

# GDPR в действие

## ДИСЦИПЛИНАРНИТЕ САНКЦИИ НА ОСНОВАНИЯ ОТ GDPR

Младен Младенов (PhD, MPS, LL.M, MPF, MSM)

Поредицата разглежда различни аспекти на съдебните претенции на основания от GDPR, административните санкции на основания от GPPR и дисциплинарните санкции на основания от GPPR. Подходът е насочен към обосновано предположение за едни бъдещи рискове за управленските, финансовите, счетоводните и юридическите екипи в организациите и в частния, и в публичния сектор. Добрите и отговорни мениджъри без забава още понастоящем трябва да възложат в тази насока одитен ангажимент на одитните звена или одитори в организациите, а на собствено отделно основание – и правни анализи на юридическите си екипи, юрисконсулти или обслужващи външни юристи или консултанти, защото професионално предвиденият риск винаги се явява здрава основа за устойчивостта на организацията в бъдещето.

**Д**исциплинарните санкции на основания от GDPR (наричан по-долу за краткост „Регламента“) със сигурност ще бъдат предмет на трудово-правна, административна и съдебна практика от сега нататък. От една страна, работниците и служителите трябва да са много внимателни и да не допускат дисциплинарни простъпки (т.е. виновно правоотношение), нарушаващи GDPR и националното законодателство по прилагането му. От друга страна, работодателите и органите по назначаване трябва да са безкомпромисни при санкционирането на подобни простъпки, имайки предвид важността на сигурността и защитата на личните данни на физическите лица в съвременния свръхтехнологичен и свръхюрисдициран свят.

### В частния и в публичния сектор

Без значение от правно-организационната им форма, всички институции, ведомства, дружества и каквито и да е организации трябва да съобразяват и акуратно да спазват европейските правила относно защитата на личните данни според Регламента, както и вътрешното право в същата област на регулация, което в националния ни контекст се намира в Закона за защита на личните данни (ЗЗЛД).

Добър пример за очаквано стереотипно действие от администратор както в частния,

така и в публичния сектор би бил текстът на Рецитал 85 от Регламента, който е в смисъл, че нарушаването на сигурността на лични данни може, ако не бъде овладяно по подходящ и навременен начин, да доведе до физи-

чески, материални или нематериални вреди за физическите лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица. Поради това, веднага след като установи нарушение на сигурността на личните данни, администраторът следва да уведоми надзорния орган за нарушението на сигурността на личните данни без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, освен ако администраторът не е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Когато таква уведомление не може да бъде подадено в срок от 72 часа, то следва да посочва причините за забавянето и че информацията може да се подаде поетапно без ненужно допълнително забавяне. Тази концепция е закрепена по императивен начин в чл.33, пар.1 от Регламента.

Неспазването на тези правила – които в своя контекст са разумни, систематични и последователни – би трябвало да ангажира съответната отговорност вътре в трудовото или служебното правоотношение. Доколкото обаче

същите са регламентарани в различни нормативни актове от законов порядък, настоящето изложение ще разгледа отделни примери на дисциплинарни простъпки през призмата на законодателството, уреждащо тези *правоотношения в частния и в публичния сектор поотделно*, за по-голяма яснота и прегледност.

### В частния сектор

Разпоредбата на чл.181 от Кодекса на труда (КТ) урежда правния институт на *Правилник за вътрешния трудов ред* (Правилник), който *inter alia* определя задълженията на работниците и служителите и урежда организацията на труда в предприятието съобразно особеностите на неговата дейност. Поне два елемента от композицията на този правен институт могат да бъдат съотнесени към GDPR. Затова те ще бъдат разгледани по-подробно тук.

Правилникът се явява вътрешноорганизационен акт за предприятието и в този контекст е неговото правно значение. От чисто функционална и организационна гледна точка обаче той се разглежда като Правила на *вътрешния трудов ред* и именно такава е наименованието на чл.181 от КТ. Двете форми биха могли да се използват като заместващи се по-нататък в текста, в зависимост от контекста на използването им.

Първият елемент от Правилата на вътрешния трудов ред, касаещ GDPR, са „определените задължения на работниците и служителите“. Например в тях би трябвало да се разпишат конкретни изисквания към който и да е работник или служител от предприятието, който извърши коригиране, изтриване или ограничаване на обработване на всеки получател, на когото *личните данни* са били разкрити, както и информиране на субекта на данните относно тези получатели, ако субектът на данните поиска това. Това пряко произтича от изискването на чл.19 в съответствие с член 16, член 17, параграф 1 и член 18 от Регламента.

Понеже задължението за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването тежи на администратора, всички негови работници, служители и организационни звена в предприятието му би трябвало да действат *системно, безпротиворечиво, еднопосочно и акуратно*. Затова първоначално задълженията трябва да са ясно, точно и императивно разписани

в правилата, а впоследствие спазването им трябва да се следи с всички възможни мерки и средства на трудовото законодателство.

По друг начин казано – Правилата трябва да следват изискванията на GDPR и на националното законодателство по прилагането му, а неспазването им трябва да се санкционира. Това е така, защото едно-единствено неотразяване например неинформиране на субекта на данните относно получателя им, се явява нарушение на администратора на данни (т.е. предприятието като цяло, по друг начин казано – на работодателя, а в нашия контекст – на администратора).

Със сигурност, тези Правила трябва да следват съответните кодекси за поведение по смисъла на чл.40 от Регламента – *национални, гилдийни, корпоративни и други*. Тяхната класификация не е ограничителна по смисъла на доста разтегливата норма на GDPR, която посочва, че държавите членки, надзорните органи, Комитетът и Комисията насърчават изготвянето на кодекси за поведение, които имат за цел да допринесат за правилното прилагане на настоящия регламент, като се отчитат специфичните характеристики на различните обработващи данни сектори и конкретните нужди на микропредприятията, малките и средните предприятия. По-нататък е добавено, че сдруженията и други структури, представляващи категории администратори или обработващи лични данни, могат да изготвят кодекси за поведение или да изменят или допълват такива кодекси с цел да бъде уточнено прилагането на Регламента.

Съответното нарушение тук би трябвало да се търси измежду голямата група *нарушения на трудовата дисциплина* според систематиката на 187 от КТ. Интересното е, че в случая, според фактическата и правна аргументация, във всеки един отделен случай биха могли да се изтъкнат различни правни хипотези.

Едната е по ал.1, т.3, предложение първо от горния законов текст, а именно – неизпълнение на възложената работа, когато изрично е възложено на работник и служител на ситематизира, уведомява или изпраща информация по смисъла на чл.19 от Регламента.

Втората е по предложение второ от същата разпоредба – неспазването на техническите и технологичните правила. Тук, естествено, всичко зависи от спецификата на дейността

та на предприятието. Колкото повече същото оперира с лични данни, толкова по-висок е стандартът на изискванията към събирането, обработването, разкриването им и т.н. В този смисъл, българското трудово право вече би трябвало да е *доразвило визията си относно техническите и технологичните правила през призмата на GDPR*. Те вече са неизменна част от трудовия процес и загърбването им еднозначно означава нарушаване на политиката за защита на личните данни и на действащото законодателство, и двете последни – нарушаване на трудовата дисциплина, доколкото същата винаги трябва да е съобразена с *действащия правов ред*.

Третата хипотеза е по чл.187, ал.1, т.10, предложение първо - изпълнение на други трудови задължения, предвидени в закони, като тук категорично може да се направи привръзка със ЗЗЛД. Такова изпълнение би било нарушението на чл.5, ал.1 от закона, като въпреки забраната е извършено обработване на лични данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели или се отнасят до здравето, сексуалния живот или до човешкия геном, без да са налице изключенията от нормата съобразно алинея втора на същия текст.

Четвъртата хипотеза е по същия текст, но по предложение второ - изпълнение на други трудови задължения, предвидени в други нормативни актове, и това категорично е самият GDPR. Такова изпълнение би било на Длъжностното лице по защита на данните (ДЛЗД), когато същото не да си сътрудничи с надзорния орган, според императивното и категорично изискване на чл.39, пар.1, б.„г“ от Регламента. Няма никакво съмнение, че същият попада в категорията „нормативни актове“, макар и да не е от систематиката на българската национална (вътрешна) правна система, но със сигурност в систематиката на *българския правов ред*. Законната дефиниция на чл.1а от Закона за нормативните актове (ЗНА) дава възможност за тази интерпретация, защото указва, че нормативният акт съдържа общи правила за поведение, които се прилагат към индивидуално неопределен кръг субекти, има нееднократно действие и се издава или приема от компетентен държавен орган. Регламентът напълно отговоря на определе-

нието, с изключение на последната му част: „издава или приема от компетентен държавен орган“. Тук обаче *разширителното тълкуване* е позволено, имайки предвид чл.7а от ЗНА - нормативен акт се издава и в случаите, когато трябва да се приемат мерки на национално ниво, необходими за изпълнение и прилагане на актове на Европейския съюз или на международни договори, сключени от Европейските общности. Такъв национален акт е вече цитираният ЗЗЛД. Но най-силното основание тук е чл.15, ал.2 от ЗНА - ако нормативен акт противоречи на регламент на Европейския съюз, прилага се регламентът. Точно поради тази причина изпълнение на трудови задължения при нарушение на GDPR би трябвало безусловно да ангажира дисциплинарната отговорност на работника и служителя.

Петата хипотеза е по предложение трето на чл.187, ал.1, т.10 - изпълнение на други трудови задължения, предвидени в правилника за вътрешния трудов ред – и тук *премисата (т.е. предпоставката) съвпада с първата и втората хипотеза по-горе, като едновременно се конкурира с тях*.

Шестата хипотеза е по същия текст, предложение последно - изпълнение на други трудови задължения, определени при възникването на трудовото правоотношение, като тук очевидно се касае за ДЛЗД. Това е така, защото ДЛЗД се назначава именно с цел защита на личните данни и това е определено още към момента на възникване на трудовото му правоотношение с работодателя му, който се явява и администратор на тези данни.

Видовете дисциплинарни наказания по КТ са разписани в чл.188 и биват забележка; или предупреждение за уволнение; или уволнение. Законодателят е въвел критерии за определяне и еднократност на дисциплинарното наказание, за да избегне *работодателски дисциплинарен* произвол. В този смисъл, чл. 189 от КТ указва, че при определяне на дисциплинарното наказание се вземат предвид тежестта на нарушението, обстоятелствата, при които е извършено, както и поведението на работника или служителя. Също там, във втората алинея на текста е отразено, че за едно и също нарушение на трудовата дисциплина може да се наложи само едно дисциплинарно наказание.

Обаче, въвн от горното, трябва да се обърне особено внимание, че съобразно чл.186 от КТ виновното изпълнение на трудовите задъл-

жения е нарушение на трудовата дисциплина. Нарушителят се наказва с предвидените в този кодекс дисциплинарни наказания независимо от имуществената, административнонаказателната или наказателната отговорност, ако такава отговорност се предвижда. Разделността на видовете юридически отговорности по смисъла на КТ е важна гаранция за *неотвратимостта на неблагоприятните правни последици за нарушителя на трудовата дисциплина*. По-подробно някои от тези въпроси са разгледани в предишни публикации на списание „Вътрешен одитор“, а именно: „Административните санкции на основания от GDPR“ и „Съдебни претенции на основания от GDPR“.

Вторият елемент от Правилата на вътрешния трудов ред, касаещ GDPR е „уредената организация на труда в предприятието съобразно особеностите на неговата дейност“. Това бе разгледано по-горе подробно във втората хипотеза по чл.187, ал.1, т.3, предложение второ от КТ – неспазването на техническите и технологичните правила. Изрично трябва да се отбележи, че *хомогенността в систематиката на КТ предполага изказ на едни и същи неща от различна гледна точка*. Съответното нарушение тук, както вече бе споменато по-горе, произтича от спецификата на дейността на предприятието. Мениджмънтът на същото би трябвало *постоянно* да извършва мониторинг и анализ на тази дейност и да актуализира по адекватен начин всички новонастъпили аспекти в проявлението ѝ, още повече – когато те касаят каквото и да е проявление на правна регулация в обхвата на GDPR.

Точно това има предвид чл.24, пар.1 от Регламента, който постановява, че като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия регламент. Тези мерки се преразглеждат и при необходимост се актуализират.

Затова, например, ако според уредената организация на труда в съответното предприятие, *разработването и предлагането за въвеждане на подходящите технически мерки* е в задълженията на например Директор на „Ди-

рекция комуникационни технологии“, а пък *разработването и предлагането за въвеждане на подходящите организационни мерки* – на Директор на „Дирекция управление на процесите“, то *неразработването и непредлагането за въвеждане на подобни мерки* би било христоматиен пример за дисциплинарно нарушение на основание от GDPR, съгласно КТ.

*Непреразглеждането и неактуализирането им е дисциплинарно нарушение от същия род*. Тук обаче само трудовоправната практика ще формира ясни и точни критерии относно времевите, калибърните и инструментални аспекти на това преразглеждане и актуализиране.

Някои насоки все пак могат да бъдат дадени още тук – това трябва да се върши в *разумна периодичност* (например – веднъж на всеки три месеца). Ако обаче динамиката на промените е толкова бърза и категорична, това би трябвало да се прави *веднъж месечно*, или дори *незабавно*.

От гледна точка на калибъра на преразглеждането и актуализирането – трябва да се действа точно там, *където има нужда от нов подход и нова ефективност*. По друг начин казано – *обемът е предразположен от разумността, обективността и резултатността на промените*.

При инструменталните аспекти на преразглеждането и актуализирането трябва да се използват всички възможни *трудоваправни* възможности на Правилника за вътрешния трудов ред; други правила, процедури, наръчници, ръководства и инструкции; заповеди на работодателя, който е и администратор на лични данни; а също и *административноправните* тълкувания, становища, разяснения и мнения на Комисията за защита на личните данни (КЗЛД); водещата *съдебна практика* по прилагане на ЗЗЛД и Регламента; както и *добрите практики* по прилагане на GDPR при други администратори на лични данни.

Интерес би представлявало разглеждането на някои от хипотезите при прилагане на най-тежкото наказание по КТ – дисциплинарно уволнение, във връзка с нарушения на GDPR. Например, според чл.190, ал.1, т.3, дисциплинарно уволнение може да се налага за системни нарушения на трудовата дисциплина. Трудовата дисциплина, когато е ясно и точно

разписана в Правилника за вътрешния трудов ред, *би могла и вече би трябвало да съдържа изисквания* за стриктно спазване на GDPR от работниците и служителите на предприятието, които боравят с лични данни. Въпросът е да се изясни какво би представлявало „системното нарушение на трудовата дисциплина във връзка с GDPR“. Отговорът е очакван с нетърпение и той би бил даден от работодателя и от съдебната практика във връзка с тази проблематика.

Дисциплинарно наказание уволнение би могло да се наложи и за *злоупотреба с доверието на работодателя*, по смисъла на чл.190, ал.1, т.4, предложение първо от КТ. Злоупотреба от страна на работник или служител с доверието на работодателя *вече би могло да съществува в нов, съвременен контекст* – неправомерно боравене с *чувствителна информация*, касаеща GDPR. Предоставянето на достъп, дори и частичен, до такава информация, особено при действащия стриктен правен режим, се основава на принципа на *личното доверие*. Неоправдаването на очакванията към това възложено доверие е типичен пример за злоупотреба с доверие. Именно това е нарушение по чл. 126, т.9, предложение първо от КТ, който закрепява правилото, че при изпълнение на работата, за която се е уговорил, работникът или служителят е длъжен да бъде лоялен към работодателя, като не злоупотребява с неговото доверие. В тази насока е и утвърдената съдебна практика (Виж Решение № 2636 от 27.04.2018 г. на СГС по в. гр. д. № 12224/2017 г.: „...за да се приеме, че е налице злоупотреба с доверието на работодателя по смисъла на чл. 190, ал. 1, т. 4 от КТ следва служителят да е извършил такива действия, които компрометират оказаното му доверие, независимо от това дали са извършени умишлено и дали е било налице намерение за извличане на имуществена облага...Злоупотребата с доверието на работодателя е пряко свързана с неизпълнението на вмененото по чл. 126, т. 9 от КТ задължение на служителя“).

Уволнение е възможно и за разпространяване на *поверителни за работодателя сведения*, според систематиката по смисъла на чл.190, ал.1, т.4, предложение второ от КТ, кореспондиращо с правилото на чл.126, т.9, предложение второ от същия кодекс, а именно - при изпълнение на работата, за която се е уговорил, работникът или служителят е длъжен да бъде лоялен към работодателя, като не раз-

пространява поверителни за него сведения. Традиционно, българската правна доктрина и юридическа практика са приемали и приемат, че става въпрос за опазване на *служебната тайна*. Тя най-често е възприемана като *производствена и търговска тайна*. Двете имат *достатъчно общи характеристики*, макар и някои от техните аспекти да могат да бъдат *категорично разграничени*. И двете касаят чувствителна за предприятието информация, която го прави уникално на пазара и спомага за развитието му с цел печалба. Разликата е, че производствената тайна е свързана с процеса на създаване на продукта, а търговската – с процеса на крайната му реализация на пазара. И двете обаче могат да се изразяват в рецепта, стандарт, марка, дизайн, наименование за произход, процедура, практика, формула, подход, способ или производните или комбинативните от и между тях. Издаването на такава информация уязвява предприятието пред конкурентите, и го прави по-малко желано от клиентите на неговите стоки и услуги.

Интересното е, че при по-широко тълкуване, *неопазването на доброто име* на предприятието по смисъла на чл.126, т.9, предложение трето от КТ, би могло да доведе до дисциплинарно уволнение както на основание чл.190, ал.1, т.4, предложение първо от КТ, така и на точка 7 от същия законов текст. Понастоящем *вече част от репутацията на фирмата е съответствието на практиката ѝ с GDPR*. Афиширането на „*Compliance with GDPR*“ е същностна характеристика на нематериалните активи на съвременната организация. Нарушаването на правилата на GDPR от работник или служител като следствие води до неопазването на доброто име на предприятието, което може да доведе до загуба на настоящи или потенциални клиенти. Тази простъпка е толкова сериозна, че изисква най-тежкото дисциплинарно наказание – уволнение. Такъв казус би бил налице например, когато на служебния Интернет-сайт се качат от работник или служител лични данни на негов *съпруг/бивши съпруг*, с цел „уреждане“ на лични отношения. И сегашната съдебна практика е в тази насока, но прибавянето към казуса на елемент от правния обхват на GDPR би бил категоричен пример. Към момента може да се цитира за знание следния съдебен акт: „Не се спори, че въпросните снимки са на ищцата, същите са с компрометиращ характер, както и че са разпространени в публичното пространство.

Именно с факта на тяхното съществуване и наличие в личния компютър на ищцата със създадена възможност за разпространение в публичното пространство е уронено доброто име на работодателя, изразяващо се в нелоялно отношение към него и zlepоставянето му пред трети лица, накърнен е както неговия престиж, така и този на службата, която ищцата представлява, като неморалното ѝ поведение безспорно разколебава доверието в работодателя, а начинът на разпространението им е друг въпрос, който в случая не касае нарушаването на трудовите задължения. Налице е тежко нарушение на трудовите задължения при изпълнение на възложената работа от страна на ищцата, изразяващо се в уронване на престижа и доброто име, както на службата, така и на работодателя - чл. 126, т. 9, предл. последно КТ“ (Из Решение № 379 от 15.07.2010 г. на ВКС по гр. д. № 471/2009 г., III г. о., ГК, докладчик съдията Светла Димитрова).

Категорично „друго тежко нарушение на трудовата дисциплина“ по смисъла на чл.190, ал.1,т.7 от КТ би било налице, когато се установи *несъобщаване на субекта на данните за нарушение на сигурността на личните данни*, съобразно чл.34 от Регламента. Изискванията му са ясни, първо - когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни. Естествено, администраторът не прави това лично, а е възложил тази функция и задача на свой работник или служител, обвързан с нея чрез трудовия договор, Кодекса за поведение и други вътрешноведомствени правила и процедури. Второ, в съобщението до субекта на данните, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията и предприетите по случая мерки. Съставянето на съобщението е възложено по длъжностна характеристика на съответния работник или служител; посочването на информацията също касае или него, или негов колега; предприемането на определени мерки касае едно или няколко организационни звена в предприятието. При всички случаи, отговорните работници и служители са видни от техните длъжностни характеристики, от Правилника за вътрешния трудов ред

или от Кодекса за поведение. Винаги обаче, когато е налице вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, и тази вероятност *не се отработи съобразно изискванията на чл.34 от Регламента*, това е тежко дисциплинарно нарушение и същото би трябвало да се санкционира с уволнение за виновния работник или служител.

Налице са някои процесуални задължения на работодателя преди налагане на дисциплинарното наказание, съобразно чл.193 от КТ. Там е указано, че работодателят е длъжен преди налагане на дисциплинарното наказание да изслуша работника или служителя или да приеме писмените му обяснения и да събере и оцени посочените доказателства. Това е с *оглед на установяване на самото нарушение, на нарушителя и на неговата вина*. При достъпа на един работник и служител в предприятието до лични данни, с които борави то, въпросът с доказването понякога е от ключово значение. Въпреки това, трябва да се помни, че когато работодателят предварително не е изслушал работника или служителя или не е приел писмените му обяснения, съдът отменя дисциплинарното наказание, без да разглежда спора по същество. Това означава, че на формално правно основание, дисциплинарното наказание ще бъде анулирано напълно.

Във връзка с особения характер на защитената от GDPR информация, трябва да се има предвид, че са налице изключително кратки срокове по чл. 194, ал.1 от КТ - дисциплинарните наказания се налагат не по-късно от 2 месеца от откриване на нарушението и не по-късно от 1 година от извършването му. По друг начин казано, възможно е нерегламентираното боравене с лични данни да е било открито преди два месеца и един ден, *но едва днес е открит конкретният нарушител, който го е извършил виновно*. При тази хипотеза, поради изтичането на двумесечния срок, наказание не може да бъде наложено. Тук съдебната практика е пределно ясна, безпротиворечива и последователна, а именно: „Заповедта, с която се налага дисциплинарно наказание, следва да бъде ясно мотивирана и по начин, че да са ясни съществените признаци на деянието от обективната страна, времето и мястото на извършването му...Когато дисциплинарното нарушение е осъществявано в рамките на определен период, а спецификата на изпълняваната работа или характера на самото нарушение

ние не позволява откриване на точния ден и час на извършването му, а контролирането им е възможно само като краен резултат, изискванията на чл. 195, ал. 1 КТ са изпълнени с посочване на периода на извършването му. Когато нарушението, изразяващо се в бездействие - неизпълнение на възложени трудови функции, е продължавало за определен период, вкл. и до откриването му, изискванията на чл. 194, ал. 1 КТ и чл. 195, ал. 1 КТ са изпълнени с посочване на момента на откриването му, тъй като извършването на нарушението и момента на откриването му съвпадат...Без значение е дали в заповедта е посочена разпоредба от КТ, която е нарушена, съответно позоваването точно ли е, правилно ли е квалифицирал (терминологично) работодателят вида нарушение. Същественото за мотивирането на заповедта, както стана ясно, е индивидуализацията на самото деяние (действие или бездействие) чрез неговите обективни и субективни признаци“ (Из Решение № 78 от 11.04.2018 г. на ВКС по гр. д. № 1835/2017 г., IV г. о., ГК, докладчик съдията Албена Бонева).

Общите формални изисквания относно акта, с който би се наложило дисциплинарно наказание за нарушения на GDPR, ще следват действащата нормативна среда, трудова и

съдебна практика. Според чл.195, ал.1 от КТ дисциплинарното наказание се налага с мотивирана писмена заповед, в която се посочват нарушителят, нарушението и кога е извършено, наказанието и законният текст, въз основа на който то се налага. Тук от особена важност е да се опишат *конкретните действия и бездействия, които влизат в противоречие с изискванията на GDPR*. Съществено е да се акцентира и на времето на извършването, както е посочено по-горе в разгледаната съдебна практика. За разлика от наказателния и от административнонаказателния процес, където по-скоро се очаква *точно фиксиране на дати*, тук е възможно да се посочи и период в неговите граници. Това е така, защото трудовото правоотношение е непрекъснато *между двете страни, докато съществува*. Тоест, правата и особено задълженията са перманентни. Тази характеристика е една от отличителните свойства на трудовото правоотношение, правейки го коренно различно от правоотношението по престъпното деяние и по административното нарушение, *които по същността си са единични и инцидентни*.

д-р Младен Младенов

*Следва продължение в брой 4/2018*

