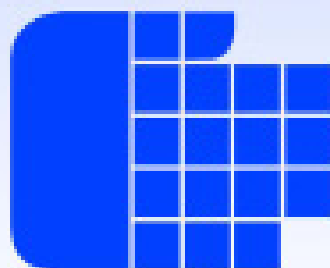


Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 5 (116), септември 2025 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода юли и август 2025 г.)

СЪБИТИЯ И ИНИЦИАТВИ.....	3
Успешно завърши обучение по чл. 10, (2), т. 6 от ЗЗЛД.....	3
Студенти по „Право“ осъществиха учебен стаж в КЗЛД	4
Среща на високо равнище в Хелзинки.....	4
Грузия - домакин на 75-ата среща на Берлинската работна група.....	5
КЗЛД прие Насоки относно използването на видеорегистратори.....	6
КЗЛД прие Препоръки за правомерно предоставяне на достъп до видеозаписи от система за видеонаблюдение на училища или детски градини.....	9
Продължава изпълнението на проект OPWHI.....	12
КОНТРОЛНА ДЕЙНОСТ.....	14

СЪБИТИЯ И ИНИЦИАТИВИ

УСПЕШНО ЗАВЪРШИ ОБУЧЕНИЕ ПО ЧЛ. 10, (2), Т. 6 ОТ ЗЗЛД



На 22 юли 2025 г. успешно приключи обучението на първата група служители, касаещо чл. 10, (2), т. 6 от Закона за защита на личните данни (ЗЗЛД). На официална церемония сертификатите на успешно завършили участници бяха връчени лично от председателя на Комисията

за защита на личните данни (КЗЛД) г-н Борислав Божинов.

Обучението бе реализирано в изпълнение на решение на КЗЛД относно структурата и съдържанието на обучителния процес, предвиден в чл. 10, ал. 2, т. 6 от ЗЗЛД. Разработено и внедрено в електронен формат, то е насочено към ръководители и служители на експертни длъжности от централната, териториалната и местната администрация, които отговарят за обработването на лични данни, включително длъжностните лица по защита на данните в институциите.

Обучението е съобразено с актуалните нормативни и практически изисквания в областта на защитата на личните данни, включително Общия регламент относно защитата на данните (GDPR), и се провежда съвместно с Института по публична администрация (ИПА).

Обучителното съдържание включва единадесет теми, като всяка тема се състои от видео лекция, презентация, материали за четене по одобреното от КЗЛД съдържание и въпроси за самооценка. Обучението съдържа и материали за самостоятелна подготовка.

То се провежда в два последователни етапа – електронно самообучение чрез платформата на Института по публична администрация и едnodневно присъствено обучение в сградата на Института. Съдържанието обхваща ключови теми като основните принципи на защита на личните данни, правата на субектите на данни, задълженията на администраторите и обработващите данни, както и ролята на длъжностното лице по защита на данните.

За успешното преминаване на курса, всеки курсист трябва да предостави решени пет задачи, както и да реши въпросите за самооценка към всяка тема с резултат над 70% верни отговори. Електронната платформа позволява динамично управление на съдържанието и резултатите от обучението, като достъп до нея се предоставя след заявка от страна на съответната администрация.

След завършване на обучението участниците придобиват знания и практически умения за прилагане на нормативната уредба в областта на защитата на личните данни, организиране на вътрешните процеси по обработване на данни, разработване на вътрешни политики, оценки на въздействие и риск, както и за използване на добри практики в сферата на защита на личните данни.

СТУДЕНТИ ПО „ПРАВО“ ОСЪЩЕСТВИХА УЧЕБЕН СТАЖ В КЗЛД



В периода 21 – 25 юли 2025 г. първата група от определените студенти от втори курс, специалност „Право“ в Софийския университет „Св. Климент Охридски“ проведеха студентски стаж в Комисията за защита на личните данни. В началото на стажа на студентите им беше представена организационната структура на КЗЛД, както и дейността на Европейския надзорен орган по защита на данните и Европейския комитет по защита на данните. Запознаха се с нормативната уредба за защита на личните данни. На студентите им бе демонстрирана

вътрешната система за разпределение, изпълнение, контрол и отчет на преписки на КЗЛД. Беше им представена и системата за подготовка на документи на ЕКЗД. Стажантите участваха и в преглед на проекти с европейско финансиране.

Студентите взеха участие в присъствения етап на обучението по чл. 10 (2) т. 6 от ЗЗЛД в Института по публична администрация. Като част от дейностите на стажа студентите работиха по индивидуални запитвания на надзорни органи от други европейски държави по механизмите за сътрудничество и съгласуваност съгласно Регламент (ЕС) 2016/679. Студентите присъстваха на заседание на КЗЛД. След приключване на стажа студентите бяха поздравени лично от председателя на КЗЛД г-н Борислав Божинов.

СРЕЩА НА ВИСОКО РАВНИЩЕ В ХЕЛЗИНКИ

В периода 1-2 юли във финландската столица Хелзинки се проведе среща на високо равнище на Европейският комитет по защита на данните (ЕКЗД). В рамките на форума членовете на Комитета приеха „Изявлението от Хелзинки относно по-голяма яснота, подкрепа и ангажираност: Подход, основан на основните права, към иновациите и конкурентоспособността“. Документът отбелязва важна стъпка към улесняване на спазването на Общия регламент относно защитата на данните (ОРЗД), особено от страна на микро, малките и средни предприятия, и поставя фокус върху отговорните иновации и засилването на съгласуваността и ефективността на регулаторните действия на европейско равнище.

Изявлението подчертава значението на защитата на личните данни като основна европейска ценност и акцентира върху необходимостта от ориентиран към човека подход при използването на лични данни. В тази връзка, членовете на ЕКЗД се ангажираха с нови инициативи за засилване на диалога със заинтересованите страни, за предоставяне на навременни, ясни и практически приложими насоки и за развитие на междурегулаторното сътрудничество в условията на динамична цифрова среда.

С цел облекчаване на административната тежест за организациите и улесняване на прилагането на изискванията на ОРЗД, ЕКЗД ще разработи нови инструменти, включително стандартни образци, контролни списъци, насоки тип „how-tos“ и често задавани въпроси. Комитетът ще изготви и общ образец за уведомленията за нарушения на сигурността на данните, като част от усилията за по-ефективно и хармонизирано управление на инциденти и в подкрепа на евентуално бъдещо общоевропейско решение за уведомяване.

В рамките на срещата беше договорено и надграждане на вътрешните работни процеси на ЕКЗД. Промените включват въвеждане на нови стандарти за планиране и подготовка на насоки, осигуряване

на по-ранна консултация със заинтересованите страни, формализиране на процеса по съгласуване на съдържанието и подобряване на механизмите за контрол на качеството и изпълнението на приетите документи. Наред с това, беше подчертана необходимостта от редовно актуализиране на насоките в светлината на натрупаната практика и обратна връзка.

ЕКЗД поставя особен акцент върху съгласуваността в прилагането на регламента от страна на националните надзорни органи, включително чрез събиране и анализ на национални становища, съдебна практика и добри практики. Продължаващото развитие на общи подходи към правоприлагането и сътрудничеството с други регулатори остава основен приоритет, включително чрез изготвяне на съвместни насоки и участие в общи форуми.

ГРУЗИЯ - ДОМАКИН НА 75-АТА СРЕЩА НА БЕРЛИНСКАТА РАБОТНА ГРУПА



На 2 и 3 юли 2025 г. в Тбилиси, Грузия се проведе 75-ата среща на Международната работна група по защита на данните в областта на технологиите, известна още като „Берлинската работна група“ (IWGDPT). Домакин на събитието беше Службата за защита на личните данни на Грузия, а срещата се състоя в Държавния университет „Иване Джавахишвили“. Форумът беше открит с приветствено слово от ръководителя на Службата – г-жа Лела Джанашвили, която акцентира върху предизвикателствата и актуалните тенденции в сферата на защитата на личните данни и неприкосновеността на личния живот в контекста на технологичния напредък. Председателят на

Берлинската група проф. Йенс Бендер, ръководител на Отдела за техническа защита на данните към Германската надзорна служба, също поздрави участниците и подчерта важността на международния диалог в областта.

В срещата взеха участие 25 представители от 14 държави, както и представители на Европейския надзорен орган по защита на данните (ЕКЗД) и Центъра за информация за електронна неприкосновеност (ЦИЕН). От страна на Комисията за защита на личните данни участие взе г-н Цветелин Софрониев, член на КЗЛД. Обсъдени бяха съвременните предизвикателства и иновации в сферата на защитата на личните данни, включително използването на невроданни, развитието на 6G технологии, цифровата идентичност и други аспекти, свързани с влиянието на технологиите върху личната неприкосновеност. В рамките на форума г-н Николоз Попиашвили – ръководител на кабинета на началника на Службата за защита на личните данни, и г-н Димитри Гугунава – ръководител на отдел „Стратегическо планиране и анализ на цифровото управление и киберсигурността“ към LEPL – Агенция за цифрово управление, представиха пред участниците актуални въпроси, свързани със защитата на личните данни в процеса на предоставяне на електронни държавни услуги чрез портала MY.GOV.GE.

По време на срещата представители на надзорните органи от различни държави изнесоха специализирани доклади за иновативни решения и практики в областта на защитата на личните данни. Участниците в „Берлинската работна група“ обмениха опит и виждания относно предизвикателствата, произтичащи от технологичния напредък. Събитието беше обобщено от първия заместник-ръководител на Службата – Отар Чахунашвили, който подчерта значението на срещата и обяви, че следващият брой на научното списание на институцията ще бъде посветен на темите и изводите от форума.

Международната работна група по защита на данните в областта на технологиите, наричана още „Берлинска група“, е създадена през 1983 г. с цел да разработва препоръки и насоки за повишаване

на стандартите за защита на личните данни в технологичната сфера. В нея участват надзорни органи, международни организации, публични институции и индивидуални експерти от цял свят. От 21 март 2016 г. грузинският надзорен орган за защита на данните е пълноправен член на Берлинската група и ежегодно участва в срещите, посветени на добрите практики и иновативни подходи при справяне с технологични предизвикателства.

КЗЛД ПРИЕ НАСОКИ ОТНОСНО ИЗПОЛЗВАНЕТО НА ВИДЕОРЕГИСТРАТОРИ

Насоки относно използването на видеорегистратори в частни превозни средства

Въведение

През последните години използването на технически средства за запис, монтирани в автомобил (т.нар. видеорегистратори), се увеличава прогресивно, тъй като устройствата стават по-достъпни и предлагат по-високо качеството на запис, вкл. и повече функционалности (като напр. за активиране на записването при посегателство върху паркирано превозно средство).

Обичайно видеорегистраторите са насочени по посока на движението и могат да записват образни и/или звукови данни за пътя отпред и/или за пътниците в превозното средство. Регулациите в отделните държавите-членки на Европейския съюз се различават значително и към момента няма единни правила, които да уреждат тяхното използване от граждани (частни лица). Някои държави имат строги забрани (напр. Португалия, Австрия, Люксембург и Швейцария), докато други позволяват използването им при определени условия.

В България използването им за момента се урежда от общите нормативни изисквания за защита на личните данни. От експлоатацията на такива записващи устройства могат да възникнат усложняващи последици за правата за защитата на неприкосновеността на личния живот и личните данни на другите участници в движението. Поради това е важно шофьорите, които инсталират видеорегистратори, да са запознати и да разбират потенциалните си задължения, които могат да произтекат от законодателството за защита на личните данни.

Правен статут на ползвателя на видеорегистратор

По общо правило задълженията за защита на данните се прилагат за тези, които събират или обработват по друг начин лична информация на физически лица (включително изображения и гласови записи). В ежедневието си обаче физическите лица могат да обработват лична информация в много различни ситуации, които са от чисто личен или битов характер. Този вид обработка на лична информация не се обхваща от задълженията за защита на данните, поради т.нар. изключение за „чисто лични или домашни занимания“.

В своята практика Съдът на ЕС посочва, че то трябва да се тълкува ограничително. В решението по дело C-212/13 Rynéš срещу Úřad от 2014 г. (касаещо спор относно използването на неподвижно закрепена камера за видеонаблюдение, която е обхващала както частно жилище, така и обществена улица), Съдът на ЕС отбелязва, че:

„Доколкото видеонаблюдение [...] покрива, макар и частично, публични места и поради това е насочено извън личната сфера на лицето, което извършва по този начин обработване на данни, то

не може да се счита за дейност, която е изцяло „лична или домашна“ по смисъла на член 3, параграф 2, второ тире от Директива 95/46.“

Въпреки че случаят е свързан със стационарна система за видеонаблюдение, той има принципи последици за всички ползватели на технология за видеонаблюдение, която записва видео и/или аудио на обществени места. Ползвателите на видеорегистратори следва да обмислят естеството и обхвата на всеки запис, който извършват, и дали той попада в обхвата на изключението за „чисто лични или домашни занимания“ или записването може да попадне под нормативните правила за защита на личните данни.

Когато видеорегистратор се използва в професионален, търговски и най-общо казано, неличен контекст, напр. от професионални шофьори, такситата, компании за доставка и др., изключението няма да се прилага и ползвателите на видеорегистратора (вкл. потенциални шофьори и/или работодатели или всеки, участващ в решението за използване на видеорегистратора) ще трябва да вземат предвид задълженията си за защита на данните.

Така напр. записването на звук вътре в превозното средство изисква много сериозна обосновка за неговата пропорционалност и необходимост, поради потенциално високия риск за запис на лични разговори на пътниците. Това разбиране е установено и в практиката на Европейския съд по правата на човека (*López Ribalda and Others v. Spain*), като подобна дейност по наблюдение и запис не следва е допустима, освен по изключение, при наличието на важни легитимни цели и при въведени подходящи гаранции за правата и свободите на засегнатите лица.

Задължения на администратора

Когато се обработват лични данни и не е приложимо изключението за „чисто лични или домашни занимания“, лицето, отговорно за записването с видеорегистратор, следва да се счита за „администратор“. Администратор е лицето, компанията или друга организация, която решава „защо“ и „как“ ще се събират и обработват по друг начин лични данни.

Когато записването с видеорегистратор се осъществява в професионален и търговски контекст или на обществено място, ползвателят следва да се приеме за администратор на лични данни. Следователно той ще е задължен да спазва законодателството за защита на данните и да ги обработва в съответствие с принципите за тяхната защита.

В тези случаи администраторите на видеорегистратори ще трябва да съблюдават следните ключовите аспекти:

Личните данни трябва да се обработват по прозрачен начин

Използването на видеорегистратор поставя някои предизвикателства по отношение на прозрачността, тъй като администраторът трябва да е в състояние да предоставя определена информация на всеки, чиито данни се събират.

☐ Така например върху и/или вътре в превозното средство трябва да има ясно видим знак, стикер или друга индикация, според случая, която да показва, че се извършва запис;

☐ Трябва да се предостави политика/уведомление, в което се описват данните за контакт, правното основание за събиране на образни и/или звукови данни на други лица, целите, за които се използват данните, и за какъв период от време ще се съхраняват;

☐ При поискване тази информация следва да може да бъде предоставена в писмена, в т.ч. електронна или устна форма, включително чрез политика/уведомление, достъпно онлайн, след като лицата, чиито лични данни се обработват, са уведомени за начина на достъп до нея;

☐ В случай на произшествие е препоръчително да се уведомят засегнатите лица, че сте записали кадри от инцидента, с цел прозрачност и осигуряване възможност на дадено лице да подаде

заявление за упражняване на правото си на достъп;

☐ Повече информация за задължението за прозрачност може да бъде намерена на интернет страницата ни <https://cpdp.bg/> и в чл. 12, 13 и/или 14 от [Регламент \(ЕС\) 2016/679 \(Общ регламент относно защитата на данните\)](#).

Личните данни трябва да се съхраняват само толкова дълго, колкото е необходимо за постигането на целта, за която са били събрани

Администраторите трябва да обмислят колко дълго е необходимо да съхраняват записите, вкл. техни копия.

☐ Записите на произшествие може да са необходими за административни или съдебни производства и поради това могат да бъдат съхранени допълнително за тази цел;

☐ Като част от гореспоменатите задължения за прозрачност, лицата следва да могат да се информират за това колко дълго ще се съхраняват записите;

☐ Записите не трябва да се съхраняват за неопределено време и следва периодично да се изтриват, след като вече не са необходими за целта, за която първоначално са били събрани, или за каквато и да е легитимна последваща цел;

☐ Повече информация за принципите за „ограничение на съхранението“ и „ограничение на целите“ може да бъде намерена в [насоките за бизнеса](#).

Личните данни трябва да се пазят сигурно

Администраторите трябва да са наясно къде се съхраняват записите (напр. на собствена памет или в „облачно“ пространство) и да контролират и ограничават достъпа до тях.

Хората имат право на достъп до данните си

Ако администраторът разполага със запис на някого, последният има право на достъп до тези данни.

☐ Правото на достъп включва правото на физическото лице да получи потвърждение дали личните му данни се съхраняват или обработват по друг начин;

☐ Правото на достъп включва и право на лицето да получи копие от личните му данни, които са в процес на обработване, както и допълнителна информация относно обработката на тези данни съобразно чл. 15 от [Регламент \(ЕС\) 2016/679 \(Общ регламент относно защитата на данните\)](#);

☐ При поискване на копие от личните данни администраторът следва да може да отговори в рамките на един месец, дори същите вече да са изтрити;

☐ Повече информация за правото на достъп до лични данни може да бъде намерена в информационната ни брошура Нови моменти относно правата на физическите лица съгласно Регламент (ЕС) 2016/679 и в Насоки 01/2022 г. на Европейския комитет по защита на данните относно правата на субектите на данни – право на достъп.

Публикуване на записи

Тези, които използват видеорегистратор на обществено място, трябва да са наясно, че публикуването на заснет материал, напр. в социалните мрежи, представлява допълнителна операция по обработване, която може да породи риск от нарушаване на правата за защита на данните на заснетите лица. Като цяло и в съответствие с мотивите на Съда на ЕС по делата Lindqvist (C-101/01) и Buivids (C-345/17), публикуването на лични данни пред неограничен кръг от лица, напр. в публичен канал или профил в социалните мрежи, не може да се счита за дейност, подаваща в обхвата на изключението за „чисто лични или домашни занимания“.

За всяко използване на записи, включващи лични данни, чието обработване не попада в обхвата на изключението, администраторът следва предварително да се увери, че има валидно правно основание за това и че въпросното обработване ще отговаря на принципите за защита на данните.

Публикуването на записи от видеорегистратори може да бъде оправдано при определени обстоятелства за журналистически цели, но това трябва да бъде внимателно балансирано с правата за

защита на данните на засегнатите лица.

Предоставяне на записи от видеорегистратор на трети страни

След надлежно писмено искане по съответния процесуален ред полицейските органи, както и органите на съдебната власт могат да поискат от Вас копие на запис от видеорегистратора във връзка с разследване на престъпление. Упражнявайки своите разследващи правомощия, тези органи са длъжни да обработват личните данни при условията и по реда на Глава VIII от Закона за защита на личните данни - Правила за защита 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, включително предпазването от заплахи за обществеността и сигурност и тяхното предотвратяване (загл. изм. - ДВ, бр. 17 от 2019 г.).

В случай на разкриване на записи от видеорегистратор на други трети страни, несвързани с наказателно разследване, следва да се отчита решението на Съда на ЕС по делото Rīgas (C-13/16). То се отнася до искане за разкриване на лични данни на лице, причинило пътнотранспортно произшествие, с цел упражняване на правни претенции. По това дело Съдът на ЕС прави заключение, че администраторът не е имал задължение да удовлетвори искането за разкриване на записа въз основа на законни интереси на третата страна.

Съдът на ЕС разяснява, че ако съществува национален закон, който позволява подобно разкриване на лични данни, съдържащи се в записи от видеорегистратор, на трета страна за предявяване на иск за гражданска отговорност, това би било допустимо.

Ролята на КЗЛД

КЗЛД разглежда жалби на лица, които смятат, че правата им за защита на данните са били нарушени. Когато установи нарушения на законодателството за защита на личните данни, тя може да упражнява корективни правомощия, включително да налага административните наказания „глоба“ или „имуществена санкция“.

КЗЛД ПРИЕ ПРЕПОРЪКИ ЗА ПРАВОМЕРНО ПРЕДОСТАВЯНЕ НА ДОСТЪП ДО ВИДЕОЗАПИСИ ОТ СИСТЕМА ЗА ВИДЕОНАБЛЮДЕНИЕ НА УЧИЛИЩА ИЛИ ДЕТСКИ ГРАДИНИ

Доста често при възникнал инцидент или конфликтна ситуация в училище или детска градина родителите на деца, участващи по някакъв начин в тях и заснети от системата за видеонаблюдение, поставят под съмнение обстоятелствата и причините за тях, респ. касателството на техните деца. За да се уверят обичайно отправят искания за получаване на достъп до съответните видеозаписи. Предоставянето на достъп до видеозаписи обаче може да породи някои усложнения, произтичащи от законодателството за защита на личните данни.

Въпреки че по силата на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) училищата и детските градини определят длъжностни лица по защита на данните, които да ги съветват и подпомагат по въпросите за защита на личните данни, се наблюдава, че повечето от тях срещат затруднения с решаването на такива казуси. Тези затруднения обикновено са свързани с невъзможност на училищата/детските градини (основно поради технологични и ресурсни причини) да прилагат специални технически мерки за защита чрез заличаване (замъгляване, маскиране) на образите на третите лица, попадащи в обхвата на видеозаснемането.

Поради високата обществена значимост на тези отношения и отчитайки задачата на надзорните органи да обръщат специално внимание на дейностите, насочени към деца, КЗЛД намира за необходимо да разясни условията за осигуряване на правомерен достъп в такива случаи.

В този смисъл, когато в училище или детска градина постъпи искане от родител на ученик/дете за достъп до запис от системата им за видеонаблюдение, следва да се отчитат следните препоръки:

По смисъла на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) правото на достъп на субекта на данни (физическо лице) включва три компонента:

- ☐ потвърждение дали се обработват лични данни, свързани с него;
- ☐ получаване на информация за основните характеристики на обработването, като напр. целта, за която се извършва, описание на категориите данни и получателите на тези данни, продължителност на обработването (срокове за съхранение), права на субекта на данните по ОРЗД и др.; и
- ☐ достъп до обработваните лични данни.

Правото на достъп следва да се разбира както като правна възможност за физическото лице да поиска информация от администратора дали се обработват лични данни, свързани с него, така за достъп до тези данни. Именно чрез достъпа лицето има възможност да провери законосъобразността на тяхното обработване.

Като законни представители на своите деца родителите упражняват правата за защита на личните им данни от тяхно име.

Съгласно чл. 15, пар. 3, изречение първо от ОРЗД при реализирането на правото на достъп до лични данни администраторът (училище или детска градина) трябва да предостави копие от личните данни, които са в процес на обработване. Следователно копие се отнася само до третия компонент от правото на достъп („достъп до обработваните лични данни“). Задължението за предоставяне на копие от данните не следва да се разбира като допълнително право на субекта на данните, а като способ за предоставяне на достъп до тях. С него се цели укрепване на правото на достъп, тъй като то включва пълна информация за всички обработвани данни и не може да се разбира като предоставяне единствено на обобщение на данните.

Правото на получаване на копие от личните данни обаче не следва да води до неблагоприятно засягане на правата и свободите на други лица (чл. 15, пар. 4 от ОРЗД). Предвид обстоятелството, че при извършването на видеонаблюдение е възможно да бъдат заснети произволен брой лица, различни от засегнатото (чийто родител иска достъп), достъпът до такъв видеозапис ще бъде свързан с допълнително обработване на лични данни и на тези други субекти на данни. В този случай предоставянето на копие от записа, без да са скрити образите на другите заснети лица, може да засегне неблагоприятно техните права и свободи (напр. последващото му публикуване в социални мрежи, медии, споделянето му между трети лица и пр.).

За да не допусне този резултат, администраторът на данните следва предварително да отчита, че предоставянето на копие от видеозаписа може да доведе до значителна намеса в правата на другите лица. Защитата на правата на трети лица обаче не следва да се използва като претекст за възпрепятстване на легитимни искания за достъп, като в такива случаи администраторът трябва да предприеме технически мерки за удовлетворяване на исканията за достъп (напр. посредством редактиране на изображенията като покриване или замъгляване на образите на третите лица). Администраторите не са длъжни да

прилагат такива технически мерки, ако могат да осигурят по друг начин изпълнението на искането за достъп до личните данни по чл. 15 от ОРЗД.

Отчитайки наличните технологии и познания, както и свързаните с тях разходи за прилагане, в случай че училищата/детските градини не могат да прилагат подходящи мерки за защита чрез заличаване (замъгляване) на образите на другите ученици/деца или други трети лица, попадащи в обхвата на заснетия видеозапис, са препоръчителни следните варианти за законосъобразно осигуряване на достъп на родителя до въпросния запис:

1. Да се поиска и получи изрично писмено съгласие от родителите на всички останали ученици/деца и/или други засегнати субекти, заснети и идентифицируеми от записа, вследствие на което да се предостави копие от видеозаписа на родителя-заявител. Тази хипотеза обаче е трудно изпълнима на практика;

или

2. Да се предоставят стопкадри (screenshots), на които се вижда образът само на неговото дете, а образите на третите лица са заличени;

или

3. Да се осигури достъп чрез преглед на място на видеозаписа, само при условие че родителите на всички останали ученици/деца и/или други засегнати субекти (директор, учители или друг педагогически или непедагогически персонал), заснети и идентифицируеми в записа, са поканени и присъстват едновременно при прегледа. В тази хипотеза всички засегнати субекти следва да подпишат декларация, че се съгласяват да се извърши преглед на записа (на конкретна дата и в присъствието на всички засегнати субекти) и че няма да разгласяват узнатата информация. При прегледа не е допустимо да се извършва презапис с лични или други устройства, поради което училището/детската градина следва да предприеме мерки в тази насока.

С цел отчетност и проследимост училището или детската градина следва да изготви протокол, който да удостоверява прегледа на записа от всички заинтересовани страни. Този вариант за осигуряване на достъп до видеозапис в най-голяма степен би задоволил очакванията на родителя, тъй като чрез него може да придобие пълна и реална представа за обстоятелствата около инцидента/конфликтната ситуация.

Независимо от примерите в настоящите препоръки, когато разследващ или съдебен орган поиска предоставянето на копие от видеозапис училището или детската градина ще са длъжни да го предоставят в цялост (без заличаване), при условие че е изискан писмено по съответния процесуален ред.

Посочените в настоящия документ примери и съвети не ограничават КЗЛД да разгледа всяка жалба или сигнал, свързани с предмета му, отчитайки спецификата и контекста на всеки конкретен случай, както и да заема различна позиция от изложените препоръки.

ПРОДЪЛЖАВА ИЗПЪЛНЕНИЕТО НА ПРОЕКТ ОРВНН



Съвместно с Асоциацията „Прозрачност без граници“ на Испания (координатор), Центъра за изследване на демокрацията, Асоциацията LiBERA, надзорният орган за борба с корупцията на Италия, университетът в Пиза и службата за борба с измамите в Каталуния, Комисията за защита на личните данни участва в проектно предложение със заглавие „OPWNI – Open the whistle: Protecting whistleblowers through transparency, cooperation and open government strategies“ по програма „Граждани, равенство, права и ценности“ на ЕК, с номер на договор – с № 101140801 – OPWNI – CERV-2023-CHAR-LITI.

Проектното предложение е одобрено и предложено за финансиране от Европейската комисия в началото на 2024 г., като същинските дейности по изпълнението му започват от началото на март 2024 г.

Проектът OPWNI се основава на подход на сътрудничество между организациите на гражданското общество, академичните среди и компетентните органи в три държави (Испания, Италия и България), които споделят редица важни предизвикателства пред защитата на лицата, подаващи сигнали за нередности. В проекта е заложено да се насърчи култура на защитено подаване от страна на сигнализиращите на нередности и да се създаде среда за защитено докладване и информиране за нарушения на правото на ЕС и други нарушения чрез набор от иновативни инструменти, обучение и практически механизми за осигуряване на прозрачност.

В резултат на реализираните дейности по проекта на 23 юни 2025 г., на Световният ден за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (World Whistleblowers' Day), беше публикувано Практическо ръководство за подаване на сигнали, което обхваща 5 ключови за областта въпроси:

- Прозрачност и комуникация
- Управление на вътрешните разследвания
- Защита на личните данни
- Подкрепа и защита на подаващите сигнали
- Измерване и оценка на въздействието

С Ръководството се дава начало на международната кампания по проекта, с която се цели да се променят възприятията за подаването на сигнали. Кампанията се реализира едновременно в България, Италия и Испания. В сътрудничество между институции и граждански организации от тези три държави се създава по-сигурна среда за лицата, които подават или биха подали сигнал за нередност, както и се подобрява системата за защита. Кампанията, която стартира на 23 юни, Световен ден на лицата, които подават сигнали за нередности, ще продължи координирано до декември 2025 г. във всяка от тези три държави.

Изработено от експерти от гражданския сектор, държавните органи, отговарящи за защитата на подаването на сигнали, и университети от България, Италия и Испания, това ръководство предлага решения на актуалните предизвикателства, вдъхновяващи примери, конкретни препоръки и практики с фокус върху откритото управление и равенството между половете.

Целта на това ръководство е да засили защитата на лицата, подаващи сигнали, и да съдейства за изграждането на култура, в която подаването на сигнали не е риск, а споделена отговорност.

Изтеглете сега <https://www.openthewhistle.eu/bg/home-bg/>

С оглед на заложените в проект ОРВНІ цели през втората половина на 2025 г. ще се проведе серия от присъствени и дистанционни обучения обхващащи публичният и частният сектор, както и НПО организациите в България. Обученията ще разгледат предизвикателства и нужди в България след транспонирането на Директива (ЕС) 2019/1937.

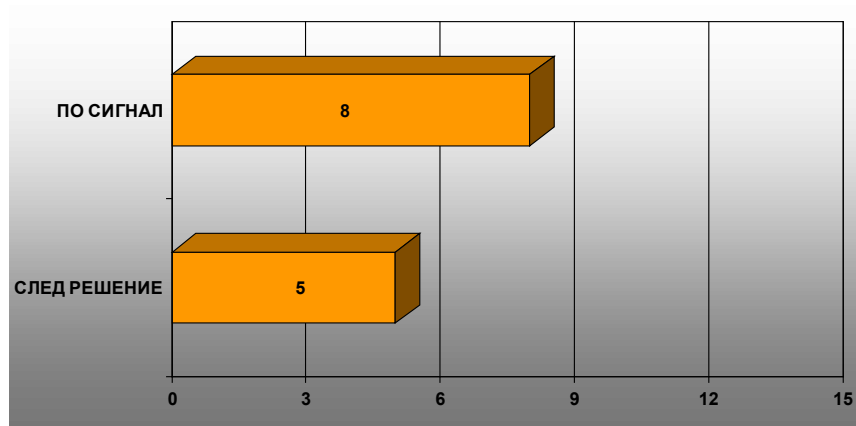


**Съфинансирано от
Европейския съюз**

КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА ЮЛИ-АВГУСТ 2025 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета за м. юли и август 2025 г. са извършени общо 13 бр. проверки – 8 бр. след постъпили в КЗЛД сигнали и 5 бр. след решение на КЗЛД.



Разгледани са 219 бр. искания, включително различни запитвания по актуални въпроси, относно защита на физическите лица във връзка с обработването на лични данни. На всички податели са изпратени съответни отговори, 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 2 бр. Разпореждания, отправени са 4 бр. Предупреждения, 3 бр. Официални предупреждения, издадени са 4 бр. Наказателни постановления, а с решение на КЗЛД са наложени 3 бр. Административни наказания (2 бр. глоби и 1 бр. имуществена санкция).



Комисия за защита на личните данни

Председател: Борислав Божинов

Членове: Василка Рангелова

Ивайло Станев

Цветана Червелякова- Илиева

Цветелин Софрониев

Информационен бюлетин № 5 (116) 2025 г.

Издава се съгласно чл. 10, ал. 3 от ЗЗЛД

Уеб сайт на КЗЛД: www.cpdp.bg

Разпространява се в електронен вид