РАБОТНА ГРУПА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПО ЧЛЕН 29

17/BG

WP 253

Насоки относно прилагането и определянето на административните наказания „глоба“ или „имуществена санкция“ за целите на Регламент (ЕС) 2016/679

Приети на 3 октомври 2017 г.

Тази работна група е създадена в съответствие с член 29 от Директива 95/46/ЕО. Тя е независим европейски консултативен орган относно защитата на личните данни и неприкосновеността на личния живот. Нейните задачи са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО.

Секретариатът е осигурен от Дирекция C (Основни права и гражданство на Съюза) на Генерална дирекция „Правосъдие и потребители“ на Европейската комисия, B-1049 Brussels, Belgium, Офис № MO-59 03/075.

Уебсайт: http://ec.europa.eu/justice/data-protection/index_en.htm

РАБОТНАТА ГРУПА ЗА ЗАЩИТА НА ЛИЦАТА ПРИ

ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

създадена с Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г.,

като взе предвид членове 29 и 30 от нея,

като взе предвид Правилника за дейността си,

ПРИЕ НАСТОЯЩИТЕ НАСОКИ:

Съдържание:

I. Въведение

ЕС проведе всеобхватна реформа на регулирането по отношение на защитата на данните в Европа. Реформата се основава на няколко стълба (основни компонента): съгласувани правила, опростени процедури, координирани действия, участие на ползвателите, по-ефективно информиране и засилени правомощия за прилагане.

Отговорностите на администраторите и обработващите лични данни бяха увеличени, за да се гарантира, че личните данни на лицата са защитени по ефективен начин. Надзорните органи разполагат с правомощия да гарантират, че принципите на Общия регламент относно защитата на данните (наричан по-нататък „Регламентът“), както и правата на засегнатите лица се спазват в съответствие с буквата и духа на Регламента.

Последователното прилагане на правилата за защита на данните е от основно значение за хармонизирания режим за защита на данните. Административните наказания „глоба“ или „имуществена санкция“ представляват основен елемент в новия режим на правоприлагане, въведен с Регламента, като заемат важно място в набора от инструменти за правоприлагане на надзорните органи заедно с другите мерки, предвидени в член 58.

Настоящият документ е предназначен да се използва от надзорните органи, за да се гарантира по-добро прилагане и изпълнение на Регламента, и изразява тяхното общо разбиране на разпоредбите на член 83 от Регламента, както и взаимодействието му с членове 58 и 70 и съответните им съображения.

По-специално съгласно член 70, параграф 1, буква д) Европейският комитет по защита на данните (наричан по-нататък „ЕКЗД“) е оправомощен да издава насоки, препоръки и най-добри практики с цел насърчаване на съгласуваното прилагане на Регламента, а в член 70, параграф 1, буква к) се предвиждат насоки относно определянето на размера на административните наказания „глоба“ или „имуществена санкция“.

Настоящите насоки не са изчерпателни, нито включват разяснения относно разликите между административноправните, гражданскоправните или наказателноправните системи при налагането на административни санкции като цяло.

За да се постигне съгласуван подход по отношение на налагането на административните наказания „глоба“ или „имуществена санкция“, който да отразява адекватно всички принципи в настоящите насоки, ЕКЗД постигна съгласие по общо разбиране за критериите за оценка в член 83, параграф 2 от Регламента, и следователно ЕКЗД и отделните надзорни органи са съгласни да използват настоящите насоки като общ подход.

II. Принципи

След като бъде установено нарушение на Регламента въз основа на оценка на фактите по случая, компетентният надзорен орган трябва да определи най-подходящата корективна мярка или мерки с цел справяне с нарушението. В разпоредбите на член 58, параграф 2, букви б)—й)[1] се посочва какви инструменти могат да бъдат използвани от надзорните органи с цел справяне с нарушение от страна на администратор или обработващ лични данни. При използването на тези правомощия надзорните органи трябва да спазват следните принципи:

---

1. Нарушението на Регламента следва да води до налагане на „еквивалентни санкции“

Понятието „еквивалентност“ е от основно значение при определянето на обхвата на задълженията на надзорните органи, за да се гарантира съгласуваност при използването на корективните им правомощия съгласно член 58, параграф 2 като цяло, и в частност налагането на административни наказания „глоба“ или „имуществена санкция“[2].

За да се гарантира последователно и високо ниво на защита на физическите лица, както и за да се премахнат препятствията пред движението на лични данни в Съюза, ***нивото на защита следва да бъде равностойно*** *във всички държави членки* (съображение 10). В съображение 11 се пояснява фактът, че равностойното ниво на защита на личните данни навсякъде в Съюза наред с другото изисква „*еквивалентни правомощия за наблюдение и гарантиране на спазването на правилата за защита на личните данни и еквивалентни санкции за нарушенията в държавите членки*“. В допълнение към това еквивалентните санкции във всички държави членки, както и ефективното сътрудничество между надзорните органи на отделните държави членки се възприемат като начин „*да се попречи на различията да възпрепятстват свободното движение на лични данни в рамките на вътрешния пазар*“, в съответствие със съображение 13 от Регламента.

В сравнение с Директива 95/46/ЕО в Регламента се определя по-солидна основа за по-високо ниво на съгласуваност, тъй като Регламентът е пряко приложим в държавите членки. Докато надзорните органи действат „напълно независимо“ (член 52) от националните правителства, администраторите или обработващите лични данни, те са задължени да си сътрудничат „*с оглед осигуряване на съгласувано прилагане и изпълнение на настоящия регламент*“ (член 57, параграф 1, буква ж).

В Регламента се призовава за по-голяма съгласуваност при налагането на санкции в сравнение с Директива 95/46/ЕО. В трансгранични случаи съгласуваността се постига най-вече чрез механизма за сътрудничество („обслужване на едно гише“) и до известна степен чрез механизма за съгласуваност, определен в новия Регламент.

В обхванатите от Регламента случаи от национален мащаб надзорните органи ще прилагат настоящите насоки в дух на сътрудничество в съответствие с член 57, параграф 1, буква ж) и

[1] В член 58, параграф 2, буква а) се предвижда, че могат да се отправят предупреждения, когато „има вероятност операции по обработване на данни [...] да нарушат разпоредбите на настоящия регламент“. С други думи, в обхванатия от разпоредбата случай все още не е извършено нарушение на Регламента.

[2] Дори ако правните системи на някои държави — членки на ЕС, не позволяват налагане на административните наказания „глоба“ или „имуществена санкция“, посочени в Регламента, прилагането на правилата в тези държави членки трябва да има ефект, равностоен на административни наказания „глоба“ или „имуществена санкция“, налагани от надзорни органи (съображение 151). Съдилищата са обвързани от Регламента, но не и от настоящите насоки на ЕКЗД.

член 63 с цел да се гарантира последователно прилагане и изпълнение на Регламента. Въпреки че надзорните органи остават независими при избора на корективни мерки измежду посочените в член 58, параграф 2, следва да се избягва избирането на различни корективни мерки от надзорните органи в сходни случаи.

Същият принцип се прилага, когато тези корективни мерки се налагат под формата на глоби или имуществени санкции.

---

2. Като всички корективни мерки, налагани от надзорните органи, административните наказания „глоба“ или „имуществена санкция“ следва да бъдат „ефективни, пропорционални и възпиращи“

Подобно на всички корективни мерки като цяло, административните наказания „глоба“ или „имуществена санкция“ следва да отразяват адекватно естеството, тежестта и последиците от нарушението, а надзорните органи трябва да оценят всички факти по случая по начин, който е последователен и обективно обоснован. Оценката за това, какви мерки са ефективни, пропорционални и възпиращи във всеки отделен случай, също така ще трябва да отразява целта, преследвана с избраната корективна мярка, т.е. възстановяване на спазването на правилата или санкциониране на неправомерно поведение (или и двете).

Надзорните органи следва да определят корективни мерки, които са „*ефективни, пропорционални и възпиращи*“ (член 83, параграф 1), както в случаите от национален мащаб (член 55), така и в случаите, свързани с трансгранично обработване на лични данни (съгласно определението в член 4, параграф 23).

В настоящите насоки се признава, че е възможно в националното законодателство да са определени допълнителни изисквания относно процедурите по правоприлагане, които надзорните органи трябва да следват. Те могат да включват например съобщаване на адрес, формуляри, крайни срокове за представяне на становища, обжалване, правоприлагане, заплащане[3].

Такива изисквания обаче не следва да възпрепятстват на практика постигането на ефективност, пропорционалност или възпиращ ефект.

Ефективността, пропорционалността и възпиращият ефект ще бъдат определени по-точно с практиките, които ще се установят в рамките на надзорните органи (във връзка със защитата на данните, както и натрупания опит от други регулаторни сектори), както и чрез съдебната практика, свързана с тълкуването на тези принципи.

С цел да налага глоби или имуществени санкции, които са ефективни, пропорционални и възпиращи, надзорният орган следва да използва определението на понятието за предприятие, предоставено от Съда на ЕС за целите на прилагането на членове 101 и 102 от ДФЕС, а именно, че понятието за предприятие **се разбира като означаващо** стопанска единица, която може да се състои от дружеството майка и всички участващи дъщерни дружества. В съответствие с

[3] Например в конституционната рамка и законопроекта относно защитата на данните в Ирландия се предвижда, че преди да се извърши оценка на размера на санкцията или санкциите, се взема официално решение относно наличието на нарушение, което се съобщава на съответните страни. Решението относно наличието на нарушение не подлежи на преразглеждане по време на оценката на размера на санкцията или санкциите.

правото на ЕС и европейската съдебна практика[4] понятието „предприятие“ трябва да се разбира като стопанска единица, която извършва търговски/стопански дейности, независимо от съответното юридическо лице (съображение 150).

3. Компетентният надзорен орган прави оценка „във всеки конкретен случай“

Административните наказания „глоба“ или „имуществена санкция“ могат да се налагат във връзка с редица нарушения. В член 83 от Регламента се предвижда хармонизиран подход към нарушенията на задълженията, посочени изрично в параграфи 4—6. Съгласно законодателството на държавите членки прилагането на член 83 може да бъде разширено, така че да обхване публичните органи и органите, установени в съответната държава членка. Освен това законодателството на държавите членки може да предвижда възможност или дори задължение за налагането на глоба или имуществена санкция за нарушаване на други разпоредби, различни от посочените в член 83, параграфи 4—6.

Съгласно Регламента се изисква оценяването на всеки случай да се извършва индивидуално[5]. Отправната точка за такава индивидуална оценка е член 83, параграф 2. Този параграф гласи: „*Когато се взема решение дали да бъде наложено административно наказание „глоба“ или „имуществена санкция“ и се определя нейният размер, във всеки конкретен случай надлежно се разглеждат следните елементи...*“. В съответствие с това и също така с оглед на съображение 148[6] надзорният орган носи отговорност да определи най-подходящата мярка или

[4] Определението в съдебната практика на Съда на ЕС е: „понятието за предприятие обхваща всяко образувание, което извършва стопанска дейност, независимо от неговия правен статут и начина му на финансиране“ (дело Höfner и Elsner, ECLI:EU:C:1991:161, т. 21). Предприятието „трябва да се схваща като обозначаващо една стопанска единица, макар и от правна гледна точка тази стопанска единица да е съставена от няколко физически или юридически лица“ (дело Confederación Española de Empresarios de Estaciones de Servicio, ECLI:EU:C:2006:784, т. 40).

[5] В допълнение към прилагането на критериите по член 83 съществуват и други разпоредби за укрепване на основата за прилагането на този подход, като например:

- съображение 141: „*Разследването въз основа на жалби следва да се извършва под съдебен контрол и в целесъобразна за конкретния случай степен*“.
- съображение 129: „*Надзорните органи следва да упражняват правомощията си в съответствие с подходящите процедурни гаранции, определени в правото на Съюза и правото на държава членка, независимо, справедливо и в разумен срок*“. *По-специално всяка мярка следва да бъде подходяща, необходима и пропорционална с оглед на осигуряването на съответствие с настоящия регламент, като се отчитат обстоятелствата при всеки конкретен случай...*“.
- член 57, параграф 1, буква е): „[...] *разглежда жалбите, подадени от субект на данни или от структура, организация или сдружение в съответствие с член 80, и разследва предмета на жалбата, доколкото това е целесъобразно*“.

[6] „*За да се укрепи прилагането на правилата на настоящия регламент, освен или вместо подходящи мерки, наложени от надзорния орган съгласно настоящия регламент, при нарушение на регламента следва да се налагат санкции, включително административни наказания „глоба“ или „имуществена санкция“. При леки нарушения или ако глобата, която може да бъде наложена, представлява несъразмерна тежест за физическо лице, вместо глоба може да бъде отсъдено порицание. Следва обаче да се отдаде надлежно внимание на естеството, тежестта и продължителността на нарушението, умишления характер на нарушението, действията за смекчаване на последиците от претърпените вреди, степента на отговорност или евентуални предишни нарушения от подобен характер, начина, по който нарушението е станало известно на надзорния орган, спазването на мерките, наложени на администратора или на обработващия лични данни, придържането към кодекс на поведение и всякакви други утежняващи или смекчаващи фактори. Налагането на санкции,*

мерки. В случаите, посочени в член 83, параграфи 4—6, този избор **трябва** да включва разглеждане на всички корективни мерки, което означава и да се разгледа дали да се наложи подходящо административно наказание „глоба“ или „имуществена санкция“, било то самостоятелно или в съчетание с друга корективна мярка съгласно член 58, параграф 2.

Глобите или имуществените санкции представляват важен инструмент, който надзорните органи следва да използват в подходящи обстоятелства. Надзорните органи се насърчават да следват внимателно обмислен и балансиран подход при използването на корективни мерки, така че отговорът на нарушението да бъде както ефективен и възпиращ, така и пропорционален. Целта е глобите или имуществените санкции да не се разглеждат като крайна мярка и да не се избягва налагането им, но същевременно и да не се използват по начин, който би обезсилил ефективността им като инструмент.

Когато ЕКЗД е компетентен в съответствие с член 65 от Регламента, той приема решения със задължителен характер по спорове между органи, свързани по-специално с определянето дали е налице нарушение. Когато чрез относимо и обосновано възражение се повдигне въпросът дали корективната мярка е в съответствие с Регламента, в решението на ЕКЗД също така се разглежда начинът, по който са спазени принципите на ефективност, пропорционалност и възпиране във връзка с административното наказание „глоба“ или „имуществена санкция“, предложено в проекта на решение на компетентния надзорен орган. Отделно ще бъдат изготвени насоки на ЕКЗД относно прилагането на член 65 от Регламента с повече подробности относно вида решение, което следва да се взема от ЕКЗД.

4. Хармонизираният подход към административните наказания „глоба“ или „имуществена санкция“ в областта на защитата на данните изисква активно участие и обмен на информация между надзорните органи

В настоящите насоки се признава, че за някои национални надзорни органи правомощията за налагане на глоби или имуществени санкции представляват новост в областта на защитата на данните, като пораждат многобройни въпроси, що се отнася до ресурсите, организацията и процедурата. Съществено е, че решенията, чрез които надзорните органи упражняват предоставените им правомощия за налагане на глоби или имуществени санкции, ще подлежат на обжалване пред националните съдилища.

Надзорните органи следва да осъществяват сътрудничество помежду си и ако е целесъобразно, с Европейската комисия, чрез определените в Регламента механизми за сътрудничество, така че да се подпомогнат официалният и неофициалният обмен на информация, например чрез провеждане на редовни работни срещи. Това сътрудничество следва да е съсредоточено върху техния опит и практика при упражняването на правомощията за налагане на глоби или имуществени санкции, така че в крайна сметка да се постигне подобрена съгласуваност.

Проактивното споделяне на информация, в допълнение към нововъзникващата съдебна практика относно използването на тези правомощия за налагане на глоби или имуществени санкции, може да доведе до преразглеждането на принципите или специфичните подробности в настоящите насоки.

включително административни наказания „глоба“ или „имуществена санкция“, следва да подлежи на подходящи процедурни мерки за защита в съответствие с общите принципи на правото на Съюза и Хартата, включително ефективна съдебна защита и справедлив съдебен процес“.

III. Критерии за оценка в член 83, параграф 2

В член 83, параграф 2 е представен списък с критерии, които се очаква да бъдат използвани от надзорните органи, когато се преценява дали следва да бъде наложена глоба или имуществена санкция и какъв да бъде нейният размер. Препоръчва се не да бъдат оценявани многократно едни и същи критерии, а да се извършва оценка, при която да се вземат предвид всички обстоятелства по конкретния случай, както е предвидено в член 83[7].

Заключенията от първия етап на оценката могат да се използват на втория етап, свързан с определянето на размера на глобата или имуществената санкция, като по този начин се избягва необходимостта от повторно оценяване с използване на същите критерии.

В настоящия раздел се съдържат насоки за надзорните органи по отношение на начина на тълкуване на отделните факти по случая с оглед на критериите в член 83, параграф 2.

а) естеството, тежестта и продължителността на нарушението

В разпоредбите на член 83, параграфи 4—6 почти всички задължения на администраторите и обработващите лични данни съгласно Регламента са категоризирани в зависимост от тяхното **естество**. С определянето в Регламента на два различни максимални размера на административните наказания „глоба“ или „имуществена санкция“ (10/20 милиона евро) вече се посочва, че нарушението на някои разпоредби на Регламента може да е по-сериозно от нарушението на други разпоредби. При все това, когато компетентният надзорен орган оценява фактите по случая в светлината на общите критерии, предвидени в член 83, параграф 2, той може да реши, че в конкретния случай има по-голяма или съответно по-малка необходимост да се реагира с корективна мярка под формата на глоба или имуществена санкция. Когато бъде наложена глоба или имуществена санкция като единствената или като една от няколко подходящи корективни мерки, се прилага категоризацията от Регламента (член 83, параграфи 4—6), за да се определи максималната глоба или имуществена санкция, която може да бъде наложена в съответствие с естеството на въпросното нарушение.

Със съображение 148 се въвежда понятието „леки нарушения“. Те могат да представляват нарушение на една или няколко от разпоредбите на Регламента, посочени в член 83, параграфи 4 или 5. В резултат на оценката на критериите в член 83, параграф 2 обаче надзорният орган може да счете, че в конкретните обстоятелства по случая нарушението например не създава значителен риск за правата на съответните субекти на данни и не засяга същността на въпросното задължение. В такива случаи глобата или имуществената санкция може (но невинаги) да бъде заменена с порицание.

В съображение 148 не се съдържа задължение за надзорния орган винаги да заменя глоба или имуществена санкция с порицание в случай на леко нарушение („*вместо глоба може да бъде отсъдено порицание*“), а по-скоро възможност, която може да бъде използвана след извършването на конкретна оценка на всички обстоятелства по случая.

Съображение 148 осигурява същата възможност за замяна на глоба или имуществена санкция с порицание, когато администраторът е физическо лице и глобата или имуществената санкция, която може да бъде наложена, би представлявала несъразмерна тежест. Отправната точка за това е, че надзорният орган трябва да прецени дали се изисква налагането на глоба или имуществена санкция с оглед на обстоятелствата по разглеждания случай. Ако прецени, че

[7] В някои държави, поради националните процесуални правила, произтичащи от конституционни изисквания, оценката на санкцията, която следва да бъде наложена, може да се извършва отделно, след като се извърши оценка за това дали е налице нарушение. Следователно това може да ограничи съдържанието и степента на подробност на проекта на решение, което се постановява от водещия надзорен орган в тези държави.

трябва да се наложи глоба или имуществена санкция, надзорният орган трябва също така да прецени дали тя би представлявала несъразмерна тежест за дадено физическо лице.

В Регламента не се посочват конкретни суми за отделни нарушения, а само таван (максимален размер). Това може да бъде индикация за относително по-ниска степен на тежест при нарушение на задълженията, посочени в член 83, параграф 4, в сравнение с посочените в член 83, параграф 5. Ефективният, пропорционален и възпиращ отговор на нарушение на член 83, параграф 5 обаче ще зависи от обстоятелствата по случая.

Следва да се отбележи, че нарушенията на Регламента, които по своето естество могат да попадат в категорията „до 10 000 000 EUR или до 2 % от общия годишен световен оборот“, както е посочено в член 83, параграф 4, при определени обстоятелства могат да бъдат причислени към по-висока категория (20 милиона евро). Такъв вероятно би бил случаят, ако тези нарушения вече са били предмет на разпореждане[8] на надзорния орган, което администраторът или обработващият лични данни не е спазил[9] (член 83, параграф 6). На практика разпоредбите на националното законодателство могат да окажат въздействие върху тази оценка[10]. Редом с естеството на нарушението, „*обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда*“ също са показателни за **тежестта** на нарушението. При наличието на няколко отделни нарушения, извършени заедно в рамките на конкретен единичен случай, надзорният орган може да наложи административни наказания „глоба“ или „имуществена санкция“ на ниво, което е ефективно, пропорционално и възпиращо, като не надхвърля максималния размер за най-тежкото нарушение. Следователно ако бъде установено нарушение на членове 8 и 12, надзорният орган може да наложи корективните мерки, определени в член 83, параграф 5,

[8] Предвидените разпореждания в член 58, параграф 2 са:

- да разпорежда на администратора или обработващия лични данни да изпълнят исканията на субекта на данни да упражнява правата си съгласно настоящия регламент;
- да разпорежда на администратора или обработващия лични данни да съобразят операциите по обработване на данни с разпоредбите на настоящия регламент и, ако е целесъобразно, това да стане по указан начин и в определен срок;
- да разпорежда на администратора да съобщава на субекта на данните за нарушение на сигурността на личните данни;
- да налага временно или окончателно ограничаване, в т.ч. забрана, на обработването на данни;
- да разпорежда коригирането или изтриването на лични данни, или ограничаването на обработването им съгласно членове 16, 17 и 18, както и уведомяването за тези действия на получатели, пред които личните данни са били разкрити съгласно член 17, параграф 2 и член 19;
- да разпорежда на сертифициращия орган да отнеме сертификат, издаден съгласно членове 42 и 43, или да разпорежда на сертифициращия орган да не издава сертификат, ако изискванията за сертифицирането не са спазени или вече не се спазват;
- да разпорежда преустановяването на потока на данни към получател в трета държава или към международна организация.

[9] При прилагането на член 83, параграф 6 по необходимост трябва да се зачита националното процесуално право. В националното законодателство се определя как се издава разпореждане, как се прави уведомление за него, от кой момент поражда действие, дали има „гратисен период“ за предприемане на мерки за спазване на правилата. По-специално следва да бъде взет предвид ефектът от евентуалното обжалване на изпълняемостта на разпореждането.

[10] В резултат на законовите разпоредби за давностни срокове е възможно предишно разпореждане на надзорния орган вече да не може да бъде взето под внимание поради периода, който е изминал от издаването на предишното разпореждане. В някои юрисдикции съществуват правила, съгласно които след като изтече давностният срок по отношение на дадено разпореждане, не може да се налага глоба или имуществена санкция съгласно член 83, параграф 6 за неспазването на това разпореждане. Всеки надзорен орган в рамките на всяка юрисдикция трябва да определи какво ще бъде отражението върху него от подобни правила.

които отговарят на категорията на по-тежкото нарушение, а именно на нарушението на член 12. Предоставянето на повече подробности на този етап попада извън обхвата на настоящите насоки (подробните изчисления ще бъдат разгледани на евентуален следващ етап от разработването на насоките).

Изброените по-долу фактори следва да се оценяват заедно, например броят на субектите на данни заедно с възможното въздействие върху тях.

Следва да се оцени **броят** на засегнатите субекти на данни, за да се определи дали това е изолиран случай, или показва по-системно нарушение или липса на подходящи практики. Това не означава, че изолираните случаи не следва да подлежат на действия по правоприлагане, тъй като дори един изолиран случай може да засегне множество субекти на данни. В зависимост от обстоятелствата по случая това ще зависи например от общия брой на регистрираните лица във въпросната база данни, броя на ползвателите на дадена услуга, броя на потребителите или цялото население на страната.

Също така трябва да се оцени **целта** на обработването на данни. В становището на Работната група по член 29 относно „ограничаването в рамките на целта“[11] бяха анализирани двата основни градивни елемента на този принцип в законодателството за защита на данните: конкретизиране на целта и съвместимо използване. Когато оценяват целта на обработването в контекста на член 83, параграф 2, надзорните органи следва да проучват степента, в която при обработването се спазват двата основни компонента на този принцип[12]. В определени ситуации надзорният орган може да сметне за необходимо да извърши по-задълбочен анализ на целта на обработването в рамките на анализа по член 83, параграф 2.

Ако субектите на данни претърпят **вреди**, трябва да бъде взета предвид степента на причинените им вреди. Обработването на лични данни може да породи рискове за правата и свободите на лицата, както е посочено в съображение 75:

> „*Рискът за правата и свободите на физическите лица, с различна вероятност и тежест, може да произтича от обработване на лични данни, което би могло да доведе до физически, материални или нематериални вреди, по-специално: когато обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация, или други значителни икономически или социални неблагоприятни последствия; или когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни; когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили; когато се*

[11] WP 203, Становище 03/2013 относно ограничаването в рамките на целта, достъпно на: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Вж. също така WP 217, Становище 6/2014 относно понятието за законни интереси на администратора на лични данни съгласно член 7 от Директива 95/46/ЕО, стр. 24, във връзка с въпроса: „Какво прави един интерес законен или незаконен?“.

обработват лични данни на уязвими лица, по-специално на деца; или когато обработването включва голям обем лични данни и засяга голям брой субекти на данни“.

Ако в резултат на нарушението на Регламента са били претърпени вреди или е вероятно да бъдат претърпени такива, надзорният орган следва да вземе това предвид при избора си на корективна мярка, макар че самият той не е компетентен да постанови конкретно обезщетение за претърпените вреди.

Налагането на глоба или имуществена санкция не зависи от това, дали надзорният орган е в състояние да установи причинно-следствена връзка между нарушението и имуществените вреди (вж. например член 83, параграф 6).

Продължителността на нарушението може да е индикация например за:

а) умишлено поведение от страна на администратора, или

б) непредприемане на подходящи превантивни мерки, или

в) неспособност да се въведат изискваните технически и организационни мерки.

б) дали нарушението е извършено умишлено или по небрежност

По принцип „умисъл“ включва съзнаване на характеристиките на нарушението и воля за извършването му, докато „неумишлено“ означава, че не е било налице намерение да се извърши нарушението, но въпреки това администраторът/обработващият лични данни не е положил дължимата грижа, както се изисква по закон.

Като цяло се приема, че умишлените нарушения, при които се демонстрира явно незачитане на законовите разпоредби, са по-тежки от неумишлените нарушения и че поради това при първите е по-вероятно да е основателно налагането на административно наказание „глоба“ или „имуществена санкция“. Съответните заключения дали нарушението е извършено умишлено, или по небрежност се правят въз основа на данните за обективните елементи на поведението, събрани от фактите по случая. Освен това нововъзникващата съдебна практика и практиките в областта на защитата на данните във връзка с прилагането на Регламента ще покажат кои обстоятелства съставляват по-ясни прагове за оценка дали нарушението е умишлено.

Примери за обстоятелства, които са показателни за умишлени нарушения, могат да бъдат неправомерно обработване на данни, разпоредено изрично от висшето ръководство на администратора или в разрез със съветите на длъжностното лице по защита на данните, или при незачитане на съществуващи политики, например получаване и обработване на данни относно служителите на конкурентно дружество с цел дискредитирането му на пазара.

Други примери могат да бъдат:

- промяната на лични данни, за да се създаде подвеждащо (положително) впечатление, че дадени цели са постигнати — свидетели сме на това в контекста на целите за времето на изчакване в болница;
- търговията с лични данни за маркетингови цели, т.е. продажбата на данните като данни, за които е дадено разрешение за обработване от субектите на данни, като не се проверява или се пренебрегва тяхното мнение за това как следва да бъдат използвани техните данни.

Други обстоятелства, като например непознаване и неспазване на съществуващите политики, човешка грешка, липса на проверка дали в публикуваната информация има лични данни, липса

на своевременно инсталиране на технически актуализации, неприемане на политики (а не просто неприлагането им), могат да са индикация за небрежност.

Предприятията следва да отговарят за осигуряването на адекватни структури и ресурси в зависимост от естеството и сложността на своята дейност. Администраторите и обработващите лични данни не могат да оправдават нарушенията на законодателството в областта на защитата на данните с недостиг на ресурси. Рутинните практики и документирането на дейностите по обработване следват основан на риска подход в съответствие с Регламента.

Съществуват „сиви зони“, които ще оказват влияние върху вземането на решения дали да се наложи корективна мярка или не, и може да се наложи органът да проведе по-обстойно разследване, за да определи фактите по случая и да гарантира, че всички специфични обстоятелства по конкретния случай са взети предвид в достатъчна степен.

в) действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни

Администраторите и обработващите лични данни са задължени да прилагат технически и организационни мерки за осигуряване на съобразено с риска ниво на сигурност, да извършват оценки на въздействието върху защитата на личните данни и да ограничат произтичащите от обработването на лични данни рискове за правата и свободите на физическите лица. Когато обаче бъде извършено нарушение и субектът на данни претърпи вреди, отговорната страна трябва да направи всичко възможно, за да ограничи последиците от нарушението за засегнатото лице или лица. Такова отговорно поведение (или липсата му) би трябвало да бъде взето предвид от надзорния орган при избора на корективна мярка или мерки, както и при определянето на размера на санкцията, която да бъде наложена в конкретния случай.

Въпреки че утежняващите или смекчаващите фактори са особено подходящи за адаптиране на размера на глобата или имуществената санкция с оглед на конкретните обстоятелства по случая, тяхната роля при избора на подходяща корективна мярка не следва да се подценява. В случаите, когато оценката въз основа на други критерии не позволява на надзорния орган категорично да заключи, че е уместно да се наложи административното наказание „глоба“ или „имуществена санкция“ като самостоятелна корективна мярка или в съчетание с други мерки по член 58, такива утежняващи или смекчаващи обстоятелства могат да помогнат при избора на подходящи мерки, като наклонят везните към мерките, които са по-ефективни, пропорционални и възпиращи в дадения случай.

Тази разпоредба функционира като оценка на степента на отговорност на администратора след извършването на нарушението. Тя може да обхване случаи, в които администраторът/обработващият лични данни очевидно не е походил необмислено/небрежно, и е направил всичко възможно да коригира своите действия, когато е разбрал за нарушението.

Регулаторният опит на надзорните органи във връзка с Директива 95/46/ЕО вече показа, че може да бъде уместно да се действа с известна степен на гъвкавост спрямо администраторите/обработващите лични данни, които са признали своите нарушения и са поели отговорност да коригират или ограничат въздействието от своите действия. Това може да включва (макар да не би довело до по-гъвкав подход във всеки отделен случай) примери като:

- осъществяване на контакт с други администратори/обработващи лични данни, които може да са участвали в допълнително обработване на данните, например ако част от данните погрешно са били споделени с трети страни.
- своевременни действия, предприети от администратора/обработващия лични данни, с цел да не се позволи нарушението да продължи или да се разрасне до степен или етап, на който би имало много по-сериозно въздействие.

г) степента на отговорност на администратора или обработващия лични данни, като се вземат предвид технически и организационни мерки, въведени от тях в съответствие с членове 25 и 32

С Регламента се въвежда много по-високо ниво на отчетност на администратора в сравнение с Директива 95/46/ЕО за защита на личните данни.

Оценката на степента на отговорност на администратора или обработващия лични данни в контекста на прилагането на подходящи корективни мерки може да включва следните въпроси:

- Въвел ли е администраторът технически мерки, които следват принципите за защита на данните на етапа на проектирането или по подразбиране (член 25)?
- Въвел ли е администраторът организационни мерки, с които се прилагат принципите за защита на данните на етапа на проектирането и по подразбиране (член 25) на всички равнища в организацията?
- Въвел ли е администраторът/обработващият лични данни подходящо ниво на сигурност (член 32)?
- Известни ли са съответните рутинни практики/политики за защита на данните и прилагат ли се на подходящото управленско равнище в рамките на организацията (член 24)?

Съгласно членове 25 и 32 от Регламента се изисква администраторите да вземат предвид „*достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица*“. С тези разпоредби не се налага задължение по отношение на целта, а задължения по отношение на средствата, т.е. администраторът трябва да извърши необходимите оценки и да достигне до подходящи заключения. Въпросът, на който след това трябва да отговори надзорният орган, е до каква степен администраторът е „отговорил на очакванията“ предвид естеството, целите или обема на обработването с оглед на наложените му задължения съгласно Регламента.

При тази оценка следва надлежно да се вземат предвид всички процедури или методи, представляващи „най-добри практики“, когато такива съществуват и се прилагат. Важно е да се вземат предвид стандартите в съответния отрасъл, както и кодексите за поведение в съответната област или професия. Професионалните кодекси могат да дадат индикация за това какво се счита за обичайна практика в областта и какво е нивото на знанията относно различните средства за справяне с типични проблеми, свързани със сигурността при обработването на данни.

Макар че в идеалния случай по принцип следва да се прилагат най-добрите практики, при оценката на степента на отговорност по всеки конкретен случай трябва да се вземат предвид специфичните обстоятелства.

д) евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни

Целта на този критерий е да се оценят досегашните резултати на образуването, извършило нарушението. Надзорните органи следва да вземат предвид, че обхватът на оценката по тази точка може да бъде изключително широк, защото всеки вид нарушение на Регламента, макар и с различно естество в сравнение с понастоящем разследваното от надзорния орган нарушение, може да бъде „свързано“ за целите на оценката, тъй като може да показва общо ниво на недостатъчни знания или незачитане на правилата за защита на данните.

Надзорният орган следва да направи оценка за следното:

- Извършвал ли е администраторът/обработващият лични данни същото нарушение и преди?
- Извършвал ли е администраторът/обработващият лични данни нарушение на Регламента по същия начин? (например вследствие на недостатъчни знания за съществуващите рутинни практики в организацията или вследствие на неподходяща оценка на риска, липса на своевременен отговор на искания от субекта на данни, необосновано забавяне при отговора на искания и др.).

е) степента на сътрудничество с надзорния орган с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него

В член 83, параграф 2 се предвижда степента на сътрудничество да може да се разглежда „надлежно“, когато се взема решение дали да бъде наложено административно наказание „глоба“ или „имуществена санкция“ и се определя нейният размер. Регламентът не съдържа точен отговор на въпроса по какъв начин да се вземат предвид усилията на администраторите или обработващите лични данни за отстраняване на вече установено от надзорния орган нарушение. Освен това е ясно, че критериите биха се прилагали обикновено при определянето на размера на глобата или имуществената санкция, която ще бъде наложена.

Когато обаче в резултат на намесата на администратора отрицателните последици по отношение на правата на лицата не са се проявили или са имали по-ограничено въздействие, отколкото биха могли да имат без тази намеса, това също би могло да се вземе предвид при избора на корективна мярка, която е пропорционална в конкретния случай.

Следният въпрос представлява пример за случай, при който евентуално би било уместно да се отчете сътрудничеството с надзорния орган:

- Реагирало ли е образуването по определен начин на исканията на надзорния орган на етапа на разследване на конкретния случай, в резултат на което въздействието върху правата на лицата е било ограничено значително?

Следва да се отбележи обаче, че не би било уместно да се придава допълнителна тежест на сътрудничество, което се изисква по закон, например образуването при всички случаи е задължено да осигури достъп на надзорния орган до помещенията с цел одит/проверка.

ж) категориите лични данни, засегнати от нарушението

По-долу са дадени някои примери за ключови въпроси, на които надзорният орган може да счете за необходимо да отговори в тази връзка, според случая:

- Свързано ли е нарушението с обработване на специални категории данни по членове 9 или 10 от Регламента?
- Могат ли данните да бъдат идентифицирани пряко или непряко?

- Обработването включва ли данни, разпространението на които би довело до непосредствени вреди/затруднения за лицето (и които попадат извън обхвата на категориите по членове 9 или 10)?
- Достъпни ли са данните пряко, без да е налице техническа защита, или са криптирани[13]?

з) начина, по който нарушението е станало известно на надзорния орган, по-специално дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението

Надзорният орган може да разбере за нарушението в резултат на разследване, жалба, статия в пресата, анонимен сигнал или уведомление от администратора. Съгласно Регламента администраторът е задължен да уведоми надзорния орган за нарушения на сигурността на личните данни. Когато администраторът просто изпълнява това задължение, спазването му не може да се тълкува като смекчаващ фактор. По подобен начин надзорният орган може да счете, че администратор/обработващ лични данни, който е действал небрежно, без да уведоми за нарушението, или поне без да уведоми за всички подробности по него, поради неадекватна оценка на степента на нарушението, също заслужава по-сериозна санкция, т.е. това вероятно няма да бъде категоризирано като леко нарушение.

и) когато на засегнатия администратор или обработващ лични данни преди са налагани мерки, посочени в член 58, параграф 2, във връзка със същия предмет на обработването, дали посочените мерки са спазени

Даден администратор или обработващ лични данни може вече да бъде в полезрението на надзорния орган с цел проследяване дали са спазени мерките, след като е било извършено предишно нарушение. В такива случаи контактите с длъжностното лице по защита на данните, ако има такова, вероятно са били интензивни. Следователно надзорният орган ще вземе предвид предишните контакти.

За разлика от критерия по буква д), този критерий за оценка цели единствено да напомни на надзорните органи да вземат предвид мерките, които самите те са постановили по-рано за същия администратор или обработващ лични данни „*във връзка със същия предмет на обработването*“.

й) придържането към одобрени кодекси на поведение съгласно член 40 или одобрени механизми за сертифициране съгласно член 42

Всеки надзорен орган има задължението да „*наблюдава и осигурява прилагането на настоящия регламент*“ (член 57, параграф 1, буква а). Администраторът или обработващият лични данни може да използва придържането към одобрени кодекси на поведение като начин да демонстрира спазването на изискванията в съответствие с член 24, параграф 3, член 28, параграф 5 или член 32, параграф 3.

Ако бъде нарушена разпоредба на Регламента, придържането към одобрен кодекс на поведение може да е индикация за степента на необходимостта от намеса от страна на надзорния орган посредством ефективно, пропорционално, възпиращо административно наказание „глоба“ или „имуществена санкция“ или друга корективна мярка. Съгласно член 40, параграф 4 одобреният кодекс на поведение съдържа „*механизми, които позволяват на [надзорния] орган да извършва задължителното наблюдение на спазването на неговите разпоредби*“.

[13] Фактът, че нарушението засяга единствено данни, позволяващи само непряко идентифициране, или дори псевдонимизирани/криптирани данни, невинаги следва да се счита за допълнителен смекчаващ фактор. За такива нарушения общата оценка на другите критерии може да сочи, в умерена или силна степен, че следва да бъде наложена глоба или имуществена санкция.

Когато администраторът или обработващият лични данни се е придържал към одобрен кодекс на поведение, надзорният орган може да се увери, че самата общност, която отговаря за прилагането на този кодекс, предприема подходящи действия срещу своя член, например чрез схеми за наблюдение и изпълнение на въпросния кодекс на поведение. Следователно надзорният орган може да счете, че тези мерки са достатъчно ефективни, пропорционални или възпиращи в конкретния случай и че не е необходимо да се налагат допълнителни мерки от самия надзорен орган. В съответствие с член 41, параграф 2, буква в) и член 42, параграф 4 чрез схемата за наблюдение могат да се наложат определени мерки за санкциониране на неспазването, включително суспендиране на членството в общността, за която се прилага кодексът, или изключване от нея на съответния администратор или обработващ лични данни. Независимо от това правомощията на органа за наблюдение не засягат „*задачите и правомощията на компетентния надзорен орган*“, което означава, че надзорният орган не е задължен да вземе предвид наложените преди това санкции по схемата за саморегулиране.

Неспазването на мерките за саморегулиране също така би могло да разкрие небрежност или умишлено неспазване от страна на администратора/обработващия лични данни.

к) всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението

Самата разпоредба съдържа примери за това какви други елементи могат да бъдат взети предвид, когато се определя дали административното наказание „глоба“ или „имуществена санкция“ е подходящо във връзка с нарушение на разпоредбите, посочени в член 83, параграфи 4—6.

Информацията относно реализираните печалби в резултат на нарушението може да бъде особено важна за надзорните органи, тъй като икономическата печалба от нарушението не може да се неутрализира чрез мерки, които нямат паричен компонент. Сам по себе си фактът, че администраторът е извлякъл изгода от нарушението на Регламента, може да е сериозна индикация, че следва да бъде наложена глоба или имуществена санкция.

IV. Заключение

Обмислянето на въпроси като посочените в предния раздел ще помогне на надзорните органи да определят въз основа на съответните факти по случая кои критерии са най-полезни, когато се взема решение дали да се наложи подходящо административно наказание „глоба“ или „имуществена санкция“ в допълнение към други мерки по член 58 или вместо тях. Като вземе предвид контекста, предоставен чрез тази оценка, надзорният орган ще определи най-ефективната, пропорционална и възпираща корективна мярка в отговор на нарушението.

В член 58 се предвиждат някои насоки относно мерките, които надзорният орган може да избере, тъй като самите корективни мерки са различни по своето естество и са подходящи за постигането на различни цели. Някои от мерките по член 58 дори могат да се съчетават, като така се постига регулаторно действие, състоящо се от повече от една корективна мярка.

Невинаги е необходимо съответната мярка да се допълва като се използва друга корективна мярка. Така например ефективността и възпиращият ефект на намесата на надзорния орган, като се отдаде необходимото внимание на това, какви мерки са пропорционални в конкретния случай, могат да бъдат постигнати чрез налагането само на глоба или имуществена санкция.

По същество органите трябва да възстановяват спазването чрез всички корективни мерки, които са на тяхно разположение. Надзорните органи също така са задължени да изберат най-подходящия канал за осъществяването на регулаторни действия. Това би могло да включва например наказателни санкции (когато съществуват на национално равнище).

Практиката на съгласувано налагане на административни наказания „глоба“ или „имуществена санкция“ в рамките на Европейския съюз постепенно се развива. Надзорните органи следва да работят заедно, когато предприемат действия, така че съгласуваността постоянно да се подобрява. Това може да се постигне чрез редовен обмен на информация чрез работни срещи за разглеждане на случаи или други мероприятия, които позволяват сравнение на случаи на поднационално, национално и трансгранично равнище. За да бъде подпомогната текущата дейност, се препоръчва към съответното подразделение на ЕКЗД да бъде създадена постоянна подгрупа.