят до недвусмислен извод за извършено нарушение на принципа по чл. 5 § 1, б. „а” от Регламента, доколкото обработването е извършено без основание, поради това, че за субекта на данни не е ясно въз основа на какво, в какви срокове и за какви цели се събират, съхраняват и обработват личните му данни, както и как да упражни правата си по Регламента, като за така установеното нарушение способства обстоятелството, че не са представени или публикувани правила и политики за защита на данните, от които да е ясно как се обработват личните данни в процесите, свързани с възникването, съществуването и прекратяването на трудовите договори.

Не са налице основанията за обработване на лични данни, регламентирани в чл. 6, § 1 от Регламент 2016/679, а именно:

- Няма изразено съгласие по смисъла на чл. 4, т. 11 и чл. 7, т. 1 от Регламента – свободно дадено, предоставено за изрични, конкретно указани и легитимни цели, което да може да бъде оттеглено също толкова лесно, колкото и да бъде предоставено.

- Обработването не е необходимо за изпълнението на договор, по който субектът на данните е страна, доколкото трудов договор в законоизискуемата писмена форма не е сключен. В тази връзка, дейностите по разпространение на лични данни пред приходната администрация се явяват без законово основание, доколкото е налице формална процедура по гл. V от Кодекса на труда и Наредба № 5/29.12.2002 г., въз основа на която следва да е налице писмена форма за действителност на трудовия договор, едва след което биха могли да се извършват дейности по разпространяване на информация пред НАП.

- Не е относима и хипотезата на предприемане на стъпки по искане на субекта на данни преди сключването на договор – не е налице подписано заявление от страна на служителя за постъпване на работа, предварителен договор и др.

- Обработването не е необходимо за спазването на законово задължение /подаване на уведомление до НАП/, което се прилага спрямо администратора – такова задължение възниква само при наличието на действително възникнало трудово правоотношение.

- Не са налице и останалите основания за законосъобразност на обработването – обработването не е необходимо, за да бъдат защитени жизненоважни интереси на субекта на данни или на друго физическо лице, не е необходимо за изпълнението на задача от обществен интерес, не е извършено при упражняването на официални правомощия, които са предоставени на администратора, не е необходимо за целите на легитимните интереси на администратора или на трета страна.

При така констатираното нарушение ефективни, възпиращи и пропорционални мерки, които биха имали необходимия превантивен ефект спрямо администратора, са тези по чл. 58, § 2, б. „г" и б. „и" от Регламента.

При така извършеното нарушение са налице повече от една операции по обработване на лични данни, извършени без основание по смисъла на чл. 6, § 1 от Регламент 2016/679 и в нарушение на принципа на чл. 5 § 1, б. „а" от Регламента, а именно – събиране на личните данни на жалбоподателката и разпространение на същите пред приходната администрация.

По тези съображения и на основание чл. 58, § 2, б. „г" от Регламента следва да се разпореди на администратора „К.Г." ЕООД да съобрази операциите по обработване на лични данни с разпоредбите на Регламента, като за целта въведе вътрешни правила и политики за защита на данните, така че да се осъществи превантивната функция, характерна за санкцията.

Поради липсата на основание за обработване на личните данни на г-жа М.Й., както и предвид необходимостта от преустановяване на незаконосъобразното съхранение на такива данни, на администратора следва да се разпореди да изтрие данните, събрани и съхранявани без основание, като за да докаже изпълнението на разпореждането следва да представи протокол за унищожаване и изтриване на данни, подписан от поне двама свидетели.

Като се вземе предвид, че спрямо администратора следва да се предприемат корективни мерки, достатъчни да гарантират превенция спрямо евентуални бъдещи нарушения, то на администратора „К.Г." ЕООД следва да се наложи кумулативно с горепосоченото разпореждане и имуществена санкция.

При съобразяване на обстоятелствата по чл. 83, § 2 от Регламента се установява следното:

- Нарушението представлява обработване на личните данни на един субект, така че биха могли да възникнат негативни последици за същия.

- Нарушението е извършено в период, който не може да се характеризира като кратък – от

21.07.2022 г. /датата на подаване на уведомление до НАП за сключен трудов договор/ до 17.08.2022 г. /дата на подаване на уведомление за прекратяването му/, при положение, че е следвало невярно разпространената информация да бъде заличена своевременно в тридневния срок по чл. 7, т. 1 от Наредбата. Няма доказателства администраторът да е прекратил неоснователното съхранение на лични данни, респективно нарушението да е преустановено към настоящия момент.

- Доколкото администраторът не е физическо лице, въпросът за умисъла не е приложим.

- Не е констатирано да са предприети действия за смекчаване последиците от нарушението.

- Администраторът не оказва навременно съдействие на Комисията при осъществяване на нейните функции и правомощия, като не е отговарял в срок на запитванията, а с предоставения на 19.07.2023 г. отговор само се препраща информация, вече предоставена на други институции, въз основа на същия казус, вместо да се даде отговор на поставените въпроси.

- Отговорността на администратора се обуславя от това, че същият не е предприел организационни и технически мерки, включително няма представени или публично оповестени правила за защита на данните, така че да може да се възприеме, че е минимизирал риска от нарушения, както в разглеждания случай, така и занапред.

- Администраторът няма предишни нарушения на Регламента, констатирани от надзорния орган.

- Сред личните данни, засегнати от нарушението, не е установено да има специални категории по смисъла на чл. 9 от Регламента.

- Нарушението е сведено до знанието на надзорния орган по жалба на субекта на данни, а не въз основа на уведомление от страна на администратора.

Администраторът има качеството „малко" предприятие по смисъла на чл. 3, ал. 2 от ЗМСП. Съобразно чл. 10г от ЗЗЛД Комисията, вземайки предвид специалните му потребности и налични ресурси, не следва с наложената санкция да затруднява евентуално осъществяваната стопанска дейност от предприятието.

Съобразявайки елементите по чл. 83, § 2 от Регламента, предвид това, че санкцията не се налага самостоятелно, а кумулативно с разпореждане, съобразявайки принципа на съразмерност по чл. 6, ал. 2 от АПК, надзорният орган намира за достатъчно санкцията да бъде определена в минимума съобразно лимитите на чл. 83, § 5 от Регламента, като по този начин същата би имала възпиращ ефект дори в своя минимум и едновременно с това не би засегнала администратора повече от необходимото за целта, с което отговаря на изискването на пропорционалност.

Предвид гореизложеното и на основание чл. 38, ал. 3 от ЗЗЛД Комисията за защита на личните данни с 4 гласа „за" и 0 „против"

РЕШИ:

1. Обявява жалба № ППН-01-556/31.08.2022 г. на М.Й. срещу „К.Г." ЕООД за основателна за нарушение на чл. 6, § 1 и чл. 5 § 1, б. „а" от Регламент 2016/679.

2. На основание чл. 58, § 2, б. „г" от Регламента издава разпореждане на администратора „К.Г." ЕООД да съобрази операциите по обработване на лични данни с разпоредбите на Регламента, като за целта приеме вътрешни правила и политики за защита на личните данни, изтрие/унищожи личните данни на жалбоподателката, документира същото с протокол, подписан от поне двама свидетели, представи доказателства за изпълнение на решението в едномесечен срок, считано от влизането му в сила.

3. На основание чл. 58, § 2, б. „и" във вр. с чл. 83, § 5, б. „а" от Регламент 2016/679 налага имуществена санкция от 2 000 /две хиляди/ лева на администратора на лични данни „К.Г." ЕООД .

Имуществената санкция да бъде изплатена в 14-дневен срок, считано от влизане в сила на настоящото Решение, по следната банкова сметка на КЗЛД в БНБ:

IBAN: BG18BNBG96613000158601 BIC BNBGBGSD

Титуляр: Комисия за защита на личните данни

БУЛСТАТ 130961721.

В случай, че санкцията не бъде изплатена в горепосочения срок, ще бъдат предприети действия по принудително изпълнение.

Настоящото решение може да бъде обжалвано чрез Комисията за защита на личните данни пред Административен съд София-град в 14-дневен срок, считано от връчването му.

ПРЕДСЕДАТЕЛ:

Венцислав Караджов /п/

ЧЛЕНОВЕ:

Цанко Цолов /п/

Мария Матева /п/

Веселин Целков /п/

СТАНОВИЩЕ
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-01-92/2023 г.
гр. София, 13.11.2023 г.

ОТНОСНО: *Ред за унищожаване на регистрационни карти на чужденци с предоставена временна закрила, издадени от Държавната агенция за бежанците при Министерския съвет*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на свое редовно заседание, проведено на 08.11.2023 г., разгледа писмо с рег. № ПНМД-01-92/19.10.2023 г. от председателя на Държавната агенция за бежанците при Министерския съвет (ДАБ при МС). В него се посочва, че на територията на Европейския съюз е въведена временна закрила с Решение за изпълнение (ЕС) 2022/382 на Съвета от 4 март 2022 година за установяване на съществуването на масово навлизане на разселени лица от Украйна по смисъла на член 5 от Директива 2001/55/ЕО и за въвеждане на временна закрила. Въз основа на посоченото решение и в съответствие с чл. 2, ал. 2 от Закона за убежището и бежанците (ЗУБ), с Решение № 144 от 10 март 22 г. на Министерския съвет, временна закрила в Република България се предоставя на разселените лица от Украйна, считано от 24.02.2022 г. Към настоящия момент срокът на действие на временната закрила в Република България е до 04.03.2024 г.

Съгласно Националния план за действие при временна закрила в Република България отговорностите на ДАБ при МС са свързани с изпълняване на функции по организиране на процесите по предоставяне на временна закрила.

На основание чл. 41, ал. 1 от ЗУБ ДАБ при МС издава регистрационна карта на чужденец, на когото е предоставена временна закрила за срока на действие на закрилата. Образецът на регистрационна карта на чужденец, на когото е предоставена временна закрила, е утвърден с Решение № 96 от 1 февруари 2023 г. за изменение на Решение № 642 на Министерския съвет от 2016 г. за утвърждаване на образци на регистрационни карти, които се издават от ДАБ при МС, изменено с Решение № 242 на Министерския съвет от 2022 г. Регистрационните карти, издавани от ДАБ при МС, не са документ за самоличност по смисъла на Закона за българските личните документи.

Регистрационните карти се издават в един екземпляр и съдържат следните данни - ЛНЧ; имена; дата и място на раждане; пол; гражданство; настоящ адрес; № на национален документ за самоличност; снимка и подпис на лицето; име, дата на раждане и ЛНЧ на придружаващи деца под 14-годишна възраст; дата на издаване и дата на валидност на регистрационната карта. Към настоящия момент всички регистрационни карти са със срок на валидност 04.03.2024 г.

Във връзка с необходимостта от създаване на организация за унищожаване на издадените регистрационни карти, чийто срок на валидност предстои да изтече и с оглед спазване разпоредбите на Регламент (ЕС) 2016/679 и Закона за защита на личните данни, от ДАБ молят за становище по следните въпроси:

1. Какъв е редът, по който следва да се осъществи физическото унищожаване на регистрационните карти след изтичане на срока им на валидност; след отпадане на основанието, поради което същите са издадени или след обявяването им за невалидни в Автоматизираната информационна система (АИС) поради технологични причини?

2. В какъв срок след изтичане на срока на валидност на регистрационните карти и обявяването им за невалидни в АИС - „Бежанци", същите следва да бъдат физически унищожени?

Правен анализ:

Унищожаването на лични данни е една от операциите по тяхното обработване и традиционно се свързва с края на техния „жизнен цикъл" (арг. чл. 4, т. 2 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД)). Понятието „унищожаване" е легално дефинирано в § 1, т. 19 от Допълнителните разпоредби на Закона за защита на личните данни, според който то представлява необратимо физическо разрушаване на материалния носител на информацията, представляваща лични данни.

По общо правило администраторът пристъпва към това действие, когато е изтекъл срокът за тяхното съхранение. Съгласно принципа за „ограничение на съхранението", прогласен в чл. 5, пар. 1, б. „д" от ОРЗД, личните данни се съхраняват във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват. Личните данни могат да се съхраняват и за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно условията на чл. 89, пар. 1 от ОРЗД, при условие че бъдат приложени подходящи технически и организационни мерки, с цел да бъдат гарантирани правата и свободите на субекта на данните.

Видно от разпоредбите на Закона за убежището и бежанците (ЗУБ) липсва нормативен ред, по който да се съхраняват и унищожават върнатите от бежанците техни регистрационни карти поради изтичане на срока им на валидност.

Решение за изпълнение (ЕС) 2022/382 на Съвета от 4 март 2022 година за установяване на съществуването на масово навлизане на разселени лица от Украйна по смисъла на член 5 от Директива 2001/55/ЕО и за въвеждане на временна закрила също не предвижда такива правила, но в съображение 19 от същото се посочва, че когато предоставят временна защита, държавите членки следва да гарантират, че при обработването на лични данни на лицата, ползващи се с временна закрила, се спазват изискванията, установени в достиженията на правото на Съюза в областта на защитата на данните, по-специално в Регламент (ЕС) 2016/679.

Доколкото липсват специални нормативни правила в това отношение, администраторът – ДАБ при МС, следва да приложи общите правила на ОРЗД за унищожаване на личните данни, съдържащи се във върнатите регистрационни карти на бежанците. За тази цел той трябва да въведе подходящи технически и организационни мерки, които да отчитат естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица (арг. чл. 24 от ОРЗД). Тези мерки трябва да включват вътрешни правила и процедури, чрез които да се регламентират фактическите и правните действия по унищожаване на регистрационните карти на бежанците.

Чрез нарочен акт (напр. заповед на председателя на ДАБ при МС) **следва да се определят ангажираните с тази дейност длъжностни лица, сроковете, последователността от действия, както и надлежно документиране, с цел отчетност и пълна проследимост, на дейностите по унищожаване на всяка регистрационна карта**. С оглед на това добра практика е унищожаването да се документира от специално определена за тази цел комисия, която да протоколира предприетите от нея действия. Доколкото в специалното законодателство не е предвиден и срок за съхранението и последващото унищожаване на върнатите от бежанците регистрационни карти, ДАБ при МС следва да определи такъв, като той трябва да е пропорционален, адекватен и подходящ. Разбира се, този срок трябва да отчита и въведената организация на работа по тяхното унищожение, за да бъде ефективен и реално изпълним.

От гледна точка на законодателството за защита на личните данни няма пречка унищожаването на регистрационните карти да се осъществява още към момента на тяхното връщане (на гише) в ДАБ при МС и нейните териториални поделения в страната. По този начин ще се избегне събирането на

множество регистрационни карти, които да бъдат съхранявани (макар и за кратък срок) и впоследствие унищожавани. В такъв случай, след като съответните служители на ДАБ при МС се уверят, че при тях се връща именно регистрационна карта с изтекъл срок на валидност, преди да я унищожат, те трябва да направят съответното отбелязване за това в Автоматизираната информационна система (АИС). Системата следва да позволява пълна отчетност и проследимост за всяка върната карта, вкл. за действията по нейното унищожаване.

В случай че дейността по унищожаване на регистрационните карти бъде възложена на външен изпълнител, между ДАБ при МС и него ще възникне отношение администратор – обработващ лични данни. По силата на чл. 28 от ОРЗД то трябва да бъде скрепено чрез писмен договор (споразумение), който да е наличен вкл. в електронна форма и да съдържа всички реквизити, посочени изчерпателно в параграф 3, буква „а" до „з" от същата разпоредба. С цел улеснение на договарящите се страни, на основание чл. 28, пар. 7 от ОРЗД Европейската комисия е приела т.нар. стандартни договорни клаузи между администратори и обработващи лични данни[1] (бланкови договорни клаузи), които отразяват всички изисквания на ОРЗД и могат да бъдат ползвани от тях напълно безплатно.

Не на последно място, при разработването и въвеждането на вътрешните си правила и процедури за унищожаване на регистрационните карти, ДАБ при МС би могла да се води (като добра практика) от режима на Инструкция № Із-59 от 11.01.2011 г. за реда и условията за унищожаване на българските лични документи, издадена от министъра на вътрешните работи.

По тези съображения и на основание чл. 58, пар. 3, б. „б" от Регламент (ЕС) 2016/679 във вр. с чл. 10а, ал. 1 от Закона за защита на личните данни и чл. 51, т. 2 и чл. 12 от Правилника за дейността на КЗЛД и на нейната администрация, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

От гледна точка на законодателството за защита на личните данни няма пречка унищожаването на регистрационните карти да се осъществява още към момента на тяхното връщане (на гише) в ДАБ при МС и нейните териториални поделения в страната. По този начин ще се избегне събирането на множество регистрационни карти, които да бъдат съхранявани (макар и за кратък срок) и впоследствие унищожавани.

В такъв случай, след като съответните служители на ДАБ при МС се уверят, че при тях се връща именно регистрационна карта с изтекъл срок на валидност, преди да я унищожат, те трябва да направят съответното отбелязване за това в Автоматизираната информационна система (АИС). Системата следва да осигурява пълна отчетност и проследимост за всяка върната карта, вкл. за действията по нейното унищожаване.

ПРЕДСЕДАТЕЛ:
Венцислав Караджов /п/

ЧЛЕНОВЕ:
Цанко Цолов /п/
Мария Матева /п/

1 Те са инкорпорирани в Решение за изпълнение (ЕС) 2021/915 на ЕК от 4 юни 2021 година относно стандартни договорни клаузи между администратори и обработващи лични данни съгласно член 28, параграф 7 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета и член 29, параграф 7 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета

СТАНОВИЩЕ
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ПНМД-17-239/2023 г.
гр. София, 24.11.2023 г.

ОТНОСНО: *Законосъобразност на видеонаблюдение за целите на оценка на представянето и изпълнението на трудовите задължения на служители във връзка с определянето на допълнителното им трудово възнаграждение*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на свое редовно заседание, проведено на 15.11.2023 г., разгледа писмо с вх. № ПНМД-17-239/20.10.2023 г. от „ЛУКОЙЛ – България“ ЕООД (Дружеството), с което се иска становище относно законосъобразността при използването на видеонаблюдение за оценка на представянето и изпълнението на трудовите задължения на служители му във връзка с определянето на тяхното допълнително трудово възнаграждение.

Дружеството притежава верига бензиностанции (обекти/бензиностанции) на територията на страната, на които се осъществява видеонаблюдение с оглед защита на легитимните му интереси. То е в процес на разработване на система, при която, въз основа на предварително определени критерии за изпълнение на компоненти на трудовите задължения, за служителите по обектите да бъдат предоставяни бонуси към трудовите им възнаграждения. Целта на Дружеството, като работодател, е да има обективно наблюдение за представянето на своите служители по обектите, а не да разчита на субективната преценка на регионалните мениджъри, които пряко отговарят и наблюдават работата на бензиностанциите и на служителите, които работят на тези обекти. Именно, за да има обективност при оценяване изпълнението на компонентите на трудовите задължения от тези служители, Дружеството изразява желание да използва наличните системи за видеонаблюдение по обектите.

Процесът по наблюдение на видеосистемите за посочените цели ще се извършва изцяло от служители на Дружеството, предоставящи работната си сила извън обектите и извън всякакъв контакт със служителите на въпросните обектите. Тези служители, отговарящи за наблюдението на видеосистемите, периодично, след обективно отчитане на изпълнението на конкретни задължения с оглед спазването на стандартите на Дружеството за висококачествено обслужване, ще изготвят справки за представянето на служителите. С оглед на данните от справките, на служителите на обектите периодично ще бъде изплащан бонус (възнаграждение с променлив характер). От дружеството подчертават, че видеонаблюдението за представянето на служителите, съответно – справките, по никакъв начин не засягат и няма да променят трудовото възнаграждение с постоянен характер. При определяне на възнагражденията с променлив характер, и с оглед яснота за формирането им, служителите ще имат право на преглед на видеозаписите, което означава, че дейността по обработването на лични данни ще се извършва в условията на пълна прозрачност. Служителите, като субекти на обработваните данни, ще бъдат информирани за целите на такова обработване, като ще бъдат осигурени и всичките им права по приложимото законодателство в областта на защитата на личните данни.

С оглед на описаната фактическа обстановка, разбирането на Дружеството е, че доколото подобно видеонаблюдение, а по възможност - и аудиозапис, води до придобивки за служителите, работодателят би могъл да въведе подобна система. По мнение на Дружеството, при нейното прилагане се защитава легитимният интерес на работодателя, а именно – поддържане на качествено обслужване на клиентите на обектите, като същевременно се обслужва и интереса на работника да получава допълнително възнаграждение с променлив характер. В тази връзка намират, че такова

обработване на лични данни е справедливо за служителите. За яснота в писмото се посочва, че към момента в Дружеството действа система за определяне на бонуси, като част от предоставяния бонус по нея зависи от субективен фактор, каквато е преценката на съответните регионални мениджъри за представянето на служителите по обектите. Желанието на Дружеството, като работодател, е да избегне именно субективния фактор, като допълнителните възнаграждения се определят на базата на обективни данни от видеозаписи (а по възможност - и на аудиозаписи), ясно показващи конкретното изпълнение на конкретни задължения от страна на служителите.

С оглед гореизложеното, Дружеството моли КЗЛД да изрази становище по следните въпроси:

1. Възможно и законосъобразно ли е използването на видеонаблюдение за оценка на представянето и изпълнението от страна на служителите на обектите на компоненти от трудовите им задължения, по предварително определени критерии и с цел заплащане на лицата на допълнителни възнаграждения с променлив характер, без по никакъв начин това да засяга трудовите възнаграждения с постоянен характер?

2. Възможно и законосъобразно ли е в допълнение на горното и със същите цели и при същите критерии, да се използват и аудиозаписи?

3. Следва ли работодателят да извърши предварителни действия и какви, тъй щото обработването на лични данни на служителите по посочения начин, да се извършва в съответствие с ОРЗД и ЗЗЛД?

Правен анализ:

Видеонаблюдението е дейност, свързана със събиране и съхранение на образни или аудиовизуални данни за лица, попадащи в обхвата на наблюдавана зона, които подлежат на пряко или косвено идентифициране въз основа на техния външен вид или други специфични признаци. Съществен елемент от тази дейност е, че самоличността на лицата може да бъде установена въз основа на тези данни, а също така се създава възможност за обработване на данни относно присъствието и поведението на лицата в съответната зона. В този смисъл видеонаблюдението попада в материалния обхват на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) и Закона за защита на личните данни (ЗЗЛД) и следва да се осъществява съобразно техните изисквания.

По общо правило, за да бъде обработването на лични данни законосъобразно в рамките на обхвата на ОРЗД, то трябва да се осъществява въз основа на някое от правните основания, посочени в чл. 6, пар. 1 и/или чл. 9, пар. 2 от същия, както и да бъдат приложени ефективно принципите, прогласени с неговия чл. 5.

Регламент (ЕС) 2016/679 въвежда специални правила относно обработването на лични данни в контекста на трудово или служебно правоотношение. Съгласно чл. 88, пар. 2 от ОРЗД правилата, които се приемат в националните законодателства на държавите членки, трябва да включват подходящи и конкретни мерки за защита на човешкото достойнство, законните интереси и основните права на субекта на данните, по-специално по отношение на прозрачността на обработването, предаването на лични данни в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност и **системите за наблюдение на работното място**.

Задължително условие е работниците и служителите да се уведомяват за тези системи, както и за правилата и процедурите, които се въвеждат от работодателите. Нещо повече, задължение на администратора е, още на етапа на планирането на въвеждане на системи за наблюдение, да се извърши прецизна оценка на риска за правата и свободите на субектите на данни, които с различна вероятност и тежест, могат да произтичат от конкретното обработване на лични данни. В този смисъл, по аргументи от съображение (75) от преамбюла на Регламент (ЕС) 2016/679, дейността по анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място изначално е изведена, като високорискова. Това предполага, преди да започне конкретното обработване

да се извърши и оценка на въздействието върху защитата на личните данни, като съществен елемент от нея са становищата на длъжностното лице по защита на данните и на засегнатите субекти на данни (в случая – работниците и служителите в търговските обекти, както и третите лица, които ги посещават, доколкото става въпрос за обществено достъпна зона и се засяга голям брой субекти на данни).

В конкретния случай става въпрос за голям брой търговски обекти, представляващи публично достъпни зони, което предполага, че същите се посещават от неограничен брой лица. Сред тези лица могат да се установят различни категории субекти на данни, като служители, клиенти, посетители и други лица, както и деца, които при посещение на бензиностанция, попадат в обхвата на системата ѝ за видеонаблюдение. Това означава, че в обхвата на видеонаблюдението попадат освен лицата, които имат пряко отношение към оценката на трудовото изпълнение, но и голям брой други лица, които нямат връзка с него и се явяват трети лица.

Съгласно законодателството за защита на данните, лицата имат право на достъп само до свои лични данни, но не и до данни на трети лица. В този смисъл, достъпът до личните данни на толкова голям брой субекти – трети лица, от страна на служителите, извършващи оценката на трудовото изпълнение, е неотносимо към целите на обработването. Принципно положение е, че при упражняване на правото на достъп по ОРЗД (напр. чрез предоставянето на копие от записи от видеонаблюдение) не следва да се влияе неблагоприятно върху правата и свободите на други лица (вж. чл. 15, пар. 4 от ОРЗД). В такива случаи администраторът следва да предприеме подходящи технически и организационни мерки за заличаване на образите на заснетите трети лица. В конкретния случай, видеозаписът може да разкрие данни на голям брой трети лица, като е технически невъзможно тези данни да бъдат замъглени, така че да се спазят изискванията на ОРЗД.

По отношение на целите на обработването – оценка на трудовото представяне и изпълнение на служебните задължения на работника/служителя, респ. определянето на съответното допълнително възнаграждение, следва да се има предвид и трудовото законодателство.

Разпоредбите на Кодекса на труда (КТ), макар и приети много преди приемането на действащото законодателство в областта на защитата на личните данни, също въвеждат защитни мерки относно зачитането на неприкосновеността на личното пространство в работен контекст. Така например, съгласно чл. 127, ал. 2 от КТ работодателят е длъжен да пази достойнството на работника или служителя по време на изпълнение на работата. Отношение към планираното обработване на лични данни има и разпоредбата на чл. 107и, ал. 3, т. 7 от КТ, според която работодателят може да въведе, за своя сметка, система за наблюдение, **ако такава се налага** да бъде монтирана на работното място и е получено писмено съгласие на работника или служителя за това, като в тези случаи задължително се зачита правото му на лично пространство. Разпоредбата е приета много преди ОРЗД, но отчита принципното разбиране, че такова обработване на лични данни следва да е справедливо, необходимо и пропорционално. Изразът „ако такава се налага“ предполага, че целите на работодателя не могат да бъдат постигнати с други средства, какъвто не е разглежданият случай.

Съгласно *Насоки № 3/2019 относно обработването на лични данни чрез видеоустройства*, приети от Европейския комитет по защита на данните (ЕКЗД) на 29 януари 2020 г. личните данни следва да са подходящи, относими и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“), вж. чл. 5, пар. 1, б. „в“ от ОРЗД. Преди да предприеме инсталиране на система за видеонаблюдение, администраторът следва във всички случаи внимателно да анализира дали тази мярка е първо, подходяща за постигането на поставената цел и второ, адекватна, и необходима с оглед на неговите цели. Мерки за видеонаблюдение трябва да се предприемат единствено, ако целта на обработването не може да бъде постигната в достатъчна степен с други средства, които водят до по-малка намеса в основните права и свободи на субекта на данните. С още по-голяма сила това важи и за записването на звук (разговори), тъй като той е допълнителна категория лични данни. Освен това, преди да започне да използва система от камери, администраторът е длъжен да оцени къде и в кои случаи мерките за видеонаблюдение са **строго необходими**.

Прекалено интрузивните мерки за наблюдение могат да причинят на служителите ненужен стрес и могат също така да подкопаят доверието в администратора. Използване на видеонаблюдение за целите на проследяване как персоналът изпълнява своите трудови задължения трябва да бъде избягвано, освен в изключителни случаи – когато това се налага от законодателството или при високорискови производствени дейности (напр. във фармацията, химическата промишленост, атомната енергия и пр.). Цели като управление на производителността на работното място, осигуряване на контрол на качеството, прилагане политиките на администратора (работодателя) или осигуряване на доказателства за разрешаване на спорове, сами за себе си не оправдават видеонаблюдението на работното място[1].

Безспорно е, че Дружеството има легитимен интерес (чл. 6, пар. 1, б. „е“ от ОРЗД) да осъществява видеонаблюдение за охранителни цели в своите търговски обекти. Тези, легитимни за администратора цели, включват обезпечаването на сигурността на обектите, защита на живота и здравето на служителите и третите лица (клиенти и посетители), опазване на имуществото и пр. При необходимост, записите от системата за видеонаблюдение могат да бъдат използвани и за целите на разрешаване на клиентски оплаквания или жалби. Обработването обаче на събраните от видеонаблюдението данни за друга цел, каквато е оценяването на личностното представяне и изпълнението на трудовите задължения на служителите за нуждите на определянето на допълнителното им трудово възнаграждение, представлява форма на последващо обработване на лични данни.

Правилата за последващо обработване на лични данни са регламентирани в чл. 6, пар. 4 от ОРЗД, съгласно който когато обработването за други цели, различни от тези, за които първоначално са били събрани личните данни, не се извършва въз основа на **съгласието** на субекта на данните или на **правото** на Съюза или правото на държава членка, което представлява необходима и пропорционална мярка в едно демократично общество за гарантиране на целите по чл. 23, пар. 1 от ОРЗД, администраторът, за да се увери дали обработването за други цели е съвместимо с първоначалната цел, за която са били събрани личните данни, *inter alia*, взема под внимание следните критерии:

- всяка връзка между целите, за които са били събрани личните данни, и целите на предвиденото по-нататъшно обработване;
- контекста, в който са били събрани личните данни, по-специално във връзка с отношенията между субекта на данните и администратора;
- естеството на личните данни, по-специално дали се обработват специални категории лични данни съгласно чл. 9 или се обработват лични данни, отнасящи се до присъди и нарушения, съгласно чл. 10 от ОРЗД;
- възможните последствия от предвиденото по-нататъшно обработване за субектите на данните;
- наличието на подходящи гаранции, които могат да включват криптиране или псевдонимизация.

За планираното обработване на лични данни съгласието е неприложимо основание, поради трудовия контекст. От друга страна, липсва изрично законодателство, което да разрешава подобно видеонаблюдение. Налице е и невъзможност да бъдат изпълнени горепосочените критерии за преценка на съвместимостта между първоначалната и последващата цел. Следователно, може да се направи обосновано заключение, че оценката на личностното представяне и изпълнението на трудовите задължения на служителите за нуждите на определянето на допълнителното им трудово възнаграждение, е друга, последваща цел, която е **абсолютно несъвместима с първоначалната** (охранителната).

Не на последно място, следва да се отбележи, че така планираното обработване на лични данни се отнася и до дейности, които попадат в обхвата на понятието „профилиране“. Съгласно легалната

---

1 The EDPS video-surveillance guidelines, Brussels, 17 March 2010; вж. също Становище № 2/2017 на РГ29 относно обработването на данни на работното място, РД249, прието на 8 юни 2017 г.

му дефиниция в чл. 4, т. 4 от ОРЗД, то означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни **за оценяване на определени лични аспекти**, свързани с физическо лице, и по-конкретно за **анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице**, неговото икономическо състояние, здраве, лични предпочитания, интереси, **надеждност, поведение, местоположение или движение**. По силата на чл. 22 от ОРЗД субектът на данните има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за него или по подобен начин го засяга в значителна степен. Това право не се прилага, когато автоматизираното решение:

- е необходимо за сключването или изпълнението на договор между субект на данни и администратор;
- е разрешено от правото на Съюза или правото на държава членка, което се прилага спрямо администратора, и в което се предвиждат също подходящи мерки за защита на правата и свободите, и легитимните интереси на субекта на данните; или
- се основава на изричното съгласие на субекта на данни.

Нито една от посочените хипотези обаче не е приложима, тъй като сключването и изпълнението на договор между субекта на данни и работодателя му не е сред приложимите основания за последващо обработване на лични данни по смисъла на чл. 6, пар. 4 от ОРЗД. От друга страна, липсват и специални правни норми, които да позволяват обработване на лични данни чрез видеонаблюдение за целите на предоставянето на допълнително възнаграждение. И накрая, въпреки че по смисъла на чл. 6, пар. 4 от ОРЗД съгласието е едно от основанията за допустимост на последващо обработване, в конкретния случай то не може да бъде валидно[2] в отношенията между работодател и работник/служител.

По тези съображения и на основание чл. 58, пар. 3, б. „б“ от Регламент (ЕС) 2016/679 във вр. с чл. 10а, ал. 1 от Закона за защита на личните данни и чл. 51, т. 2 и чл. 12 от Правилника за дейността на КЗЛД и на нейната администрация, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

Последващото обработване на записите от видеонаблюдението, включващо и звукозапис, за целите на оценката на личностното представяне и изпълнението на трудовите задължения на служителите на „ЛУКОЙЛ - България“ ЕООД, за нуждите на определяне на допълнителното им трудово възнаграждение, не съответства на изискванията на чл. 6, пар. 4 от Регламент (ЕС) 2016/679, следователно е недопустимо.

ПРЕДСЕДАТЕЛ:
ВЕНЦИСЛАВ КАРАДЖОВ

ЧЛЕНОВЕ:
ЦАНКО ЦОЛОВ
МАРИЯ МАТЕВА
ВЕСЕЛИН ЦЕЛКОВ

2 Вж. Насоки 5/2020 на ЕКЗД относно съгласието в съответствие с Регламент (ЕС) 2016/679, приети на 4 май 2020 г.

СТАНОВИЩЕ
НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № ППН-02-662/2023 г.
гр. София, 05.12.2023 г.

ОТНОСНО: *Проект на Наредба за изменение и допълнение на Наредба № 1 от 2017 г. за реда за установяване концентрацията на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози, публикуван на Портала за обществени консултации*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на свое редовно заседание, проведено на 29.11.2023 г., разгледа писмо с вх. № ППН-02-662/30.10.2023 г., подадено от адвокат в САК относно публикувания на Портала за обществени консултации (https://www.strategy.bg/[1]) *проект на Наредба за изменение и допълнение на Наредба № 1 от 2017 г. за реда за установяване концентрацията на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози.* Той счита, че е необходимо КЗЛД и Инспекторатът към Висшия съдебен съвет (ИВСС) да изразят становище по подготвяните изменения и допълнения в наредбата, с оглед съществуващия риск от нарушаване на правото на защита на личните данни и правото на неприкосновеност на личния живот на гражданите. Той изразява мнение, че разпоредбите на Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680 не допускат резултатите от изследвания, които контролните органи предписват за целите на осигуряване на пътната безопасност да могат да бъдат ползвани в наказателни производства по подобен на предвидения в проекта начин.

След като подробно излага мотиви за твърдението си, адвокатът подава писмото, озаглавено като „сигнал“ и до двата надзорни органа с оглед тяхната компетентност, както и до Министерство на вътрешните работи, Министерство на правосъдието и Министерството на здравеопазването, като счита, че е налице неопределеност на целите на обработването на лични данни, регламентирано с посочения по-горе проект на наредба – едновременно за целите на контрола по Закона за движението по пътищата (ЗДвП) и за целите на разкриването, разследването и наказването на престъпления по чл. 343б от Наказателния кодекс (НК).

Правен анализ:

Безспорно е, че при установяването на концентрацията на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози се обработват лични данни, при това от категорията на т.нар. специални (чувствителни) лични данни по смисъла на чл. 9 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД). Тяхното обработване по принцип е забранено, освен ако не са налице условията по чл. 9, пар. 2 от същия регламент. В конкретния случай се прилага хипотезата на чл. 9, пар. 2, б. „ж“ от ОРЗД, според която обработването на такива данни е необходимо по причини от важен обществен интерес на основание правото на Съюза или **правото на държава членка**, което е пропорционално 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 данните.

Наредба № 1 от 19 юли 2017 г. за реда за установяване концентрацията на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози е подзаконов нормативен акт, който се

1 https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=7904 (Дата на откриване: 24.10.2023 г., Дата на приключване: 23.11.2023 г.)

издава на основание чл. 174, ал. 4 от Закона за движението по пътищата (ЗДвП). С чл. 174 от ЗДвП се дефинират условията за ангажиране на административнонаказателната отговорност на водачите на моторни превозни средства, които управляват с концентрация на алкохол в кръвта при определени граници и/или след употребата на наркотични вещества или техни аналози. По силата на тази законова разпоредба съответните контролни органи имат задължение да установяват концентрацията на алкохол в кръвта на водачите и/или употребата на наркотични вещества или техни аналози. Следователно чл. 174 от ЗДвП във връзка с чл. 9, пар. 2, б. „ж“ от ОРЗД представлява валидно правно основание за обработването на резултатите от тестовете.

Прецизното и навременно определяне на точните стойности на концентрация на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози са абсолютна предпоставка за ангажирането на съответния вид юридическа отговорност –административнонаказателна или наказателна. За целите на разграничаването на отговорността законодателят е извършил преценка съобразно степента на обществена опасност на деянието като е въвел количествен критерий, според който водачите, управляващи моторно превозно средство с концентрация на алкохол в кръвта си **над 1,2 на хиляда, установено по надлежния ред**, се наказват с лишаване от свобода от една до три години и с глоба от двеста до хиляда лева (арг. чл. 343б, ал. 1 от Наказателния кодекс (НК)). Нормата препраща към надлежния ред за установяване концентрацията на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози, който е установен с Наредба № 1. Следователно чл. 343б от НК във връзка с чл. 49 и чл. 51, ал. 1 от Закона за защита на личните данни (ЗЗЛД) представлява валидното правно основание за обработването на резултатите от тестовете, за да се ангажира наказателната отговорност на лицата.

Следва да се има предвид, че Наредба № 1 се разглежда в контекста на специалното законодателство (ЗДвП и НК), приложимо за дейностите, регламентирани с нея, както и във връзка с приложимите изисквания за защита на личните данни (ОРЗД или ЗЗЛД). Посочените нормативни актове съдържат разпоредби, които вземат предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица. В този смисъл, Наредба № 1 въвежда правила за технологията и организацията на работа на различните участници в процеса по установяване на концентрацията на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози (арг. чл. 7, ал. 2 от Закона за нормативните актове). Тя обаче не създава нови правни основания нито за извършване на контролна дейност от страна на органите по ЗДвП, нито за произтичащото обработване на лични данни и задължението за тяхното незабавно предаване на органа на досъдебното производство. Това задължение за длъжностните лица[2], в конкретния случай, осъществяващи контролна дейност по ЗДвП, възниква по силата на чл. 205, ал. 2 от Наказателно-процесуалния кодекс (НПК)[3].

---

2 **Чл. 93, т. 1 от НК***: „Длъжностно лице“ е това, на което е възложено да изпълнява със заплата или безплатно, временно или постоянно:*
а) служба в държавно учреждение с изключение на извършващите дейност само на материално изпълнение;
б) ръководна работа или работа, свързана с пазене или управление на чуждо имущество в държавно предприятие, кооперация, обществена организация, друго юридическо лице или при едноличен търговец, както и на нотариус и помощник-нотариус, частен съдебен изпълнител и помощник-частен съдебен изпълнител.

3 **НПК, Задължение на гражданите и длъжностните лица за уведомяване**
Чл. 205. (1) Когато узнаят за извършено престъпление от общ характер, гражданите са обществено задължени да уведомят незабавно орган на досъдебното производство или друг държавен орган.
(2) Когато узнаят за извършено престъпление от общ характер, длъжностните лица трябва да уведомят незабавно органа на досъдебното производство и да вземат необходимите мерки за запазване на обстановката и данните за престъплението.
(3) В случаите на ал. 1 и 2 органът на досъдебното производство незабавно осъществява правомощията си за образуване на наказателното производство.

Съгласно съображение (50) от преамбюла на ОРЗД „*съобщаването от администратора за евентуални престъпни деяния или заплахи за обществената сигурност и предаването на съответните лични данни в отделни случаи или в няколко случая, свързани с едно и също престъпно деяние или заплахи за обществената сигурност, на компетентен орган следва да се разглеждат като част от законния интерес, преследван от администратора*“. Нещо повече, по българската правна система съобщаването за извършено престъпление е въздигнато в законово задължение, което представлява необходима и пропорционална мярка в едно демократично общество, целяща да гарантира правата и свободите на гражданите. В този случай, операцията по предаването на лични данни за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност, отговаря и на изискванията за последващо обработване на лични данни по смисъла на чл. 6, пар. 4 във връзка със съображение (50) и чл. 23, пар. 1, б. „г“ от ОРЗД.

По отношение на проекта за изменение и допълнение на Наредба № 1 липсват предпоставките за извършването на предварителна консултация по чл. 12, ал. 2 от ЗЗЛД. Независимо от това, задължение за предварителна консултация възниква по смисъла на чл. 36, пар. 4 от ОРЗД и чл. 65, ал. 2 от ЗЗЛД. Доколкото обаче чрез настоящото становище по подадения от адвоката сигнал вече е извършен детайлен правен анализ на проекта за изменение и допълнение на Наредба № 1, КЗЛД счита, че отпада необходимостта администраторите (МВР, МП и МЗ) да пристъпват към процедура по предварителна консултация с КЗЛД.

В заключение следва да се отбележи, че законодателството за защита на личните данни не е пречка за извършването на нормативно регламентираните контролни правомощия по установяване на концентрацията на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози, както и за съответното своевременно ангажиране на административнонаказателната или наказателната отговорност на лицата. Както е прогласено в преамбюла на ОРЗД, обработването на лични данни следва да е предназначено да служи на човечеството. Правото на защита на личните данни не е абсолютно, а трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права и интереси на хората съгласно принципа на пропорционалност.

По тези съображения и на основание чл. 58, пар. 3, б. „б“ от Регламент (ЕС) 2016/679 във вр. с чл. 10а, ал. 1 от Закона за защита на личните данни и чл. 51, т. 2 от Правилника за дейността на КЗЛД и на нейната администрация, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. Писмо с вх. № ППН-02-662/30.10.2023 г., озаглавено като „сигнал“, не съдържа данни за извършено нарушение, нито за реална опасност от извършване на такова, поради което същото е разгледано от КЗЛД в рамките на производството по изразяване на становища.

2. *Проектът на Наредба за изменение и допълнение на Наредба № 1 от 2017 г. за реда за установяване концентрацията на алкохол в кръвта и/или употребата на наркотични вещества или техни аналози*, публикуван на Портала за обществени консултации, съответства на изискванията на Регламент (ЕС) 2016/679 и Закона за защита на личните данни.

ПРЕДСЕДАТЕЛ:
ВЕНЦИСЛАВ КАРАДЖОВ

ЧЛЕНОВЕ:
ЦАНКО ЦОЛОВ
МАРИЯ МАТЕВА
ВЕСЕЛИН ЦЕЛКОВ

По решение на Комисията за защита на личните данни в настоящия бюлетин публикуваме е цялост експозета по теми от областта на защита на личните данни, изготвени през едномесечния стаж в КЗЛД на победителите от миналогодишния конкурс за студенти.

ПРАВОТО ДА БЪДЕШ ЗАБРАВЕН - ОТ 1890 ДО ЕРАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

Пламена Янчева, студент V курс в специалност "Право"
Юридически факултет, Университет за национално и световно стопанство, гр. София

Резюме

През различните етапи от човешката история, в понятието „правото да бъдеш забравен" е влаган различен смисъл, с оглед нуждите на обществото в съответните времена. От зародиш на идеята за регулация на „правото да бъдеш оставен на мира", през очертаване на основата му в Директива 95/46/ЕО, до затвърждаването на позицията му в Регламент (ЕС) 2016/679, правото на изтриване „извървява" дълъг път, изпълнен с много въпроси, някои от които не намират отговор и до днес. Едно от най-големите предизвикателства в ерата на изкуствения интелект се оказва предоставянето на достатъчно висока защита на личните данни, както и гаранции, че следите им ще бъдат заличени с натискането на един бутон.

Ключови думи: *Защита на личните данни; правото да бъдеш забравен; неприкосновеност на личния живот; право на изтриване; изкуствен интелект*

Двадесет и първи век е векът на дигитализацията. Технологиите и изкуственият интелект са все по-необходими в живота на съвременното общество и съпътстват всяка ежедневна дейност – обучения, работа, развлечения, новини, разговори, всичко е в нашите устройства, на един клик разстояние. Необходимостта от употреба на мобилни устройства във все по-широк аспект от действия е причина за предоставяне на по-голям поток от персонална информация от страна на субектите на данни, съответно – за тяхната обработка. В човешката история не е известен период, в който да са се обработвали, съхранявали и разпространявали толкова лични данни, колкото в наши дни. Когато встъпваме в трудови правоотношения, когато създаваме свои профили в дигиталното пространство, когато се съгласяваме с политиките за бисквитки, дори когато отключваме мобилните си устройства с пръстов отпечатък или face ID, предоставяме личните си данни. В кои случаи обаче можем да поискаме да „бъдем забравени" и доколко това право ни гарантира неприкосновеност на личния живот?

Историята на личните данни като понятие и тяхната правна защита датира от края на XIX век. През 1890 адвокатите Самюъл Д. Уорън и Луис Д. Брандис публикуват статия със заглавие „Правото на личен живот"[1] в Harvard Law Review. В нея за пръв път се засяга темата относно правото на всеки да „бъде оставен на мира". Авторите сочат, че тогавашните съвременни достижения на техниката и развитието на търговската дейност, са заплаха за личния и семеен живот. Това твърдение е обусловено от обстоятелството, че по тези времена все по-често се поставя въпросът за намесата в личния живот на гражданите при заснемането им и публикуването във вестници на снимките, без тяхно съгласие.

1 *Warren,S., Brandeis, L., article "The Right to Privacy", Harvard Law Review, December 15, 1890*

Сочи се голямата нужда от механизми за защита на личното пространство, поради грубото нахлуване в личния живот на гражданите от страна на пресата.

Днес, 133 години по-късно, във времена на най-бързо технологично развиващото се общество, „правото да бъдеш забравен“ е все по-дискутирана тема, а необходимостта от правни механизми, които да го гарантират, е все по-належаща.

Първи стъпки в Европейското законодателство, целящи да предоставят обща правна рамка по отношение на защитата на лични данни, са направени през 1995 г. с приемането на Директива 95/46/ЕО[2] (наричана по-нататък Директивата). Предмет на Директивата е защита основните права и свободи на физическите лица и в частност -правото им на личен живот при обработването на лични данни. Един от недостатъците на Директивата обаче е периодът на нейното приемане. Същата е приета преди технологиите и интернет да станат толкова съществена част от живота на обществото, което от своя страна води до много въпроси и неуредени хипотези в годините след приемането ѝ. Една от тези хипотези е и „правото да бъдеш забравен“, което не беше изрично имплементирано в цитирания Европейски акт, но въпреки това не лиши субектите на данни от правомощието да упражнят правото на изтриване на техните лични данни, макар само в определени случаи. Съгласно чл. 6, б. „д“ от Директивата „Държавите-членки предвиждат, че личните данни трябва да се поддържат във форма, която позволява идентифицирането на съответните физически лица за срок не по-дълъг от необходимия за целите, за които тези данни са събрани или обработени допълнително“. Чл. 12, б. „б“ предоставя гаранции относно правото на всеки субект на данни да получи от администратора „Според случая, поправянето, изтриването или блокирането на данните, чиято обработка не е в съответствие с разпоредбите на настоящата директива, и по-конкретно поради непълнота или неточност на самите данни“. Разширителното тълкуване на двата члена отразява основата на „правото да бъдеш забравен“, а именно: изтриване на личните данни, когато е изтекъл предвидения срок за тяхното съхранение или когато обработването им не е в съответствие с Директивата.

Следователно, въпреки че Директивата не урежда изрично правото на изтриване, все пак очертава неговите основи.

Ключов момент в историята на правото на изтриване е Решение на Съда на Европейския съюз (наричан по-долу СЕС) през 2014 г. по дело С-131/12[3] (наричано по-нататък Решението), постановено при действието на Директивата. Същото се отнася до преюдициално запитване относно тълкуването на чл. 2, б. „б“ и „г“, чл. 4, пар. 1, б. „а“ и „в“, чл. 12, б. „б“ и чл. 14, пар. 1, б. „а“ от Директивата.

Запитването е отправено в рамките на спор между Google Spain SL и Google INC, от една страна, и Agencia Española de Protección de Datos (Агенция за защита на данните, наричана по-нататък „AEPD“) и г-н Costeja González, от друга. Повод за образуване на делото е отправено искане на испанския гражданин, г-н Costeja González, за изтриване на статии от испанския вестник La Vanguardia Ediciones SL, свързани с принудителна продажба на негово недвижимо имущество от 19 януари и 9 март 1998 г., както и заличаване от страна на Google Inc. и Google Spain на резултати, свързани с публикацията, които се появяват при търсене на името му. След отказ публикацията от вестника и информацията от интернет търсачката на Google да бъдат премахнати, г-н Costeja González подава жалба до AEPD. Доводите на г-н Costeja González се основават на обстоятелството, че още преди години е изпълнил изцяло задълженията си, поради което посочването на името му в статиите, се явявало ирелевантно. С решение от 30 юли 2010 г. AEPD отхвърля жалбата в частта ѝ, отнасяща се до La Vanguardia, и я уважава в частта ѝ срещу Google Spain и Google Inc. От своя страна Google Spain и Google Inc. подават пред AEPD отделни жалби срещу посоченото решение и същата юрисдикция съединява образуваните по жалбите дела. Органът спира производството по делото, тъй като счита,

2 Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни

3 Решение на Съда на Европейския съюз С-131/12 (Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González)

че е необходимо да отправи преюдициално запитване до СЕС, отнасящо се до въпросите „Какви задължения носят лицата, които управляват интернет търсачки, във връзка със защитата на личните данни на заинтересованите лица, които не желаят определена информация, която е публикувана в уебсайтове на трети лица и съдържа техни лични данни, позволяващи информацията да се свърже с тези лица, да бъде качена, индексирана и предоставена свободно на разположение на потребителите на интернет?“.

СЕС постановява, че Google е администратор на лични данни по смисъла на чл. 2, б. „а“ от Директивата и операциите, които извършва трябва да се квалифицират като „обработване“ по смисъла на б. „б“ от тази разпоредба. СЕС признава, че обработката на данни е извършена извън територията на ЕС, тъй като компанията Google Search се управлява от Google Inc., което е дружеството майка в групата Google и седалището му е в САЩ. Въпреки това обаче СЕС разширява териториалния обхват на приложното поле на Директивата, като заключва, че Google Spain и Google Inc. са тясно свързани, поради което Google Inc. е правно обвързано от Директивата.

Най-важното заключение, което СЕС прави в контекста на правото на изтриване е, че дори когато лични данни се обработват законосъобразно, е възможно след време обработването да стане несъвместимо с Директивата, когато данните вече не са необходими за целите, за които са събирани и обработвани (напр. когато данните вече са ирелевантни или прекомерни за целите на обработването, когато не са актуализирани или не са адекватни и т.н.). В такива хипотези информацията и съответните връзки, посочени в списъка на резултатите, трябва да бъдат изтрити. Следва обаче да се прави преценка във всеки отделен случай дали съответното лице има право отнасящата се до него информация да не се свързва повече с името му към настоящия момент. От това право не би могло да се възползва лице, което е в обществения живот. Според СЕС вмешателството в неговите основни права е обосновано поради приоритетния интерес на обществото да има достъп до въпросната информация.

В резултат от това решение всеки субект на данни може да поиска заличаване на връзките към интернет страници, съдържащи информация, която нарушава неговите права, от интернет търсачките, опериращи на територите на държавите-членки на ЕС, дори в случаите, в които обработването на данни е било законосъобразно. В тази връзка е създадена и платформа за упражняване на това право с интернет страницата на Google[4], както и Отчет за прозрачност на Google[5]. Следва да се уточни, че исканията за заличаване не водят до пълното изтриване на личните данни. При подаване на такова искане до интернет търсачка, личните данни няма да бъдат изтрити нито от уебсайта източник, нито от индекса и кеш паметта на доставчика на търсачки. Субектът на данни може да иска например заличаването на лични данни от индекса на търсачката, които произхождат от медийно издание (напр. статия от вестник). В този случай връзката към личните данни може да бъде заличена от индекса на търсачката; въпреки това въпросната статия ще остане под контрола на медийното издание и може да остане обществено достъпна, дори ако вече не се вижда в резултатите от търсенето въз основа на заявки, които по принцип включват името на субекта на данни[6].

Едно от най-големите достижения на Правото на Европейския съюз бе приемането на Регламент (ЕС) 2016/679[7] (т.нар. Общ регламент относно защитата на данните), наричан по-нататък Регламентът, който влезе в сила през 2018 г. Предназначен да замести Директива 95/46/ЕО и да актуализира правилата относно неприкосновеността на личния живот и защитата на данните в ерата на дигитализацията, Регламентът даде повече яснота по отношение на правото на изтриване, като

4 Линк към платформата: https://reportcontent.google.com/forms/eu_removal?hl=en

5 Линк към отчета: https://transparencyreport.google.com/eu privacy/overview?hl=en&requests_over_time=country:BG&lu=requests_over_time

6 Насоки 5/2019 относно критериите за прилагането на „правото да бъдеш забравен“ при възникване на дела, свързани с предоставяне на услуги за търсене на информация, съгласно ОРЗД (част 1), версия 2.0, приет на 7 юли 2020 г.

7 Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година 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 (Общ регламент относно защитата на данните)

го уреди изрично в чл. 17. Всъщност, „правото да бъдеш забравен“ е имплементирано в GDPR във връзка с постановяването на Решението по дело C-131/12. Посочената разпоредба запазва замисъла на „Правото да бъдещ забравен“, инкорпориран в Директивата, като го разширява, давайки на субектите на данни по-голям контрол върху достъпа до техните лични данни и свободата на избор дали техните данни да продължат да се обработват.

Чл. 17 гарантира правото на всеки субект на данни да поиска от администратора да изтрие свързаните с него лични данни, без ненужно, в следните хипотези:

- Отпадане на необходимостта от обработването им;
- При оттегляне на съгласието на субекта на данни, но само ако няма друго правно основание за обработването;
- При възразяване срещу обработването;
- При констатация относно незаконосъобразност при обработване на личните данни;
- При необходимост от спазване на правно задължение, съгласно Европейското или националното законодателство, което се прилага спрямо администратора;
- В някои хипотези на обработване на лични данни на деца.

От друга страна разпоредбата гарантира правото на администратора да откаже изтриването на данни, при наличието на определени обстоятелства, а именно:

- При упражняване на правото на свобода на изразяване и право на информация;
- За спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;
- В определени хипотези, свързани с причини от обществен интерес в областта на общественото здраве;
- За целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;
- За установяването, упражняването или защитата на правни претенции.

Регламентът предвижда и задължение за администратора, от когото се иска изтриване на данните и който е направил личните данни публични, да уведоми другите администратори, които обработват личните данни на съответния субект, да изтрият всички връзки, копия или реплики на тези данни. Следва да се подчертае, че това задължение е само за уведомяване, а не за постигане на реален резултат.

Важна стъпка в развитието на правото на изтриване е постановяването на решение на Съда на Европейския съюз по дело C-460/20[8]. В основата на казуса е искането на двама инвестиционни мениджъри към Google да отмени резултатите от търсене, направено въз основа на техните имена, което предоставя връзки към статии, критикуващи инвестиционния им модел. Според ищците статиите съдържат неточни твърдения. От своя страна ръководството на Google отказва да се съобрази с горепосочените аргументи, тъй като не са били налице доказателства относно това дали статиите съдържат неточни твърдения.

С цитираното решение Съдът на ЕС постановява, че лицата, които искат да бъдат изчистени неточни резултати от търсачките, следва да докажат очевидната неистинност на съответната информация или на поне част от нея, при положение че тя не е от маловажно значение. В случай на такова доказване, управляващият интернет търсачката е длъжен да уважи искането и да премахне

8 *Решение на Съда на Европейския съюз C-460/20 (TU/Google LLC)*

резултатите. Съдът приема, че управляващият интернет търсачката трябва да има предвид всички обстоятелства по конкретния случай, за да реши дали дадено съдържание може да продължи да бъде включвано в списъка с резултатите от търсенето. В решението е подчертано, че правото на свобода на изразяване и на информация не може да се взема предвид тогава, когато дори част от информацията, включена в съдържанието, към което се препраща, се окаже неистина, при положение че тя не е от маловажно значение.

На национално равнище Комисията за защита на личните данни (наричана по-долу КЗЛД) също е имала възможност да се произнесе по тема, свързана с правото на изтриване. Със становище от 04.02.2019 г.[9] КЗЛД отговори на някои неясноти, свързани с „правото да бъдеш забравен“, в контекста на обработване на лични данни за журналистически цели. Комисията е била сезирана от различни медии с информация, че при тях са постъпили искания за упражняване на правото на изтриване от лице, за което са били публикувани статии и снимки, касаещи осъждането му с влязла в сила присъда за извършено престъпление. Поставен е въпрос, свързан с основателността на отправените искания за упражняване на правото „да бъдеш забравен. Надзорният орган приема, че правото на изтриване не е абсолютно право и упражняването му може да бъде дерогирано на някое от изрично посочените в Регламент (ЕС) 2016/679 основания. Според КЗЛД при обработване на лични данни за журналистически цели, информацията трябва да касае въпроси, отнасящи се до обществено значими ценности. Предвид обстоятелството, че една от основните функции на наказателната репресия е постигането на генерална превенция (т.е. въздействието върху обществото с цел въздържане от извършване на престъпления), в конкретния случай е налице основание за отказ на предявеното право на изтриване на лични данни. Обработването им е необходимо за упражняване на правото на свобода на изразяване, правото на информация и за изпълнението на задача от обществен интерес, а именно информиране на обществото, както за извършените престъпления, така и за личността на извършителя, предвид неговата завишена обществена опасност. По аргумент на противното, правото на изтриване би било безспорно приложимо при заявление за изтриване на медийни публикации за наказателно преследване на лице, което впоследствие е напълно оправдано[10], освен ако случаят се отнася до лице от обществения живот.

Динамичното развитие на технологиите и все по-широкото използване на различни алгоритми за изкуствен интелект, поставят редица въпроси, свързани с упражняването на „правото да бъдеш забравен“. В своята книга „Принципи“[11] авторът Рей Далио пише: „В бъдеще изкуственият интелект ще оказва огромно влияние върху вземането на решения във всяка една област на живота… Сега, независимо дали ви харесва или не, всеки има достъп до цифровите ви данни и може да научи много неща за вас, а тези данни могат да бъдат въведени в компютри, които да ги използват за всичко – от това да предскажат каква покупка вероятно ще направите, до вашите житейски ценности...“. Възниква въпросът как и можем ли да упражним в пълен обем правото си на изтриване, в случай че наши данни са попаднали „в ръцете на“ изкуствен интелект?

Изкуственият интелект е огромно предизвикателство пред съвременното законодателство, отнасящо се до защитата на личните данни. Някои автори дори твърдят, че възможността за приложимост на правото на изтриване в контекста на изкуствения интелект, граничи с невъзможното[12]. Спецификите се състоят в обстоятелството, че алгоритмите обработват данни и управляват информация по различен начин от мозъка при хората. Например изкуственият интелект е способен да работи с думи, без да разбира тяхното значение, да коригира граматични, пунктуационни и други грешки, без да разбира езиковите правила, да превежда текстове на различни езици, без да знае съответния език

9 *Становище на Комисията за защита на личните данни, рег. № НДМСПО-01-78/04.02.2019 г., гр. София*

10 *Джутев, Д., Спартанска, Ц., статия „GDPR и правото „да бъдеш забравен“, Акаунтинг нюз, 18.06.2019 г.*

11 *Далио, Р. „Принципи“, издателство „Изток-Запад“, 2018, стр. 254*

12 *Li, T., Villaronga, E., Kieseberg, P., article “Humans Forget, Machines Remember: Artificial intelligence and the Right to Be Forgotten”, Boston University School of Law, 2018*

и т.н. Това е така, тъй като обработката на данни е поверена на алгоритми, които не могат да мислят абстрактно и не е необходимо да „разбират“ информацията, с която работят, за да я класифицират и свържат по значим за потребителите начин. Ето защо, предвид обстоятелството, че алгоритмите просто изчисляват, те не могат нито да „помнят правилно“, нито да „забравят правилно“. Например конкретен уебсайт се счита за „подходящ“ от алгоритъма, ако твърде много потребители са го посетили, както и обратното – алгоритъмът „забравя“ това, което е забравено от потребителите[13]. Всеки запис на данни, попаднал в база данни на изкуствен интелект, може да се съхранява на различни места във вътрешни механизми, в архиви и т.н. Когато алгоритъмът умножава данни, той „не обръща внимание“ на този процес и „не го помни“ и „разбира“. Следователно това се оказва съществена пречка пред упражняване на правото на изтриване. В този смисъл, както потребителите, така и регулаторите следва да имат предвид, че „правото да бъдеш забравен“ се упражнява в различен обем, когато става въпрос за огромни бази данни, обработвани от изкуствен интелект, в сравнение с бази данни, съхранявани във файлова система.

С оглед нуждата от Европейска правна рамка в контекста на защитата на лични данни в среда с изкуствен интелект, след близо две години обсъждания, на 8 декември 2023 г. бе постигнато съгласие за Законодателен акт за изкуствения интелект (ИИ) в ЕС. С приемането на акта се цели установяване на ясни задължения при употребата на изкуствен интелект (напр. задължения за прозрачност, за установяване на гаранции спазване на законодателството за авторското право на ЕС и GDPR); насърчаване на инвестициите и иновациите в сектора; установяване на ред, по който да бъдат подавани жалби относно системи, използващи изкуствен интелект; установяване на санкции при неспазване на задълженията и т.н. Очаква се новият законодателен акт да влезе в сила в началото на следващата година, след като Европейският парламент и Съвета на министрите официално го ратифицират, а правилата ще започнат да се прилагат две години по-късно.

Осигуряването на висока степен на защита на личните данни е огромно предизвикателство пред съвременното законодателство, с оглед бързото развитие на информационните технологии и големият поток от информация, която се дигитализира. Днес, повече от всякога, човечеството се нуждае от гаранции, осигуряващи правото на неприкосновеност на личния живот. Една от тези гаранции е именно „правото да бъдеш забравен“. В ерата на изкуствения интелект това право обаче не винаги може да бъде упражнено в пълен обем. Остава открит въпросът дали законодателството и изкуствения интелект ще „намерят общ език“, за да предоставят пълни гаранции относно защитата на данните в електронна среда.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ:

1. Warren,S., Brandeis, L., article “The Right to Privacy”, Harvard Law Review, December 15, 1880- https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

2. Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни - https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=celex%3A31995L0046

3. Решение на Съда на Европейския съюз C-131/12 (Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González) - https://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d55d64d9a37b5a477eac11d72c1de1eb84.e34KaxiLc3qMb40Rch0SaxuNb3z0?text=&docid=152065&pageIndex=0&doclang=BG&mode=req&dir=&occ=first&part=1&cid=265967

4. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година 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 (Общ регламент относно защитата на данните) - https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679

13 Esposito, E., article “Algorithmic memory and the right to be forgotten on the web”, 17.04.2017

5. Насоки 5/2019 относно критериите за прилагането на „правото да бъдеш забравен“ при възникване на дела, свързани с предоставяне на услуги за търсене на информация, съгласно ОРЗД (част 1), версия 2.0, приет на 7 юли 2020 г. - https://www.cpdp.bg/userfiles/file/EDPB/EDPB_Guidelines_201905_rtbfsearchengines_Bg.pdf

6. Решение на Съда на Европейския съюз C-460/20 (TU/Google LLC) - https://curia.europa.eu/juris/document/document.jsf?text=&docid=268429&pageIndex=0&doclang=BG&mode=req&dir=&occ=first&part=1&cid=12735

7. Становище на Комисията за защита на личните данни рег. № НДМСПО-01-78/04.02.2019 г. гр. София - https://www.cpdp.bg/?p=element_view&aid=2183

8. Джутев, Д., Спартанска, Ц., статия „GDPR и правото „да бъдеш забравен“, Акаунтинг нюз, 18.06.2019 г. - https://accountingnews.bg/gdpr-%D0%B8-%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D1%82%D0%BE-%D0%B4%D0%B0 %D0%B1%D1%8A%D0%B4%D0%B5%D1%88 %D0%B7%D0%B0%D0%B1%D1%80%D0%B0%D0%B2%D0%B5%D0%BD-569.html

9. Далио, Р. „Принципи“, издателство „Изток-Запад“, 2018, стр. 254

10. Li, T., Villaronga, E., Kieseberg, P., article “Humans Forget, Machines Remember: Artificial intelligence and the Right to Be Forgotten”, Boston University School of Law, 2018 - https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1816&context=faculty_scholarship

11. Esposito, E., article “Algorithmic memory and the right to be forgotten on the web”, 17.04.2017- https://journals.sagepub.com/doi/10.1177/2053951717703996.

ПРЕДАВАНЕ НА ДАННИ КЪМ ТРЕТИ ДЪРЖАВИ

Бориславa Савова, студент IV курс в специалност „Публична администрация“
Философски факултет, Софийски университет „Св. Климент Охридски“

Резюме

През практически пример се разглеждат разпоредбите на Общия регламент относно защитата на данните и практиката на Европейския комитет по защита на данните относно предаването на данни към трети държави. Текстът завършва с „Основните практически стъпки при предаване на лични данни към трети държави, които износителят на данни трябва да следва.

Ключови думи: *Защита на личните данни; предаване на данни към трети държави; неприкосновеност на личния живот; принцип на отчетност; трети държави;*

Въведение

Предаването на данни към трети държави извън границите на Европейския съюз (ЕС) и Европейското икономическо пространство (ЕИП) е урегулирано в рамките на 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 (Общ регламент относно защитата на данните, ОРЗД) и в Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления

или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета. Конкретно изследване е ориетирано към предаването на данни на данни към трети държави по смисъла на глава V от ОРЗД. Основното право на защита на личните данни е залегнало в член 8 от Хартата на основните права на Европейския съюз и в член 16 от Договора за функционирането на Европейския съюз.

ОРЗД „е важна стъпка за укрепване на основните права на физическите лица в цифровата ера и за улесняване на извършването на стопанска дейност чрез изясняване на правилата за предприятията и публичните органи на цифровия единен пазар. Изготвянето на един-единствен законодателен акт също така слага край на разпокъсаността в различните национални системи и на ненужната административна тежест“[1].

С Директива (ЕС) 2016/680 се „защитава основното право на гражданите на защита на данните, когато лични данни се използват от органите за наказателно правоприлагане за целите на правоприлагането. По-специално с нея се гарантира, че личните данни на жертвите, свидетелите и заподозрените в престъпления лица се защитават надлежно, като същевременно ще се улеснява трансграничното сътрудничество в борбата с престъпността и тероризма“[2].

Настоящият реферат разглежда дейността по обработването на данни в средно предприятие и по – конкретно какъв е процесът на законосъобразно изнасяне на данни извън рамките на ЕС и ЕИП от предприятието. Този процес е проследен чрез ОРЗД, тъй като се отнася за международни търговски отношения.

Казус:

Средно предприятие с име „А“, със средносписъчен брой на персонала по – малък от 250 души и годишен оборот, който не превишава 97 500 000 лв., и/или стойност на активите, която не превишава 84 000 000 лв.[3]

Приема се, че предприятието, за да осъществи своята дейност, предава лични данни към трети държави и представлява мултинационална компания. Предметът на дейност на дружеството е онлайн търговия. Сред основните стъпки при предаването на данни към трети държави е да бъдат ясно уточнени ролите на участниците в обработването.

Понятието „администратор“

Понятието „администратор“ е определено в член 4, параграф 7 от ОРЗД като: „физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка“(Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД).

Частта от определението, която гласи, че администратор е „физическо или юридическо лице, публичен орган, агенция или друга структура“ се свързва с вида на правния субект, който може да бъде администратор. „Това означава, че по принцип няма ограничение по отношение на вида на правния субект, който може да поеме ролята на администратор. То може да бъде организация, но може да бъде и физическо лице или група физически лица. На практика обаче обикновено самата организация, а не дадено физическо лице в рамките на организацията (като главен изпълнителен директор, служител или член на управителния съвет), действа като администратор по смисъла на ОРЗД. Що се отнася до

1 *https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_bg*

2 *https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_bg*

3 *Как се определя дали едно предприятие е микро, малко и средно? https://evroprogrami.com/polezno/chesto-zadavani-vaprosi/kak-se-opredelya-dali-edno-predpriyatie-e-mikro-malko-i-sredno/*

обработването на данни в рамките на група от дружества, трябва да се обърне специално внимание на въпроса дали дадено предприятие може да действа като администратор или обработващ лични данни, например, когато се обработват данни от името на дружеството майка“. (Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД). В случая не е налице група от дружества, а едно дружество, което за целите на настоящият казус е администратор и обработва лични данни по смисъла на ОРЗД.

Следователно целите и средствата, определени от администратора, трябва да са свързани с „обработването на лични данни“. Според член 4, параграф 2 от ОРЗД обработването на лични данни „означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни“. В резултат на това понятието „администратор“ може да бъде свързано или с една операция по обработване или със съвкупност от операции. На практика, това може да означава, че администрирането, извършвано от конкретен правен субект, може да обхваща въпросното обработване в неговата цялост, но може да се ограничава и до определен етап на обработването.

Пример: Пазарно проучаване

Дружество А желае да проведе проучване с цел да разбере кои видове потребители е най-вероятно да се интересуват от неговите продукти. Изпълнението на задачата е възложено на доставчик на услуги XYZ, чрез сключване на договор.

Дружество А дава указания на XYZ относно вида информация, от която се интересува, и предоставя списък с въпроси, които да бъдат зададени на участниците в пазарното проучване.

Дружество А получава само статистическа информация (напр. идентифициране на потребителските тенденции по региони) от XYZ и няма достъп до самите лични данни. Въпреки това, решението обработването да се извърши е взето от дружество А, обработването се извършва за целите и дейността му и дружество А е предоставило на XYZ подробни указания относно това каква информация да събира. Следователно дружество А все пак трябва да се счита за администратор по отношение на обработването на лични данни, което се извършва с цел предоставяне на поисканата от него информация. Докато съгласно условията на сключеният договор XYZ следва да обработва данните единствено за целите, определени от дружество А и съгласно неговите подробни указания, и следователно трябва да се счита за обработващ лични данни (Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД).

От примера следва, че дружеството А може да отдаде права за обработване на данни към друго дружество, без възможността това дружество да определя самостоятелно целите и средствата, като го прави обработващ лични данни. Обработващият лични данни не трябва да обработва данните по никакъв друг начин, освен съгласно указанията на администратора. Тези указания все пак могат да предоставят известна свобода на преценка по отношение на това кой е най-добрият начин за обслужване на интересите на администратора. Обработващият обаче нарушава ОРЗД, в случай че излезе извън рамките на указанията на администратора и започне да определя свои собствени цели и средства за обработването. В такъв случай обработващият лични данни ще се счита за администратор по отношение на това обработване и може да подлежи на санкции[4].

Всяко обработване на лични данни от страна на обработващ лични данни трябва да се урежда с договор или с друг правен акт, който е в писмена форма, включително електронна, и е обвързващ. Администраторът и обработващият лични данни могат да изберат да сключат свой собствен договор, съдържащ всички задължителни елементи, или да разчитат изцяло или частично на стандартни договорни клаузи. В договора следва да се определят изискванията по отношение на предаването на данни към трети държави или международни организации, като се вземат предвид разпоредбите на глава V от ОРЗД[5].

4 Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД

5 Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД

Чии лични данни обработва предприятието?

Предприятието обработва личните данни на служителите си, на клиентите, на доставчици и на транспортни фирми.

Какво представлява понятието „трета държава”?

„Трета държава” е всяка държава извън Европейския съюз или Европейското икономическо пространство.

За предаването на данни към трети държави се прилага принципът на отчетност, който е необходим, за да се гарантира ефективното прилагане на нивото на защита, предвидено в ОРЗД. „Отчетност на практика означава способността на администратора на лични данни във всеки един момент да докаже, че обработва личните данни законосъобразно, добросъвестно, прозрачно и в минимален обем за постигане на ясно определени цели, като данните се съхраняват точни и само за времето, необходимо за постигане на тези цели, а посоченото обработване е обезпечено с подходящо ниво на сигурност и защита на данните“ (# 8 Отчетността като нов принцип на GDPR, 2018 г.).

Принципът на отчетност

„Отчетността предполага надлежно документиране на всички процеси по обработване на лични данни в предприятието. Иначе казано, предприятията трябва да създадат „документална следа“ относно обработването – да разполагат с писмен документ, който позволява проследимост на процесите по обработване на данните и който може да се ползва като доказателство при проверка от КЗЛД относно спазването на изискванията на ОРЗД“ (# 8 Отчетността като нов принцип на GDPR, 2018 г.).

Кои са институциите, които могат да вземат пряко участие в предаването на данни и да влияят на процеса:

- ЕКЗД – независим европейски надзорен орган, който гарантира, че Общият регламент относно защитата на данните (ОРЗД) и Директивата относно правоприлагането в областта на защитата на данните се прилагат последователно в държавите от ЕС, както и в Норвегия, Лихтенщайн и Исландия; също так съветва Европейската комисия по въпроси в областта на защитата на данните и по всяко предложение за ново законодателство на ЕС от особено значение за защитата на личните данни.

- Европейската комисия – извършва преценка дали държава извън ЕС и ЕИП предлага адекватно ниво на защита на личните данни съгласно член 45 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данниет, ОРЗД); също така приема решения за адекватно ниво на защита на данните.

- Европейският парламент и Съвета на ЕС по всяко време могат да поискат от ЕК да поддържа, измени или оттегли решението за адекватност на основание надвишаване на компетенциите, които са заложени в регламента.

- Националните надзорни органи за защита на данните в ЕС/ЕИП.

Как и в кои законодателни актове е урегулирано предаването на данни към трети държави?

Предаването на данни към трети държави е урегулирано в конкретна законодателна и институционална рамка. Основният закон, които регулира тази дейност е Общият регламент относно защитата на данните и по – конкретно глава V на същия.

Приемаме, че предприятието А, което е предмет на настоящя казус, предава данни извън границите на България и извън границите на ЕС и ЕИП. Според глава V от ОРЗД това може да се случи при спазване на следните правила:

• въз основа на решение за адекватно ниво на защита от Европейската комисия съгласно ОРЗД;

• ако са осигурени „подходящи гаранции", чрез други инструменти за предаване на лични данни към трети държави (Задължителни фирмени правила, Стандартни договорни клаузи, Кодекси на поведение, Механизми за сертифициране, печати или маркировки за защита на данните – като последните три възможности са въведени с ОРЗД);

• при липса на някое от горните, чрез „дерогации в особени случаи", когато предаването се осъществява по изключение.[6]

В първото, от отбелязаните по-горе правила, се споменава включването на Европейската комисия като участник в процеса за предаване на данни. Тя приема решения относно адекватното ниво на защита на данните, тези правомощия произтичат от член 45 от ОРЗД. Процедурата за приемане на такова решение на ниво ЕС минава през следните фази:

- изготвяне на предложение от Европейската комисия;

- получаване на становище от Европейския комитет по защита на данните;

- одобрение от представителите на страните членки на ЕС;

- приемане на решението от Европейската комисия.[7]

Какво, според ОРЗД, представлява нивото на адекватност и кои елементи включва това понятие ?

„При оценяване на адекватността на нивото на защита на данните ЕК отчита по-специално следните елементи:

а) върховенството на закона, спазването на правата на човека и основните свободи, съответното законодателство — както общо, така и секторно, включително в областта на обществената сигурност, отбраната, националната сигурност и наказателното право и достъпа на публичните органи до лични данни, а също и прилагането на такова законодателство, правилата за защита на данните....;

б) наличието и ефективното функциониране на един или повече независими надзорни органи във въпросната трета държава или на които се подчинява дадена международна организация...;

в) международните ангажименти, които съответната трета държава или международна организация е поела, или други задължения, произтичащи от правно обвързващи конвенции или инструменти, както и от участието ѝ в многостранни или регионални системи, по-конкретно по отношение на защитата на личните данни." (член 45, глава V от ОРЗД);

Решенията, приети от ЕК остават в сила, докато не бъдат изменени, заменени или отменени с нейно решение, прието в съответствие с параграфи 3 или 5 от член 45 от ОРЗД). В акта за изпълнение се предвижда механизъм за периодичен преглед най-малко веднъж на четири години, при който се отчитат всички имащи отношение промени в третата държава или международната организация.

По отношение на второто правило при липса на решение съгласно член 45, параграф 3, администраторът или обработващият лични данни може да предава лични данни към трета държава или международна организация само ако е предвидил подходящи гаранции и при условие че са налице приложими права на субектите на данни и ефективни правни средства за защита. (член 46, глава 5 от ОРЗД). Това правило може да бъде илюстрирано с делото Schrems II. На 16.06.2020г. Съдът на Европейския Съюз (СЕС) постановява решение по делото C-311/18 – Facebook Ireland и Schrems, известно повече като Schrems II, с което обявява за недействително Решение 2016/1250 на Комисията съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между Европейския съюз и Съединените американски щати.

---

6 https://www.cpdp.bg/?p=sub_rubric&aid=271

7 https://www.cpdp.bg/?p=element&aid=438

Със същото решение Съдът разгледжа валидността на Решение 2010/87/ЕО на Комисията относно стандартните договорни клаузи като обявява същото за валидно. Съдът постановява, че валидността зависи от това дали Решение 2010/87/ЕО включва ефективни механизми, които позволяват да се гарантира на практика спазването на съпоставимо ниво на защита, на това което се гарантира в рамките на ЕС от Регламент (ЕС) 2016/679, и че предаването на лични данни в съответствие с такива клаузи се спира или забранява в случай на нарушение на клаузите или при невъзможност за спазването им.

Решенията относно адекватното ниво на защита не възпрепятстват субектите на данни да подадат жалба. Те не възпрепятстват и надзорните органи да сезират национален съд, ако се съмняват във валидността на дадено решение, така че националният съд може да отправи преюдициално запитване до Съда на ЕС, за да провери тази валидност (Препоръки 01/2020 относно мерките, които допълват инструментите за предаване, за да се гарантира спазването на нивото на защита на личните данни, заложено в ЕС).

Подходящите гаранции могат да се приложат без да се изисква специално разрешение от надзорния орган, посредством:

а) инструмент със задължителен характер и с изпълнителна сила между публичните органи или структури;

б) задължителни фирмени правила в съответствие с член 47 от ОРЗД;

Задължителните фирмени правила (ЗФП) са въведени като инструмент за трансфери на данни в член 47 от Общия регламент относно защитата на данни. Те представляват политики, базирани на европейските стандарти за защита на данните, които се изготвят от мултинационални компании с цел осигуряване на адекватни ниво на защита на предаваните данни между юридическите лица в рамките на корпорацията. Те трябва да включват всички основни принципи за защита на данните и приложими права, както и да бъдат възприето от всички отделни юридически лица, за да бъдат правно обвързващи (Препоръки 1/2022 относно заявлението за одобрение и елементите и принципите, които могат да бъдат намерени в задължителните фирмени правила на администратор на лични данни (чл. 47 от ОРЗД)).

в) стандартни клаузи за защита на данните, приети от Комисията в съответствие с процедурата по разглеждане, посочена в член 93, параграф 2 от ОРЗД;

Договорните клаузи, осигуряващи подходящи гаранции за защита на данните, могат да се използват като основание за прехвърляне на данни от ЕС към трети страни съгласно ОРЗД. Те включват типови договорни клаузи, така наречените стандартни договорни клаузи, които са „предварително одобрени“ от Европейската комисия. (Съвместно становище 2/2021 на Европейския комитет по защита на данните и Европейския надзорен орган по защита на данните във връзка с Решението за изпълнение на Европейската комисия относно стандартните договорни клаузи за трансфера на лични данни към трети държави).

г) стандартни клаузи за защита на данните, приети от надзорен орган и одобрени от Комисията съгласно процедурата по разглеждане, посочена в член 93, параграф 2 от ОРЗД;

д) одобрен кодекс за поведение съгласно член 40, заедно със задължителни ангажименти с изпълнителна сила на администратора или обработващия лични данни в третата държава да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни;

Кодексите за поведение по смисъла на ОРЗД представляват доброволен инструмент, който може да се използва като доказателство за прилагането на подходящи мерки за доказване на съответствието с Регламент (ЕС) 2016/679, както и като основание за трансфер на данни. При използване на кодекси за поведение, следва да бъде извършен анализ от износителя на данни върху нивото на защита, което се предоставя (Насоки 4/2021 относно кодексите за поведение като средство за предаване на данни).

е) одобрен механизъм за сертифициране съгласно член 42, заедно със задължителни и изпълними ангажименти на администратора или обработващия лични данни в третата държава да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни. (член 46, глава 5 от ОРЗД)

„Механизми за сертифициране, печати или маркировки за защита на данните, които представляват доброволен инструмент за доказване прилагането на подходящи гаранции за защита на данни, в съответствие с ОРЗД. Те позволят на субектите на данни бързо да оценят нивото на защита на данните на съответни продукти и услуги.“ (Информационна брошура на КЗЛД „Предаване на лични данни извън Европейския съюз” 2022 г.)

Пример за съществуващи сертификати за предаване на данни са „Подходът за научни изследвания, базирани на общностно участие“ (CBPR) на Азиатско-тихоокеанско икономическо сътрудничество (АТИС). Действителната връзка на нормативните критерии и механизмите за защита на данните в тях не отговаря напълно на условията на механизмите за сертифициране на защита на данните, предвидени в чл. 42 и 43 от ОРЗД (Насоки 7/2022 относно сертифицирането като инструмент за предаване на данни)

При условие че компетентният надзорен орган е дал разрешение, подходящите гаранции, посочени в параграф 1, могат да бъдат предвидени по-специално и посредством:

а) договорни клаузи между администратора или обработващия лични данни и администратора, обработващия лични данни или получателя на личните данни в третата държава или международната организация; или

б) разпоредби, които да се включват в административните договорености между публичните органи или структури, съдържащи действителни и приложими права на субектите на данни.

Надзорният орган прилага механизма за съгласуваност по член 63 в случаите, посочени в параграф 3 от член 46, от ОРЗД.

Кога се прилагат дерогации в особени случаи?

Едно от основните условия за използване на няколко дерогации е предаването на данни да бъде „необходимо“ за определена цел. Критерият за необходимост следва да се прилага, за да се оцени възможното използване на дерогациите по член 49, параграф 1, букви б), в), г), д) и е). Този критерий налага износителят на данни в ЕС да направи оценка на това, дали предаването на лични данни може да се счита за необходимо за конкретната цел на дерогацията, която ще се използва (Насоки № 2/2018 относно дерогациите по член 49 от Регламент 2016/679).

Според ОРЗД:

При липса на решение относно адекватното ниво на защита съгласно член 45, параграф 3 или на подходящи гаранции съгласно член 46, включително задължителни фирмени правила, предаване или съвкупност от предавания на лични данни към трета държава или международна организация се извършва само при едно от следните условия:

а) субектът на данните изрично е дал съгласието си за предлаганото предаване на данни, след като е бил информиран за свързаните с предаването възможни рискове за субекта на данните поради липсата на решение относно адекватното ниво на защита и на подходящи гаранции;

б) предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;

в) предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;

г) предаването е необходимо поради важни причини от обществен интерес;

д) предаването е необходимо за установяването, упражняването или защитата на правни претенции;

е) предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

ж) предаването се извършва от регистър, който съгласно правото на Съюза или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай (член 46, глава 5 от ОРЗД).

Когато предаването не може да се основава на разпоредба на членове 45 или 46, включително разпоредби относно задължителни фирмени правила, и не е приложима нито една от дерогациите в особени случаи. Предаването на данни на трета държава или международна организация може да се извършва само ако предаването не е повторяемо, засяга само ограничен брой субекти на данни, необходимо е за целите на неоспоримите законни интереси, преследвани от администратора, над които не стоят интересите или правата и свободите на субекта на данни и администраторът е оценил всички обстоятелства, свързани с предаването на данните, и въз основа на тази оценка е предоставил подходящи гаранции във връзка със защитата на личните данни. Администраторът уведомява надзорния орган за предаването на данни. В допълнение към предоставянето на информацията, посочена в членове 13 и 14, администраторът информира субекта на данни за предаването, както и за преследваните неоспорими законни интереси.

Извод:

„Основните практически стъпки при предаване на лични данни към трети държави, които износителят на данни трябва да следва са:

1. Стъпка: Да е наясно къде ще предава личните данни, за да може да може да гарантира равностойно ниво на защита.

2. Стъпка: Да провери дали държавата има решение за адекватно ниво на защита, прието от Европейската комисия.

3. Стъпка: Да провери кой инструмент за предаване на лични данни, изброени в глава V от ОРЗД е най-подходящ в конкретния случай.

4. Стъпка: Да прецени дали законодателството или практиката на третата държава биха засегнали приложените от него инструментите за предаване, във връзка с конкретното предаване.

5. Стъпка: Да определи и приеме допълнителни мерки, за да приведе нивото на защита на данните в съответствие ОРЗД, т.е. със стандарта на ЕС за равнопоставеност.

6. Стъпка: Да предприеме формални процедурни стъпки, след като е набелязал ефективните допълващи мерки. Това са мерки допълващи инструментите за предаване на лични данни към трети страни съгласно член 46 от ОРЗД.

7. Стъпка: Да извършва периодично оценка на нивото на защита и да следи за промени, които могат да имат отношение на предаването на данни в определена трета държава“. (Информационна брошура на КЗЛД „Предаване на лични данни извън Европейския съюз” 2022 г.).

Източници:

Защита на данните в ЕС https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_bg

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА Първи доклад относно прилагането и функционирането на Директива (ЕС) 2016/680 относно правоприлагането в областта на защитата на данните („ДПЗД“) 2022 г. https://data.consilium.europa.eu/doc/document/ST-11583-2022-INIT/bg/pdf

Регламент (ЕС) 2016/679 – (Общ регламент относно защитата на данните, ОРЗД)

Директива (ЕС) 2016/680 относно правоприлагането в областта на защитата на данните

Закон за защита на личните данни

Как се определя дали едно предприятие е микро, малко и средно? https://evroprogrami.com/polezno/chesto-zadavani-vaprosi/kak-se-opredelya-dali-edno-predpriyatie-e-mikro-malko-i-sredno/

Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД

Насоки 4/2021 относно кодексите за поведение като средство за предаване на данни

Препоръки 01/2020 относно мерките, които допълват инструментите за предаване, за да се гарантира спазването на нивото на защита на личните данни, заложено в ЕС

Насоки 7/2022 относно сертифицирането като инструмент за предаване на данни

Информационна брошура на КЗЛД „Предаване на лични данни извън Европейския съюз” 2022 г.

Съвместно становище 2/2021 на Европейския комитет по защита на данните и Европейския надзорен орган по защита на данните във връзка с Решението за изпълнение на Европейската комисия относно стандартните договорни клаузи за трансфера на лични данни към трети държави

Препоръки 1/2022 относно заявлението за одобрение и елементите и принципите, които могат да бъдат намерени в задължителните фирмени правила на администратор на лични данни (член 47 от ОРЗД)

Трансферът на лични данни в контекста на решение по дело Schrems II; Балев, Константин; 2020

https://www.riskcompliance.bg/news/%D0%BB%D0%B8%D1%87%D0%BD%D0%B8-%D0%B4%D0%B0%D0%BD%D0%BD%D0%B8-schrems/

8 Отчетността като нов принцип на GDPR, 2018 г. http://privacyblog.dpc.bg/index.php/2018/05/22/8-accounting-as-a-new-gdpr_principle/

http://privacyblog.dpc.bg/index.php/author/marketing/

Комисия за защита на личните данни
Председател: Венцислав Караджов
Членове: Цанко Цолов
Мария Матева
Веселин Целков

Информационен бюлетин № 1 (106) 2024 г.
Издава се съгласно чл. 10, ал. 3 от ЗЗЛД
Уеб сайт на КЗЛД: www.cpdp.bg
Разпространява се в електронен вид

ISSN 2367-7759