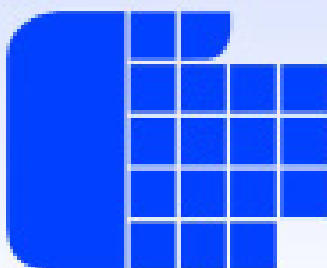


Комисия за Защита на Личните Данни

**ИНФОРМАЦИОНЕН
БЮЛЕТИН**



Брой 1 (118), януари 2026 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода ноември и декември 2025 г.)

СЪБИТИЯ И ИНИЦИАТИВИ.....	3
Изменение на Правилника за дейността на КЗЛД и нейната администрация.....	3
Приета е нова стратегия на КЗЛД- Хоризонт 2030.....	4
КЗЛД отбеляза 28 януари- Ден за защита на данните.....	4
ЕКЗД проведе второ заседание с органите за защита на данните на държавите с решение за адекватност	5
76 заседание на комисията за защита на даните в телекомуникациите.....	6
Заседание на Комитета за координиран надзор.....	9
Заседание на координационата група за надзор на митническата информационна система	10
Председателят на КЗЛД откри събитие на IAPP Bulgaria Knowledgenet chapter.....	11
Годишна среща с компетентните органи по чл.20 от ЗЗЛСПОИН.....	12
Продължава изпълнението на проект ОРWNI	14
Информационна брошура по ЗЗЛСПОИН	15
Разработка на победителя от студентския конкурс за есе	18
КОНТРОЛНА ДЕЙНОСТ.....	29

СЪБИТИЯ И ИНИЦИАТИВИ

ИЗМЕНЕНИЕ НА ПРАВИЛНИКА ЗА ДЕЙНОСТТА НА КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И НЕЙНАТА АДМИНИСТРАЦИЯ

Комисията за защита на личните данни открива процедура за обществено обсъждане на проект на Правилник за изменение на Правилника за дейността на Комисията за защита на личните данни и нейната администрация.

Мотиви към проекта на Правилник за изменение на Правилника за дейността на Комисията за защита на личните данни и на нейната администрация

Дата на публикуване на проекта: 06.11.2025г.

Дата на приключване на общественото обсъждане: 06.12.2025г.

Информацията относно общественото обсъждане е публикувана и на Портала за обществени консултации

ПРИЕТА Е НОВА СТРАТЕГИЯТА НА КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ -ХОРИЗОНТ 2030

На свое редовно заседание на 04 декември 2025г. Комисията за защита на личните данни (КЗЛД, комисията) прие своя нова „Стратегия на КЗЛД за развитие в областите на защитата на личните данни и на защитата на лицата, подаващи сигнали или публично оповестяващи информация за нарушения - Хоризонт 2030“ (Стратегията). Стратегията на КЗЛД - Хоризонт 2030, представлява от една страна продължение на Стратегията на КЗЛД – Хоризонт 2022, като отчита преимуществата на натрупания над 20-годишен опит на Комисията и взема предвид проблемните области и слабости в досегашното прилагане на нормативната уредба в областта на защитата на личните данни, а от друга страна е надградена и интегрира възложените на КЗЛД нови функции в ролята ѝ на централен орган за външно подаване на сигнали и за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения, съгласно ЗЗЛПСПОИН.

Стратегията отчита, както изискванията на националната, така и на европейската правна рамка, а също и практиката в двете области, включително и проектите на нормативни актове на европейско ниво към момента на приемането ѝ. Европейската комисия приема, че гражданите заемат централно място в цифровата трансформация на ЕС, а в новата икономика на данните личните данни на физическите лица са един от основните ѝ елементи. Стратегията е насочена и към потребностите на гражданите по отношение на публичните институции в Република България при защитата на личните им данни, което се изразява в осигуряване на повече публичен контрол, подобряване качеството на предоставяните публични услуги и гарантиране на по-висок стандарт на защита. Като национален надзорен орган по защита на данните КЗЛД ще продължава да се стреми да осигурява реална и последователна защита на високо равнище на основните права на защита на данните и неприкосновеността на личния живот, като едновременно бъде и ефективна и отговорна институция. Като централен орган за външно подаване на сигнали и за защита на лицата, на които такава защита се предоставя по смисъла на ЗЗЛПСПОИН, КЗЛД ангажира своите усилия и постави началото на изграждането на единна система за защита на лицата, подаващи сигнали за нарушения.

В Стратегията е заложен и конкретният подход за изпълнението ѝ, като средствата и индикаторите за оценка на изпълнението ще бъдат подробно описани в План за изпълнение и контрол на изпълнението. Конкретните стъпки за достигането на желаните резултати ще бъдат заложи в годишните планове за дейността на КЗЛД и изпълнение на длъжността на ръководителите и служителите в комисията.

По своята същност Стратегията на КЗЛД е замислена като отворен документ, който може да отговори адекватно на променящите се обществени отношения, породени от възникващи глобални заплахи и бурното развитие на сектора на информационните и комуникационни технологии.

Стратегията съдържа в себе си и механизъм за мониторинг и оценка на изпълнението. Предвидено е изготвянето на междинна оценка и анализ на изпълнението. Целта на този механизъм е възможността за коригиращи действия за постигане на очакваните резултати и по този начин стратегическите цели на КЗЛД да се реализират най-ефективно.

Наличието на стратегически документ на КЗЛД дава възможност за предвидимост и устойчиво развитие в областите на защитата на личните данни и на защитата на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. Стратегията е основа за дългосрочната дейност на комисията и предвид динамиката на новите тенденции за развитие в областите на защитата на личните данни и на защитата на лицата, подаващи сигнали или публично оповестяващи информация за нарушения, съдържа в себе си и механизъм за преосмисляне на оперативните и краткосрочни действия на комисията, който при необходимост да послужи като основа за работа по надграждането ѝ.

Пълният текст на Стратегия на КЗЛД – Хоризонт 2030 може да намерите [тук](#).

КЗЛД ОТБЕЛЯЗВА 28 ЯНУАРИ – ДЕН ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

По случай ежегодните чествания на Деня за защита на личните данни — 28 януари, представям на Вашето внимание предложение за провеждане на следните инициативи и мероприятия за 2026 година:

1. Обявяване на традиционен студентски конкурс за есе на актуална тема, свързана с предизвикателствата пред защита на личните данни. - предназначено за студенти в последната година от обучението във висше училище

Мероприятието предлагам да бъде извършено на следните етапи:

- На 28 януари — публикуване на покана;
- Първи етап: Електронно кандидатстване;
- Втори етап: Презентация пред конкурсната комисия;
- Награждаване на официална церемония в зала „Заседателна“ на КЗЛД.

Съгласно вече утвърдената практика класираните на първо, второ и трето място да бъдат включени в програма на КЗЛД за платен стаж в Комисията.

2. „Първо национално състезание по защита на личните данни

1 Предложението е образователна инициатива под формата на състезание, насочена към студенти по право от различни университети в страната, с цел да развие практически знания и умения в сферата на защитата на личните данни. Състезанието е предвидено да се проведе в два основни етапа, симулирайки реален административен процес, **ВКЛЮЧИТЕЛНО** обжалване пред съд. Преди двата основни етапа от състезанието са предвидени редица организационни дейности.

Инициативата предлагам да бъде извършено на следните етапи:

- Подготовка на състезанието, планиране, набиране и регистрация на участниците.
- Първи етап — провеждане на административно производство пред Комисията за защита на личните данни и оценяване на резултатите на участниците;

= Втори етап: провеждане на съдебно производство пред Административен съд; - финално оценяване и награждаване;

Победителите ще бъдат наградени на официална церемония, проведена публично, с участието на партньорите и експертите, подкрепящи инициативата в зала „Заседателна” на КЗЛД, бул. „Проф. Цветан Лазаров” 2. Всички участници ще получат удостоверение за участие.

3. Разяснителната дейност в училище за защита на личните данни на децата (под название „Лична сигурност”) в рамките на провеждания „ час на класа”.

Мероприятието е предвидено във връзка с политиката на превенция и информираност, която е част от приетата на КЗЛД Стратегия за развитие в областите на защитата на личните данни и на защитата на лицата, подаващи сигнали или публично оповестяващи информация за нарушения - Хоризонт 2030.

Предвижда се със съдействието на Министерството на образованието и науката и други заинтересовани страни да се изготвят и популяризират електронни модули за самообучение или брошури, които да са насочени към нуждите на децата и юношите с цел превенция, информираност и повишаване на осведомеността на обществото в областта на защитата на личните данни.

4. Създаване на онлайн анкета, насочена към администратори на лични данни за получаване на обратна връзка относно нуждите и удовлетвореността им във взаимоотношенията им с надзорния орган.

Предложеното мероприятие има за цел да се получи в КЗЛД актуална информация относно взаимодействието на институцията с лицата, обработващи лични данни и отчитане

на степента на удовлетвореност спрямо нуждите, включително проучване на мнение, отношение, нагласи и очаквания. Това ще спомогне за подобряване на административните услуги, които КЗЛД предоставя в рамките на нейната компетентност.

5. Поредица учебни посещения на студенти от висши учебни заведения

Предложената инициатива има за цел да популяризира дейността на КЗЛД сред студентите в България. Същата може да се обяви по повод 28 януари, като на тази дата или около нея може да се осъществи посещение на курсанти от Академията на МВР. Следващите учебни посещения може да се планират през 2/3 месеца, т.е. през месец март/април за студенти от СУ „Св. Климент Охридски”, през май/юни за студенти от Югозападния университет „Неофит Рилски”, през септември/октомври за студенти от Нов български университет, през ноември/декември за студенти от Университета за национално и световно стопанство. Посещенията могат да бъдат проведени като полудневни събития за запознаване на участниците с дейността на отделните звена от администрацията, както и с производствата пред КЗЛД.

б. Кръгла маса за представители на висшите учебни заведения

Събитието има за цел да ангажира академичната общност с проблемите при прилагането на Общия регламент относно защитата на данните. Същото може да бъде обявено по повод 28 януари, да бъде проведено през месец април (около 10-та година от приемането на ОРЗД) или през месец май, в сътрудничество с Академията на МВР. Кръглата маса може да бъде планирана като полудневно събитие с до две основни дискусии (презентация и сесия с въпроси и отговори след нея).

7. Финално събитие по проект ОРWHI— Open the whistle: Profecfing whistleblowers through transparency, cooperation аш! open government stratfegies

На 28 януари може да се проведе финалното събитие за разпространение на резултатите по проект ОРWHI, финансиран от Европейския съюз чрез програма „Граждани, равенство, права и ценности”. Гостите на събитието между 30 и 60 човека, вкл. представители на други държавни институции, работодателски организации, неправителствен сектор, академичните среди, ще бъдат запознати с разработените по проекта интелектуални продукти и извършени дейности.

Събитието започва с регистрация от 9.30 ч. в наета зала в центъра на София. Официалното откриване е от 10.00 ч. и ще приключи в 12.30 ч. с коктейл. Средствата за реализирането му са предвидени в бюджета на проекта и ще бъдат разходвани от Центъра за изследване на демокрацията (ЦИД) като един от двата български партньори по проект. Събитието ще се обяви като инициатива по проекта, съвместно реализирана от КЗЛД и ЦИД.

ЕКЗД ПРОВЕДЕ ВТОРО СЪВМЕСТНО ЗАСЕДАНИЕ С ОРГАНИТЕ ЗА ЗАЩИТА НА ДАННИТЕ НА ДЪРЖАВИТЕ С РЕШЕНИЕ ЗА АДЕКВАТНОСТ

По време на декемврийското пленарно заседание на Европейският комитет по защита на данните (ЕКЗД) беше проведено онлайн заседание с комисари и представители на органите за защита на данните от държавите, които са с решение на ЕС относно адекватното ниво на защита на данните (списък). Решението относно адекватното ниво на защита е ключов механизъм в законодателството на ЕС за защита на данните, който позволява свободното движение на лични данни от Европа към трети държави или международна организация, предлагащи адекватно ниво на защита на данните.

Това заседание е второто по рода си след като първото се осъществи през октомври 2024 г. с органите по защита на данните от петнадесетте държави с решение на ЕС относно адекватното ниво на защита. След него ЕКЗД и органите за защита на данните от държавите и

организацията с решение на ЕС относно адекватното ниво на защита засилиха сътрудничеството си чрез обмен на информация относно някои консултативни дейности и събиране на опит относно международното сътрудничество в областта на правоприлагането в областта на защитата на данните.

Надзорните органи за защита на данните с решение относно адекватното ниво на защита и Европейската патентна организация са ключови партньори за ЕКЗД и имат ключова роля в съвместните усилия за укрепване на защитата на данните в световен мащаб.

Според председателя на ЕКЗД г-жа Ану Талус първото съвместно заседание през октомври 2024 г. е допринесло за по-тясно сътрудничество и обмен на ценни знания и опит в областта на защитата на данните. Високата степен на ангажираност, демонстрирана по време на втора среща на ЕКЗД и органите за защита на данните от държавите и Европейска патентна организация, за които Европейският съюз прие решение относно адекватното ниво на защита, е знак за ангажимента да се продължи работата в тази обща посока. От своя страна проведеното заседание е възможност за всички участници да споделят мнения за минали дейности и актуална информация относно следващите приоритети в областта на правоприлагането и консултациите.

Европейската комисия има правомощието да определя въз основа на член 45 от Регламент (ЕС) 2016/679 дали дадена държава извън ЕС предлага адекватно ниво на защита на данните. Приемането на решение относно адекватното ниво на защита включва предложение на Европейската комисия; становище на Европейския комитет по защита на данните; одобрение от представители на държавите от ЕС; приемане на решението от Европейската комисия.

Заседанието се проведе по време на декемврийската пленарна сесия на ЕКЗД, на която се приеха и препоръки относно правното основание за изискването за създаване на потребителски профили на уебсайтовете за електронна търговия. Като общо правило потребителите следва да имат възможност да използват уебсайта за електронна търговия, включително възможността да извършват покупки, без да създават профил. В такива случаи ЕКЗД препоръчва уебсайтовете за електронна търговия да предлагат избор: или режим „гост“, който позволява на потребителите да правят покупки, без да създават профил, или възможност за доброволно създаване на профил. Този подход свежда до минимум събирането и обработването на лични данни и следователно е в съответствие с принципа на ОРЗД за защита на данните на етапа на проектирането и по подразбиране.

Задължителното създаване на профил обаче може да бъде оправдано в ограничен брой случаи, включително предлагане на абонаментна услуга или предоставяне на достъп до изключителни оферти.

В препоръките се подчертават усилията на ЕКЗД за насърчаване на прагматични, лесни за ползване и защитаващи неприкосновеността на личния живот практики в сектора на електронната търговия.

Те са обект на обществена консултация до края на месец януари 2025 г.

На декемврийското пленарно заседание на ЕКЗД беше проведено предварително обсъждане на предложението за цифров „омнибус“, по което ЕКЗД и ЕНОЗД ще излязат със съвместно становище.

В своето изявление от Хелзинки ЕКЗД направи предложения за постигане на по-голяма яснота, подкрепа и ангажираност. ЕКЗД и ЕНОЗД приветстват обсъждането на ефективното цифрово регулиране и остават ангажирани с намирането на решения за улесняване на спазването на ОРЗД, особено за малките организации. ЕКЗД и ЕНОЗД ще се съсредоточат върху начина, по който предложението на Европейската комисия ще окаже въздействие върху основните права на физическите лица, и дали то ще доведе до опростяване за организациите и по-голяма правна сигурност.

След гласуване, членовете на ЕКЗД избраха г-жа Йелена Вирант Бурник, Комисар по информацията на Република Словения, за нов заместник-председател на Комитета.

През следващите пет години госпожа Бурник ще работи в тясно сътрудничество с председателя на ЕКЗД Ану Талус и с другия заместник-председател господин Здравко Вукич, за да се гарантира последователното прилагане на правилата на ЕС за защита на данните и да се насърчи ефективното сътрудничество между органите за защита на данните в цяла Европа.

76 ЗАСЕДАНИЕ НА МЕЖДУНАРОДНАТА РАБОТНА ГРУПА ПО ЗАЩИТА НА ДАННИТЕ В ТЕЛЕКОМУНИКАЦИИТЕ



В периода 19-20 ноември 2025 г. в Монтевидео, Уругвай, се проведе 76-тата среща на Международната група по телекомуникации, известна още като „Берлинската група“. Събитието се проведе по покана на проф. д-р Ана Брайън Нугрес – специален докладчик на ООН за правото на неприкосновеност на личния живот и Университетът в Монтевидео, Уругвай с подкрепата на Комисия за регулиране и контрол на личните данни на Уругвай (URCDP).

На заседанието е представен доклад на Съвета на Европа, включващ основните дейности, извършени от Комитета по Конвенция 108 от януари до ноември 2025 г. В него се подчертава работата на Комитета по надзора на прилагането на Конвенция 108, прави се преглед на разработените стандарти, подкрепата, предоставяна на органите за защита на данните, и действията за насърчаване на международното сътрудничество.

Протоколът за изменение на Конвенция 108 (№ 223, „Конвенция № 108 +“) има 46 подписа и 33 ратификации, включително ратификациите от Гърция и Монако през март 2025 г., като остава само 5 ратификации за влизането му в сила. На всяко пленарно

заседание Комитетът обсъжда националните процедури за подписване и ратифициране от страните, които все още не са ги приключили, както и новите искания за присъединяване.

На 48-ото си пленарно заседание Комитетът е приел Насоки относно общите принципи на член 11 от Конвенция 108 +, в които се изясняват условията, при които могат да се правят законни изключения от правилата за защита на данните. Това представлява значителна стъпка в тълкуването и предоставянето на насоки в областта на обществената сигурност за това как да се гарантира подходяща защита на неприкосновеността на личния живот въз основа на единствения правно обвързващ многостранен договор за защита на данните.

На 49-ото пленарно заседание през ноември комисията прие работния план за периода 2026-2029 г. (с приоритети за приключване на процеса на ратификация, неприкосновеност на личния живот и нови технологии, предаване на данни, неприкосновеност на личния живот в областта на обществената сигурност).

Освен това понастоящем Комитетът работи по проект на насоки относно неприкосновеността на личния живот и защитата на данните в контекста на големите езикови модели - базирани на системи (LLM). Целта е да се осигури практическа, основана на риска рамка за идентифициране, оценяване, смекчаване и наблюдение на рисковете за неприкосновеността на личния живот през целия жизнен цикъл на големите езикови модели. Документът поставя в контекст основните принципи на Конвенция № 108 + за тази специфична технологична среда, в която се изясняват ключови понятия и се очертават основните предизвикателства, породени от LLM.

Друг документ, по който се работи е проект за насоки относно защитата на данните в контекста на невронауките. Целта е да осигурят всеобхватна рамка за защита на основните права в контекста на нововъзникващите неврологични технологии.

В документа се тълкуват и прилагат основните принципи на Конвенция № 108 + по отношение на обработването на невронни данни (като се разглеждат законосъобразността, пропорционалността, прозрачността, свеждането на данните до минимум, сигурността и съдържателното съгласие), като същевременно се определят специфичните рискове за неприкосновеността на личния живот и правата на човека, присъщи на събирането, използването и извеждането на невронна информация.

След приемането на примерните договорни клаузи на Съвета на Европа през 2024 г. Комитетът обмени мнения относно напредъка, постигнат от различните държави в тяхната вътрешна процедура за одобрение.

Освен това, Комитетът по Конвенция 108 провежда дискусии по допълнителни инициативи относно международното предаване на данни. От Секретариата се очаква да изготви въпросник и проект на план за действие, както и да очертае процедурата за назначаване на докладчици, които ще спомогнат за популяризирането на стандартите и инструментите на Конвенция 108 +, като например модели на договорни клаузи за предаване на лични данни, в световните форуми за защита на данните. Това включва работа с платформи като Организацията за икономическо сътрудничество и развитие (ОИСР), Глобалната асамблея за защита на неприкосновеността, Европейския комитет за защита на данните (ЕКЗД) и др.

Комитетът приветства новите наблюдатели на Конвенция 108:

- Мрежа на африканските органи за защита на данните (NADPA)
- Еквадор, представяван от Служба за защитата на личните данни
- Чилийска асоциация на специалистите в областта на защитата на личните данни
- Колумбийският орган за защита на данните

Комитетът е участвал активно в множество международни събития през годината, а също така поддържа сътрудничество с други структури на Съвета на Европа по теми като изкуствен интелект и достъп до информация.

Друг документ, който е разгледан на това заседание е работният документ за „Споделянето на данни“. Документът е изготвен от италианския надзорен орган като водещ, подпомаган от словенския, корейския и каталунския надзорен орган. Темата на работния документ е определена на 75-тото заседание на подгрупата, проведено на 2-3 юли 2025 г. в гр. Тбилиси, Грузия. Документът подчертава стратегическото и икономическо значение на синтетичните данни като ключов актив за бизнеса и правителствата, с прогнозиран растеж на глобалния пазар от стотици милиони щатски долари през 2025-2026 г. до десетки милиарди към 2035 г., движен главно от генеративния ИИ в различни отрасли.

Още един документ, който е разгледан на заседанието, е преработеният проект за „Поверителни изчисления в облак“. Той има за цел да опише технологията за подобряване на неприкосновеността на личния живот, наречена поверителни изчислителни технологии, както са внедрени в облачните инфраструктури.

Поверителните изчисления са технология за подобряване на неприкосновеността на личния живот, предназначена за защита на използваните данни, като по този начин се разширяват класическите схеми за защита на данните в покой (когато се съхраняват на електронен носител) и на транзитните данни (когато се предават от един източник на получател).

Поверителни изчисления могат да бъдат внедрени във всяка компютърна инфраструктура, включително мобилни/периферни устройства, когато те могат да дадат възможност за приложения, които се нуждаят от високо равнище на доверие и надеждност, като например управление на самоличността и удостоверенията в приложенията на портфейла за цифрова самоличност. Настоящият документ, обаче се ограничава до внедряването на поверителни изчисления в облачните инфраструктури. Това е сценарий, който придоби особено значение през последните години с търговски платформи в облак като Google Cloud, Microsoft Azure или Amazon Web Services, които предоставят поверителни изчисления на широка аудитория.

Берлинската група е представила първи проект на документ „Съвместна комуникация и отчитане“ (JCAS), която в бъдеще ще комбинира безжична комуникация и сензорно засичане, позволявайки мрежите да откриват обекти и движение чрез радиосигнали. Целта е да се повлияе на текущите процеси по стандартизация, така че да се осигури „защита на данните по дизайн“.

По темата за правото на неприкосновеност на личния живот генералният секретар на Организацията на обединените нации (ООН) е представил доклад, изготвен от специалния докладчик за правото на неприкосновеност на личния живот Ана Брайън Нугрирес. Същият е в съответствие с Резолюция 28/16 на Съвета на ООН по правата на човека. Настоящият доклад допълва доклада на специалния докладчик относно правото на неприкосновеност на личния живот на фондациите и принципите за регулиране на невротехнологиите и обработването на неврологични данни от гледна точка на правото на неприкосновеност на личния живот от 16 януари 2025 г. (A/HRC/58/58). Целта на доклада е да положи основите за разработването на законодателство за невротехнологиите от гледна точка на правото на неприкосновеност на личния живот.

Друг документ, който е представен на заседанието, е докладът „Основи и принципи на регулирането на невротехнологиите и обработването на неврологични данни от гледна точка на правото на неприкосновеност на личния живот“, който също е на специалния докладчик на ООН за правото на неприкосновеност на личния живот Ана Брайън Нугрирес. Документът поставя основата за създаването на концептуална рамка за регулиране на използването на неврологични технологии и обработване на неврологични данни от гледна точка на правото на неприкосновеност на личния живот.

По-специално в доклада се разглеждат ключови определения и се установяват основни принципи, които да ръководят регулирането в тази област, включително защитата на човешкото достойнство, защитата на неприкосновеността на личния живот, признаването на неврологичните данни като изключително чувствителни лични данни и изискването за информирано съгласие за тяхното обработване.

Поставя се акцент върху включването на етични норми и защитата на правата на човека при проектирането и използването на тези технологии, както и върху прилагането на принципа на предпазните



мерки, демонстрираната отчетност, сигурното боравене с неврологични данни, недискриминацията и ефективната защита на правата на лицата при обработването на техните неврологични данни. Този подход има за цел да създаде стабилна основа, за да се гарантира, че регулирането на невротехнологиите е последователно, етично и предназначено да защитава основните права.

Отделни доклади за дейността на надзорните органи

бяха предоставени от: Швеция, Германия, Испания, Франция, Канада, Италия, Словения, Каталония, Грузия, Калифорния, Европейският орган.

ЗАСЕДАНИЕ НА КОМИТЕТА ЗА КООРДИНИРАН НАДЗОР



В периода от 9 до 10 декември 2025 г., се проведе двадесет и първото заседание на Комитета за координиран надзор (ККН) в град Брюксел, Кралство Белгия. Той е структура, чиято основна цел е осигуряването на координиран надзор над широкомащабните информационни системи, функциониращи на територията на ЕС, които се използват от органи, служби и агенции на ЕС. Създаден е в рамките на Европейския комитет за

защита на данните (ЕКЗД) и се състои от представители на националните органи за защита на данните на всяка държава членка на ЕС и Европейският надзорен орган по защита на данните.

Към настоящия момент ККН осъществява координация и надзор в рамките на обработването на лични данни в Информационната система на вътрешния пазар на ЕС, системата за съдебно сътрудничество по наказателноправни въпроси ЕВРОЮСТ, обработването на лични данни при осъществяването на действия от страна на Европейската прокуратура, Европейската прокуратура, Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол), Шенгенската информационна система (ШИС), Визовата информационна система, Системата Вход/Изход (СВИ).

Обработването на лични данни в следните широкомащабни системи и агенции на ЕС също ще попадне в обхвата на координиращите дейности на комитета:

- Европейската система за информация и разрешение за пътуване (ETIAS);
- Европейската информационна система за съдимост за лица, граждани на трети страни (ECRIS-TCN);
- Европейска база данни за дактилоскопия в областта на убежището (ЕВРОДАК);
- Митническа информационна система (МИС);
- Оперативната съвместимост между СВИ, ETIAS, ECRIS-TCN, ЕВРОДАК, ВИС и ШИС.

По време на заседанието се дискутира и приоритизацията на новите информационни системи, които в бъдеще могат да попаднат в обхвата на ККН - Механизъм за корекция на въглеродните емисии на границите (Carbon Border Adjustment Mechanism), Временен регистър, информационна система за обезлесяване на горите (Transitional Registry, Information System for Deforestation and Forest Degradation), дейности по обработване на данни, произтичащи от Акта за данните, системата AGORA (Акта за цифровите услуги), регулаторни лаборатории за оперативна съвместимост (Interoperability Regulatory

В рамките на частта, посветена на Шенгенската информационна система, се направи и кратко въведение в темата, свързана с Проверката на лог файловете по член 12 от регламентите за Шенгенската информационна система, по отношение на която предстои разработване на ръководство, предназначено за компетентните органи.

Акцент бе поставен върху Ръководството за правата на физическите лица, свързано със системата „Вход/Изход“, като се даде възможност на участниците да се включат към екипа по разработването на документа.

По отношение на частта от заседанието, посветена на Европол, бяха представени два доклада от Европейския надзорен орган по защита на данните - Съвместна надзорна дейност по отношение на обработването на данни на непълнолетни лица и Предварителната консултация по проекта Mjolnir.

Един от акцентите бе официалното представяне на новия заместник-координатор на ККН – г-ца Радостина Такова, главен експерт в отдел „Международно сътрудничество и управление на проекти“ в Комисията за защита на личните данни.

ЗАСЕДАНИЕ НА КООРДИНАЦИОННАТА ГРУПА ЗА НАДЗОР НА МИТНИЧЕСКА ИНФОРМАЦИОННА СИСТЕМА



CIS SCG

На 4 декември 2025 г. се проведе второто за тази година заседание на Координационната група за надзор на Митническата информационна система (МИС). В него взеха участие 20 представители на 15 държави-членки на Европейския съюз, на Европейския надзорен орган по защита на данните (ЕНОЗД), подпомагани от Секретариата на Групата. На заседанието се включиха и представители на Европейската комисия (ЕК) и на Европейска служба за борба с измамите (OLAF). По време на заседанието бяха приети съдържанието на общата част от Наръчника за упражняване правото на достъп до МИС и предложението към ККН за съвместно писмо до ЕК относно изясняването на приложимата правна рамка за МИС. Обсъдено беше съдържанието на въпросника относно националните институции с достъп до МИС. Единодушно участниците преизбраха за втори мандат досегашния председател на Групата – представителят на българския надзорен орган по защита на данните – г-н Христо Аламинов. Следващото заседание на Координационната група е планирано да се проведе през месец юни 2026 г.

ПРЕДСЕДАТЕЛЯТ НА КЗЛД ОТКРИ СЪБИТИЕ НА IAPP BULGARIA KNOWLEDGENET CHAPTER



На 30 октомври председателят на Комисията за защита на личните данни (КЗЛД) г-н Борислав Божинов взе участие в събитие, организирано от българското подразделение на Международната асоциация на професионалистите по защита на личните данни – IAPP Bulgaria KnowledgeNet Chapter.

Форумът събра водещи експерти в областта на защитата на лични данни, които обсъдиха бъдещето на защитата на данните в контекста на програмата на Европейската комисия и предложенията за опростяване на Регламент (ЕС) 2016/679 (GDPR) и Директива 2002/58/ЕО (ePrivacy). Участниците обсъдиха ключови концепции на GDPR и ePrivacy, както и влиянието на текущите регулаторни и правоприлагащи подходи на ЕС върху бизнеса и икономиката.

Събитието бе открито с приветствени речи на председателя на Комисията за защита на личните данни и на заместник-министъра на правосъдието. Беше поставен акцент върху баланса между технологичния напредък, бизнеса и правата на хората.

Участници в панелната дискуссия бяха Tatjana Lukoševičienė (Meta), Вяра Савова (European Crypto Initiative), Радослав Маринков (The Coca-Cola Company), Кирил Калев (Paysafe), както и проф. Мартин Захариев (Димитров, Петров и Ко). Модератор на дискуссията беше адв. Ирена Колева, мениджър в Адвокатско дружество „Делойт Лигъл“ и съпредседател на IAPP Bulgaria KnowledgeNet Chapter.

Дискуссията се фокусира върху значението на защитата на личните данни в дигиталната ера и взаимодействието между GDPR, ePrivacy и други цифрови регулации като Акта за изкуствения интелект, Акта за цифровите услуги), Акта за цифровите пазари и Директива NIS2. Подчерта се съществената роля на професионалистите в областта на защитата на лични данни и предизвикателствата, пред които те се изправят

ГОДИШНА СРЕЦА С КОМПЕТЕНТНИТЕ ОРГАНИ ПО ЧЛ. 20 ОТ ЗЗЛПСПОИН



На 17 ноември в зала 2 на Софийския университет „Св. Климент Охридски“ бе осъществена годишна среща между представители на Комисията за защита на личните данни (КЗЛД) и представители на компетентните органи по чл. 20 от Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (ЗЗЛПСПОИН).

Основната цел на срещата беше

обсъждането на начините за подобряване на взаимодействието и комуникацията между органите и КЗЛД при работата по сигналите, подадени по реда на ЗЗЛПСПОИН, както и събиране на статистически данни за нуждите на изготвянето на ежегодния доклад на Комисията, който тя изпраща на Европейската комисия.

КЗЛД е определена като централен орган за външно подаване на сигнали и за защита на лицата, на които такава защита се предоставя по смисъла на ЗЗЛПСПОИН.

В много кратки срокове Комисията успява да положи основите на националната система за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. Акцентът по приложението на закона е поставен върху информационно-разяснителната дейност сред задължените субекти по ЗЗЛПСПОИН – работодателите от публичния и частния сектор, с цел създаване на необходимите условия за законосъобразно изпълнение на техните законови задължения.

Ключов момент за приложението на закона е комуникацията и взаимодействието с компетентните органи по чл. 20 от ЗЗЛПСПОИН, които са натоварени с правомощията да извършват проверките по твърдяните нарушения от сигнализиращите лица. Важната роля на тези органи произтича и във връзка с двойното им качество и разграничението между функциите им на задължен субект по чл. 12 от закона и на компетентен орган по чл. 20 от ЗЗЛПСПОИН.

В тази връзка и с оглед на законовите задължения, разписани в чл. 29, ал. 3 от ЗЗЛПСПОИН, Комисия за защита на личните данни организира най-малко веднъж годишно обща среща с компетентните органи по чл. 20, на която се анализира дейността по работата със сигналите през изминалата календарна година, както и актуалните трудности и проблеми, пред които се изправят, както компетентните органи, така и централния орган за външно подаване на сигнали.

До приемането на Директива (ЕС) 2019/1937 защитата на лицата, сигнализиращи за нередности, е разпокъсана в различните държави членки, както и непоследователна в различните области на обществени отношения. Опитът обаче показва, че недостатъчната защита на лицата, подаващи сигнали дори в една държава членка води до отрицателно въздействие върху прилагането на политиките на Съюза и в други държави членки, доколкото последиците от нарушенията на правото имат все по-често трансгранично измерение. От друга страна, в резултат на недостатъчната защита потенциалните сигналподатели се въздържат да подават сигнали поради страх от ответни действия с цел отмъщение. С приемането на Директива (ЕС) 2019/1937 се цели предоставянето на балансирана и ефективна защита на лицата, сигнализиращи за нередности, като се отчита тяхната ключова роля за разкриването и предотвратяването на нарушения. Въвеждат се общи минимални стандарти и се осигурява всеобхватна и съгласувана правна рамка за защита на лицата, с което да се преодолее липсата на сигнали и съответното неблагоприятно въздействие и сериозни вреди на обществения интерес.

Директива (ЕС) 2019/1937 е транспонирана в българската правна система в ЗЗЛПСПОИН. Основната цел на закона е именно осигуряването на защита на лицата в публичния и в частния сектор, които подават сигнали или публично оповестяват информация за нарушения на българското законодателство или на актове на Европейския съюз, станала им известна при или по повод изпълнение на трудовите или служебните им задължения или в друг работен контекст.

ПРОДЪЛЖАВА ИЗПЪЛНЕНИЕ НА ПРОЕКТ ОРВНІ



В рамките на проект „OPWNI – Open the whistle: Protecting whistleblowers through transparency, cooperation and open government strategies“ (№ 101140801 – OPWNI – CERV- 2023-CHAR-LITI), финансиран по програма „Граждани, равенство, права и ценности“ на Европейската комисия, Комисията за защита на личните данни (КЗЛД) и Центъра за изследване на демокрацията (ЦИД) успешно реализираха серия от събития, насочени към разяснения и обучение относно защитата на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. През месеците ноември и декември 2025 г. са проведени общо 7 събития за разяснения и обучения от които:

- 3 присъствени – в София, Пловдив и Благоевград; и
- 4 вебинара.

Събитията бяха насочени, към представителите на публичния и частния сектор и Неправителствените организации (НПО). Целта им беше да се повиши осведомеността и капацитетът за ефективно прилагане на механизмите за защита на лицата, подаващи сигнали за нарушения, да се насърчи прозрачността и да се споделят практически подходи за обработване на сигнали и изграждане на вътрешни за организациите канали за подаване на сигнали.

През месец декември 2025 г. по проекта беше организирана и Peer-to-peer сесия между органите, определени, като външни канали за подаване на сигнали съгласно Директива (ЕС) 2019/1937, в България, Италия, Испания и Каталуния. Сесията цели обмена на опит и добри практики в областта на защитата на лицата, подаващи сигнали, управлението на външните канали за докладване и преодоляването на предизвикателства при трансграничното сътрудничество.

Тези дейности допринасят за укрепване на културата на сигурно подаване на сигнали в България и другите държави по проекта, като подпомагат изграждането на по-ефективни механизми за борба с нарушенията и защита на обществения интерес.

Дейностите по проект OPWNI за повишаване на осведомеността и повишаване на културата на сигурно подаване на сигнали ще продължат и през месец януари 2026 г., когато е планирано да се проведе национално събитие за разпространение на резултатите по проекта.



ИНФОРМАЦИОННА БРОШУРА ПО ЗЗЛПСПОИН

Ръководство по Закона за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения (ЗЗЛПСПОИН)

1. ЦЕЛИ ЗА ЗЗЛПСПОИН И РЕД ЗА ПОДАВАНЕ НА СИГНАЛИ ПО РЕДА НА ЗАКОНА

1.1 Какво цели законът?

Целта на ЗЗЛПСПОИН е да осигури защита на лицата, които подават сигнали или публично оповестяват информация за нарушения, които нарушения застрашават или увреждат обществения интерес и са станали известни в работен контекст.

1.2 Искаш да подадеш сигнал, но не знаеш къде?

Канали за подаване на сигнал

1) Вътрешен канал - задължителен за организации с над 50 служители, за работодателите в публичния сектор и общини с население над 10 000 души.

Вътрешният канал има задължение да осигури:

- лице за контакт
- регистър
- достъпна информация относно процеса по подаване на сигнали
- процедура за проверка на твърдените нарушения
- защита на подателя

2) Външен канал - Комисия за защита на личните данни (КЗЛД)

Използва се, когато:

- работодателят няма вътрешен канал
- сигналподателят няма доверие във вътрешния канал
- налице е риск от прикриване
- налице е сериозно нарушение

В случай, че работодателят ти няма изграден вътрешен канал за подаване на сигнали по реда на ЗЗЛПСПОИН, можеш да сигнализираш Комисията за защита на личните данни по следните начини:

- а. На официалния сайт на Комисията <http://www.cdpd.bg> в секцията „Подаване на сигнали за нарушения съгласно закона за защита на лицата подаващи сигнали или публично оповестяващи информация за нарушения“ → „Подай сигнал“
- б. Лично в деловодството на КЗЛД, находящо се в гр. София, бул. „Цветан Лазаров“ № 2, ет. 1
- в. Чрез Системата за сигурно електронно връчване (ССЕВ)
- д. По електронната поща whistleblowing@cpdp.bg
- е. Чрез куриерска фирма
- ф. По пощата
- г. По факс

1.3 Етапи при обработка на сигнал:

- 1) Регистриране
- 2) Проверка за редовност, допустимост, правдоподобност и достоверност

- 3) Проверка / препращане на компетентни органи
- 4) Прилагане на мерки за защита
- 5) Обратна връзка от извършената проверка

2. ИНФОРМАЦИЯ ЗА СИГНАЛОПОДАТЕЛИТЕ

2.1 Кой може да подаде сигнал?

- Служител на служебно или трудово правоотношение
- Лица, които упражняват свободна професия или занаятчийска дейност
- Стажанти и доброволци
- Съдружник, акционер, едноличен собственик на капитала, член на управителен или контролен орган на търговско дружество, член на одитния комитет на предприятие
- Лице, което работи за физическо или юридическо лице, изпълнители, негови подизпълнители или доставчици
- Лице, на което предстои да започне работа и е получило информацията по време на подбора
- Лице, което се е сдобило с информацията, докато е било на трудово или служебно правоотношение, но същото към момента на подаване на сигнала е прекратено

2.2 В кои хипотези може да бъде подаден сигнал?

Можеш да подадеш сигнал, ако отговаряш на изискванията в т. 2.1 и научиш (в работен контекст), че на работното ти място се извършват нарушения в областта на:

- Обществените поръчки
- Финансовите услуги
- Безопасността на продуктите
- Безопасността на транспорта
- Опазването на околната среда
- Радиационната защита и ядрената безопасност
- Безопасността на храните и фуражите, здравето на животните и хуманното отношение към тях

- Общественото здраве
- Защитата на потребителите
- Защитата на личните данни
- Киберсигурността
- Финансовите интереси на Европейския съюз
- Правилата на вътрешния пазар, конкуренцията и държавните помощи
- Трансгранични данъчни схеми
- Заплащането на дължими публични държавни и общински вземания
- Трудовото законодателство
- Изпълнението на държавната служба

Също така можеш да подадеш сигнал, ако отговаряш на изискванията в т. 2.1 и научиш (в работен контекст) относно извършването на престъпление от общ характер.

2.3 Може ли да се подаде анонимен сигнал?

Не, по анонимни сигнали не се образува производство.

2.4 Правило за поверителност

Следва да знаеш, че за подадения сигнал е налице правилото за поверителност, тоест не се разкриват данни за подателя и за свързаните лица, когато сигналът е приет за разглеждане по реда на ЗЗЛПСПОИН и отговаря на изискванията на закона. Разкриване на самоличността се извършва само след разрешение от подателя.

2.5. Притесняваш се да не се предприемат ответни действия срещу теб, ако подадеш сигнал?

В случай, че бъдат предприети ответни действия срещу лице във връзка с подадения сигнал, компетентните органи по чл. 20, ал. 1 от ЗЗЛПСПОИН предприемат коригиращи мерки. Коригиращите мерки имат за цел да преустановят предприетите ответни действия посочени по-горе до приключване на извършената от компетентните органи проверка.

3. ИНФОРМАЦИЯ ЗА ЛИЦАТА, НА КОИТО СЕ ПРЕДОСТАВЯ ЗАЩИТА

3.1. От кога лице, подало сигнал има право на защита по реда на този закон?

Защита по Закона се предоставя на сигнализиращо лице от момента на подаването на сигнала или публичното оповестяване на информация за нарушение, в случаите, когато са налице законоустановените предпоставки.

3.2 На кого освен на сигналоподателя може да се предостави защита?

- Лица, които помагат на сигнализиращото лице в процеса на подаване на сигнал и чиято помощ следва да е поверителна
- Лица, които са свързани посредством работата или роднини на сигнализиращото лице и които могат да бъдат подложени на ответни действия поради сигнализирането
- Юридически лица, в които сигнализиращото лице притежава дялово участие, за които работи или с които е свързано по друг начин в работен контекст

3.3. Условия за получаване на защита по реда на ЗЗЛПСПОИН:

- Сигналът е подаден по реда на ЗЗЛПСПОИН с изрично посочване на този ред
- Подателят е лице, което притежава някое от качествата в т. 2.1
- Сигналът е достоверен, правдоподобен и попада в предметния обхват, посочен в т. 2.2
- Сигналът е подаден при наличието на „работен контекст“
- Налице е засегнат обществен интерес, а не личен такъв
- Защита може да бъде предоставена при положение, че не е налице хипотезата на осъществени „ответни действия“ преди подаването на сигнала
- Лицето е подало сигнала добросъвестно, тоест имало е основателна причина да смята, че информацията е вярна към момента на подаването на сигнала

3.4 Предоставяне на защита при публично оповестяване на информация за нарушение

Лице, което публично оповестява информация за нарушение, има право на защита, когато са изпълнени изискванията по т. 3.2 и някое от следните допълнителни условия:

- Липса на действия след подаден сигнал
- Непосредствена или явна опасност за обществен интерес
- Риск от унищожаване на доказателства

3.5 Какви мерки за защита притежаваш, ако разкриеш своята самоличност за времето на извършване на проверката по сигнала?

Налице е забрана на работодателя да извършва следните репресивни ответни действия спрямо теб, а именно:

- уволнение
- понижение
- дисциплинарни наказания
- изменение на работата – място, характер, продължителност на работното време
- принуда, заплахи
- предсрочно прекратяване на срочен трудов договор
- влошаване на условията на труд
- увреждане на репутацията
- прекратяване на лиценз или разрешение

- предсрочно прекратяване или разваляне на договор за доставка на стоки или услуги
- насочване на лицето към извършване на медицински преглед

4. ИНФОРМАЦИЯ ЗА ЗАДЪЛЖЕНИТЕ СУБЕКТИ (РАБОТОДАТЕЛИТЕ)

4.1 Изграждане на вътрешен канал

За организации с 50 или повече служители, за работодателите в публичния сектор и за общини с население с 10 000 или повече души е задължително изграждането на вътрешен канал за подаване на сигнали.

4.2 Споделяне на ресурси

Ако си работодател в частния сектор с 50 до 249 души персонал, си задължен субект и можеш да споделяш ресурси за получаването на сигнали и за предприемане на последващи действия по тях при спазване изискванията на ЗЗЛПСПОИН.

Ако си работодател в частния сектор с над 250 души персонал, си задължен субект, но нямаш законова възможност за споделяне на ресурси за създаване на вътрешен канал.

4.3 Какви са последиците, ако си задължен субект, а нямаш изграден вътрешен канал за подаване на сигнали?

Подлежиш на имуществена санкция в размер от 5 000 до 20 000 лв., а за повторно нарушение - в размер от 10 000 до 30 000 лв.



РАЗРАБОТКА НА ПОБЕДИТЕЛЯ ОТ СТУДЕНТСКИЯ КОНКУРС ЗА ЕСЕ

Заглавие

Фрагментация и концентрация на нелични данни в Европейския съюз: Икономически, правни и стратегически измерения на управлението на данните

Въведение

Данните се превърнаха в основата на цифровата икономика и важна част от дебата за стратегическата автономност на Европа. Те действат като стимул за иновации в почти всеки сектор: от промишлеността и транспорта до здравеопазването и изкуствения интелект (ИИ). Един от начините, по който Европа се стреми да се наложи в световен план е чрез изграждането и утвърждаването на единен пазар за данни². Фрагментацията и концентрацията на данни се очертават като две основни предизвикателства в този стремеж. Фрагментацията на данни се отнася до изолирането на данни в

отделни бази или в рамките на национални (или регионални) граници, както и до правните 27 или техническите бариери, които пречат на свободното движение на данни между юрисдикции, организации и частни лица.

Концентрацията на данни, от друга страна, описва натрупването на огромни масиви от данни и капацитет за тяхната обработка, в ръцете на няколко доминиращи фирми, което води до дисбаланс в пазарната сила. ЕС е изправен пред две основни предизвикателства. Първо, значителна концентрация на данни на цифровите пазари поради агломерацията на данни от страна на няколко фирми гиганти. Второ, значителна фрагментация на данните поради разпръснатото им създаване и липсата на стимули, за тяхното споделяне. И двете тенденции рискуват да подкопаят колективната стойност на данните за европейската икономика.

Този доклад акцентира върху неличните данни. Това са данни, които не са свързани с идентифицирано или идентифицируемо физическо лице, с цел да не се разширява ненужно обхвата. Тоест, въпросите, свързани с личните данни и поверителността са извън обхвата на доклада. Вместо това, ще се анализира създаването, икономиката и регулирането на нелични данни. Например, производствени данни от индустриални машини, показания от сензори (IoT), агрегирани корпоративни масиви от данни, информация от публичния сектор и други данни, които са напълно анонимизирани. Неличните данни са ключов ресурс за икономически растеж, развитие на изкуствения интелект и индустриални иновации, без да засягат пряко личния живот на хората. Европейската стратегия за данни (2020 г.) на Европейската комисия предвижда създаването на единно европейско пространство за данни, в което личните данни могат да се прехвърлят безопасно, а неличните данни да циркулират свободно, като по този начин се повиши глобалната конкурентоспособност и суверенитетът на Европа. За да се постигне тази политизирана визия, е необходимо както да се намали фрагментацията, така че данните да могат да циркулират и да взаимодействат в рамките на единния пазар, така и да се предотврати вредната концентрация на данни, която би могла да задуши конкуренцията и иновациите.

Този доклад анализира фрагментацията и концентрацията на нелични данни в ЕС и оценява действащата правна рамка. Глава 1 представя концепциите и причините те да възникват. Глава 2 разглежда ключовите инструменти на ЕС (FFNPD, Open Data Directive, DGA, Data Act, DMA) и как адресират тези проблеми. Глава 3 обобщава резултатите, оценява баланса между мерките срещу фрагментацията и концентрацията и формулира препоръки.

Глава 1: Концептуална и стратегическа рамка

1.1 Фрагментация на данните в икономиката на данните в ЕС

Техническата дефиниция на фрагментацията е противоположното на „свободното движение“ на данни. То възниква, когато данните са „изолирани“. Данни се считат за изолирани, когато са разделени от организационни, национални или технически граници, така че не могат лесно да бъдат комбинирани или обменяни. Фрагментирането често произтича от правни бариери, например национални закони, които ограничават износа на данни от страната, или технически несъвместимости - например патентовани стандарти, които правят наборите от данни от различни източници несъвместими.

Конкретен пример за правни бариери водещи до фрагментация на данни е френският закон за съхранение на здравни данни. Френското законодателство изисква всички данни, свързани със здравето на френските граждани, да се съхраняват и обработват във Франция от сертифицирани доставчици (съгласно режима *Hébergeur de Données de Santé*). Това означава, че болниците (или клауд компании, които ги обслужват) не могат да прехвърлят данните на сървъри извън Франция без изрично

[A European strategy for data | Shaping Europe's digital future 2](#) Ibid.
[Introducing Daniel Schnurr - CERRE](#)
Ibid.

разрешение . Някои държави членки наложили закони за локализация на данните, които изискват определени данни да се съхраняват на сървъри на тяхна територия, което фрагментира единния цифров пазар . Такива правила принуждават компаниите да дублират ИТ инфраструктурата си във всяка страна или да ограничават трансграничните услуги за данни, което пречи на ефективното използване на данни в ЕС като единен пазар. Подобна фрагментация възниква и при специфични 28секторни силози, например железопътни оператори в различни страни членки. Тук основната бариера са различни национални стандарти и операционни системи .

В Стратегията за данните от 2020 г. и потвърдена от 2025 (Data Union Strategy) , Комисията разглежда неоправданата фрагментация като пречка за иновации, ефективност и мащаба на единния пазар . Фрагментираният данни увеличават разходите за инфраструктура и услуги, ограничават конкуренцията и тежат особено на МСП. Едно от основните предизвикателства за Европа е да задържи и разрастне своите стартиращи и иновативни компании, като често цитиран от ЕК пример са компаниите в сферата на ИИ , които поради липсата на подходящи ресурси в Европа често търсят разрастване в САЩ. Целта на политиката е да се премахнат произволни или протекционистки бариери, като същевременно се запазят необходимите гаранции за сигурност и поверителност.

Макар че някои обществени интереси могат да оправдаят съхранението на данни на местно равнище, например, правителството може да ограничи преноса на данни, свързани с националната сигурност¹⁵. ЕС разрешава правила за локализация само на строги основания,

свързани с обществената сигурност и пропорционално ста . Консенсусът е, че фрагментацията в голяма степен затруднява развитието на икономиката на данните. Целта на политиката е да се осигури надежден обмен на данни чрез премахване на произволни или протекционистки бариери, като същевременно се запазват необходимите гаранции за сигурност и поверителност.

1.2 Концентрация на данни и „монополи върху данни“

Концентрацията на данни се отнася до пазарна структура, при която голяма част от ресурсите от данни и способността да се извлича стойност от тях се контролира от малък брой участници. В днешната цифрова икономика няколко технологични компании и платформи са натрупали огромни масиви от данни и аналитични възможности, създавайки значителна разлика между тях и по-малките фирми. Това се подхранва от network effects и икономии от мащаба. Фирмите с огромни масиви от данни могат да подобряват своите услуги и алгоритми, привличайки повече потребители и по този начин генерирайки още повече данни: едно самоусилващо се предимство . Класически пример за това са големите онлайн платформи. Малък брой участници могат да натрупат големи количества данни, събирайки важни познания и конкурентни предимства от богатството и разнообразието на данните, с които разполагат . От своя страна тези платформи могат да използват натрупаните от тях потребителски или бизнес данни, за да консолидират и допълнително укрепят пазарните си позиции. Концентрацията на данни не се ограничава до потребителските платформи, а се наблюдава и в промишлеността. Например, производителите на IoT устройства или превозни средства често по подразбиране запазват ексклузивен достъп до данните, генерирани от тези продукти, като по този начин възпрепятстват собствениците на устройствата или независимите доставчици на услуги да използват тези данни. По същия начин пазарът на клауд инфраструктура е силно концентриран, като няколко глобални доставчици доминират клауд услуги в Европа. ЕС е станал силно зависим от външни доставчици за обработката и съхранението на данни . Само Амазон, Майкрософт и Гугъл заемат над 70% от пазара на ЕС .

[Dentons - New EU regulation on the free flow of non-personal data: what is non-personal data and should I be worried about transfers of non-personal data?](#) - точка 2

[A European strategy for data | Shaping Europe's digital future](#)

[EUR-Lex - 52020DC0066 - EN - EUR-Lex](#) - точка 4 от комуникацията

Когато големи масиви от данни и капацитет за обработката им се концентрират в малък брой компании, това подкопава конкуренцията²¹ и иновациите. Доминиращите платформи могат да използват данни от бизнес потребители, за да предлагат конкуриращи продукти и да налагат обременителни условия, което създава бариери за навлизане. Например, доминиращ AppStore или пазар за електронна търговия може да използва данните, които събира от бизнес потребители в трети страни, за да пусне на пазара собствени конкурентни продукти или да наложи обременителни условия на тези предприятия, които на практика нямат алтернативни канали за достигане до своите клиенти. Малките предприятия зависят от достъп до данни, които могат да бъдат задържани или предоставяни при неблагоприятни условия. Така стойността на икономиката на данните остава заключена в няколко силоза, вместо да се разпределя в полза на общественото благосъстояние. Затова политиката на ЕС се ориентира към отваряне на достъпа до концентрирани данни, без да подкопава легитимни бизнес модели.

1.3 Двойно политическо предизвикателство

Фрагментирането и концентрацията на данни представляват двете страни на една политическа дилема. Ако данните не могат да се преместват или комбинират, се губи стойност. Ако ползите от данните се натрупват от малък брой участници, стойността се разпределя в тесни граници, в ущърб на благосъстоянието на потребителите и конкуренцията. И двете явления пречат на визията на ЕС за процъфтяваща и справедлива икономика на данните. От една страна, ЕС трябва да премахне фрагментираните бази на данни (насърчавайки свободния поток и оперативната съвместимост), а от друга да предотвратят блокирането на данните от доминиращи участници (осигурявайки по-широк достъп и лоялна конкуренция). Съответно стратегията на ЕС преследва мерки за управление на данните, които намаляват фрагментацията, като същевременно ограничават необоснованата концентрация. Следващата глава разглежда как това разбиране е превърнато в конкретни закони и инициативи на ЕС, насочени към управлението на нелични данни. В общи линии решението е насърчаването на засилен поток на данни и директна пазарна интервенция.

Глава 2: Правни и политически инструменти на ЕС ЕС отговоря на предизвикателствата, описани в глава 1, с поредица от законодателни мерки. В съответствие с Европейската стратегия за данни от 2020 г. (и потвърдено от 2025г.), която призовава за създаването на единно европейско пространство за данни, в което данните да могат да циркулират свободно и да се споделят с цел иновации и справедливост. Новата правна рамка на ЕС разглежда както фрагментацията, така и концентрацията на данни от различни ъгли.

2.1 Регламент за свободното движение на данни и Директива за отворените данни

Регламент (ЕС) 2018/1807 относно свободното движение на нелични данни

Регламентът, приложим от 2019 г., представлява първия опит на ЕС да ограничи фрагментацията в областта на неличните данни. Основното правило (чл. 4) забранява на държавите членки да изискват локализиране на такива данни, освен при строго обосновани съображения, свързани с обществената сигурност. Така предприятията могат свободно да съхраняват и обработват данни навсякъде в ЕС.

Регламентът гарантира и че публичните органи не могат да бъдат лишени от достъп до данни само защото те се намират в друга държава членка; съществуващите механизми за административно сътрудничество следва да бъдат използвани при трансгранични искания. Чл. 6 насърчава разработването на кодекси за поведение за улесняване на прехвърлянето между доставчици на облачни услуги. Пример са саморегулиращите се кодекси SWIPO от 2019 г.

По отношение на взаимодействието с Регламент (ЕС) 2016/679 (GDPR), Комисията издава през 2019 г. насоки за „смесените набори от данни“. Личните данни продължават да се ползват от защитата на GDPR, докато неличните елементи следва да могат да се движат свободно в ЕС. Регламент

292018/1807 премахва вътрешните бариери пред трансграничната мобилност на нелични данни, ограничава правната фрагментация и забранява неоправданото локализиране на данни.

Директива (ЕС) 2019/1024 относно отворените данни и повторното използване на информация от общественения сектор

Директивата, приложима от юли 2021 г., хармонизира правилата за отворените данни в ЕС. Тя задължава публичните органи да предоставят данните си за повторна употреба по подразбиране, в машинен формат и при минимални ограничения. Забраняват се ексклузивни споразумения с частни субекти.

Новост е въвеждането на „набори от данни с висока стойност“, определени в Регламент за изпълнение (ЕС) 2023/138. Тези категории, включително геопространствени данни, метеорологични данни, статистика, данни за дружества и мобилност, трябва да бъдат предоставяни безплатно, чрез API и възможност за масово изтегляне.

Директивата намалява фрагментацията, като осигурява еднакви правила за достъп до ключови публични данни в целия ЕС, и ограничава концентрацията, като прави ценните публични ресурси достъпни за всички участници, включително стартиращи и малки предприятия. Тя е основа за създаването на национални портали за отворени данни и на обединения европейски портал data.europa.eu. Комисията наблюдава изпълнението и може да започва процедури за нарушение при неизпълнение.

2.2 Закон за управление на данните (DGA)

Законът за управление на данните (Регламент (ЕС) 2022/868) създава първата цялостна европейска рамка за доверено и доброволно споделяне на данни. Той запълва регулаторни празнини, които не са покрити от правилата за отворени данни и от регламента за свободното движение на нелични данни. Основният му принос е установяването на механизми за контролирана повторна употреба на защитени публични данни. Публичните органи в ЕС разполагат със значителни масиви от данни, които не могат да бъдат публикувани свободно поради конфиденциалност, търговска тайна или права на интелектуална собственост. DGA задължава държавите членки да създадат единна контактна точка, която да разглежда искания за достъп до такива данни. Достъпът се предоставя само при наличие на технически и организационни гаранции, включително защитени среди за обработка и мерки за анонимизация. Регламентът забранява публичните органи да сключват ексклузивни договори за повторна употреба, което предотвратява създаването на затворени канали за достъп и гарантира равнопоставени условия за всички ползватели.

Друг ключов компонент е регламентирането на услугите за посредничество при споделяне на данни. Това са оператори, които свързват притежатели и ползватели на данни, без сами да използват или монетизират предоставената информация. DGA налага изисквания за неутралност, прозрачност и регистрация пред национален компетентен орган. Целта е компаниите да могат да споделят данни чрез доверена инфраструктура, която намалява риска от злоупотреби и правна несигурност. Европейската комисия поддържа централен регистър на всички сертифицирани посредници. Също, DGA въвежда режим за алтруизъм, при който признати оператори могат да събират дарени данни за научни и обществени цели при строги правила за прозрачност и етично управление, прилагайки GDPR при лични данни, с цел създаване на обществени масиви от данни, достъпни за широк кръг участници.

2.4 Закон за цифровите пазари (DMA)

[Introducing Daniel Schnurr - CERRE](#)

Ibid.

[Introducing Daniel Schnurr - CERREn](#)

[A European strategy for data | Shaping Europe's digital future](#)

Законът за цифровите пазари - регламент (ЕС) 2022/1925 (DMA) - е конкуренционен режим, насочен към големите онлайн платформи, определени като гейткипъри. Той въвежда правила, които ограничават концентрацията на данни и коригират информационните асиметрии. Гейткипърите трябва да предоставят на бизнес потребителите безплатен и незабавен достъп до данните, генерирани от тяхната дейност на платформата. Те нямат право да използват непублични данни на тези предприятия, за да получат предимство, както беше установено в разследванията срещу Amazon Marketplace за използване на данни на търговци от трети страни. Подобни опасения за злоупотреба с данни и самопредпочитане бяха повдигнати и в разследванията срещу Google във връзка с Google Shopping. Платформите трябва да осигуряват преносимост на данните за крайните потребители и не могат да комбинират лични данни от различни услуги без съгласие. Тези задължения целят да отворят затворените екосистеми и да намалят информационната власт на доминиращите компании.

Прилагането на DMA трябва да бъде съвместимо с GDPR. Споделянето на данни с бизнеса следва да зачита правата на субектите на данни. ЕК и Европейският комитет по защита на данните (EDPB) подготвят насоки, за да се осигури съгласуваност между режима за достъп до данни и защитата на личните данни.

Правилата на DMA отслабват предимствата, произтичащи от концентрацията на данни, и позволяват на по-малки конкуренти да получат достъп до ресурси, които преди това бяха ограничени до големите платформи. Законът не се занимава пряко с фрагментацията, но чрез стандартизиране на практиките в целия ЕС предотвратява избягването на задължения чрез различия в националните режими. DMA допълва останалите инструменти за данни и е ключов за ограничаване на прекомерната концентрация на информационна мощ в няколко глобални платформи.

2.5 Закон за данните (DA)

В тази нормативна картина Законът за данните (Data Act) е най-пряката намеса на ЕС в разпределението на контрол върху индустриалните и IoT данни. Неговият замисъл е да пренареди правата върху данните, генерирани при експлоатацията на „свързани продукти“ и свързани услуги, така че те да не останат изцяло заключени при производителя или доставчика на инфраструктура, а да бъдат достъпни за ползвателя на продукта и за трети страни по негов избор. От гледна точка на неличните данни това има особено значение за сектори като промишленост, енергетика, транспорт и земеделие, където огромни масиви от операционни и технически данни (логове от сензори, телеметрия, данни за производителност) понастоящем се съхраняват единствено в системите на производителя. Data Act изисква тези данни да могат да бъдат извлечени в използваем формат и при определени условия да бъдат пренасочени към други доставчици на услуги (например независими сервиси, доставчици на аналитични решения, оптимизационен софтуер). Така се регулира едно от ядрата на концентрацията на нелични данни - фактическата монополизация на индустриални данни от страна на производителя на оборудването.

Регламентът засяга и договорните механизми, чрез които големите предприятия укрепват контрола си върху данните. В много вертикални вериги (автомобилна индустрия, машиностроене, логистика) достъпът до нелични данни се урежда чрез стандартни договори, които малките и средните предприятия приемат без възможност за преговор. Data Act въвежда тест за „грубо неравноправни“ клаузи в договори между предприятия и предвижда, че определени типове ограничения върху ползването и повторната употреба на данни са недействителни, когато са наложени едностранно спрямо МСП. Това включва, например, клаузи, с които една страна си запазва неограничено право да използва и комбинира данните на другата, без реципрочен достъп или компенсация. В резултат регламентът не просто улеснява споделянето на данни, а ограничава използването на договорно право за затваряне на нелични данни в частни екосистеми.

Особено важен за структурата на пазара на нелични данни е и блокът от разпоредби, посветени на облачните и edge услуги. Към момента значителен дял от европейските индустриални

и корпоративни данни се обработват в инфраструктурата на няколко големи доставчици, като смяната на доставчик е свързана с технически блокировки, несъвместими интерфейси и високи транзакционни разходи. Data Act въвежда поэтапни задължения за улесняване на прехвърлянето на данни и работни натоварвания между доставчици, включително постепенно премахване на таксите за прехвърляне и изисквания за предоставяне на информация, необходима за „функционално еквивалентни“ услуги при новия доставчик. Това намалява фрагментацията, като насърчава по-голяма оперативна съвместимост между инфраструктурите, и едновременно с това атакува концентрацията, като прави излизането от доминиращи облачни платформи по-реалистично за предприятията. В дългосрочен план тази уредба цели да предотврати сценарий, при който не само данните, но и способността те да бъдат обработвани ефективно, е съсредоточена в тесен кръг глобални доставчици. Регламентът предвижда и специфичен режим за ситуации на „изключителна необходимост“, при които публични органи могат да поискат достъп до определени нелични данни, държани от частни оператори. Например, при природни бедствия, здравни кризи или задачи, свързани със сигурността на важни инфраструктури. От гледна точка на фрагментацията това създава юридически мостове между множество частни масиви от данни, които иначе биха останали разпръснати и недостъпни за системен анализ. В същото време строги критерии за необходимост, целево ограничение и компенсация на разходите трябва да предотвратят превръщането на този механизъм в източник на нова прекомерна концентрация на данни в публични ръце. Така Data Act работи не само с хоризонтални принципи (свободно движение, недискриминация), но и с прецизни процедурни гаранции за балансиране на достъпа.

Накрая, значима е и институционалната архитектура на регламента. Като изисква държавите членки да определят компетентни органи и като интегрира прилагането на Data Act в европейски структури за координация, той цели да предотврати появата на нова регулаторна фрагментация по линии на национални тълкувания и практики. В съчетание с другите инструменти Data Act представлява „операционният слой“ на политиката на ЕС. Чрез въвеждането на конкретни права за достъп до нелични данни, правила за договорна справедливост и механизми за инфраструктурна преносимост той превръща абстрактната цел за намаляване на фрагментацията и концентрацията в приложими, правно изпълними задължения.

Глава 3: Оценка и заключение

3.1 Влияние върху защитата на лични данни

Макар настоящият доклад да е насочен към неличните данни, не може да се пренебрегне фактът, че европейската рамка за управление на данните функционира в среда, в която личните и неличните данни съжителстват върху едни и същи инфраструктури, в едни и същи бази и в рамките на едни и същи бизнес модели. Всяка политика, насочена към намаляване на фрагментацията и концентрацията на нелични данни, неизбежно влияе върху начина, по който се прилага защитата на личните данни и върху практическата работа с GDPR. Дори когато законодателят формално изключва личните данни от обхвата на даден инструмент, реалността на смесените набори от данни и техническата възможност за повторна идентификация правят границата между двете категории нестабилна и динамична. Инструментите, които целят да ограничат фрагментацията, като свободното движение на нелични данни, оперативната съвместимост на инфраструктурите и създаването на общи европейски пространства от данни, стимулират по-интензивно движение и комбиниране на информационни масиви. Това увеличава броя на участниците, които имат достъп до дадени данни, и улеснява обединяването на различни източници. При чисто неличните данни този ефект се възприема като положителен, защото повишава икономическата стойност и ефективността на използването им. При смесените набори обаче натискът към агрегиране поставя под изпитание принципите на минимизация, ограничаване на целите и псевдонимизация, заложен в GDPR. Колкото по-широко се прилагат механизми за повторна употреба и споделяне, толкова по-голяма става вероятността данни, които формално са анонимизирани, да бъдат повторно свързани с конкретни субекти чрез кръстосване с други масиви или чрез нови аналитични техники.

Мерките срещу концентрацията на данни, като задълженията за споделяне на данни от големи платформи, правата на достъп до данни от свързани продукти и улесняването на cloud преносимостта,

водят до „разпръскване“ на достъпа до данни към по-широк кръг субекти. От гледна точка на конкуренцията и иновациите това е желан резултат. От гледна точка на защитата на личните данни обаче той означава, че увеличен брой администратори и обработващи получават правни основания да достигат до нови категории данни и метаданни. Ако тези нови права и задължения не бъдат стриктно подчинени на критериите на GDPR за правно основание, пропорционалност и ограничаване на целите, съществува риск инструментите срещу концентрацията да допринесат за разширяване на екосистеми за наблюдение, профилиране и вторична употреба, макар целта им формално да е коригиране на пазарни дисбаланси.

Тази амбивалентност се изостря от насочените промени в самия GDPR, предложени в контекста на по-широката реформа на цифровата рамка. Идеята за „таргетирано“ адаптиране на GDPR има за цел да намали административната тежест и да внесе по-голяма яснота по спорни понятия като легитимен интерес, оценка на въздействието и координация между надзорните органи. По-голямата предвидимост при прилагането на GDPR би могла да улесни и прилагането на новите режими за нелични данни, тъй като администраторите ще имат по-ясни ориентири кога и при какви условия могат да използват смесени набори, да разчитат на определени правни основания или да споделят данни в рамките на общите европейски пространства. В същото време всяко облекчаване на процедурите, например чрез по-гъвкаво тълкуване на легитимния интерес или опростяване на оценките на въздействието, крие риск да понижи прага на защита точно в момент, в който инфраструктурите за споделяне и повторна употреба на данни се разрастват и стават по-комплексни.

Правната техника, използвана в разгледаните инструменти, се стреми формално да предотврати конфликт с GDPR. DGA, Data Act, Регламентът за свободното движение на нелични данни и DMA изрично заявяват, че не засягат прилагането на правилата за защита на личните данни и че при наличие на лични елементи GDPR запазва своя приоритет. На ниво текст това решение елиминира йерархични противоречия между актовете. На практическо ниво обаче администраторите са изправени пред двоен регулаторен импулс. От тях се очаква да максимизират споделянето и полезността на неличните данни, включително в смесени масиви, и едновременно с това да ограничават обработването на лични данни до строго необходимото. Това увеличава значението на вътрешните процеси по оценка на риска, по картографиране на потоците от данни и по прилагане на техники за разделяне, псевдонимизация и анонимизация, които да бъдат устойчиви на повторно идентифициране в среда на интензивен поток на данни.

Институционалните механизми за координация се опитват да адресират тази сложност. Участието на органите за защита на данните в Европейския съвет за иновации в областта на данните и съвместните насоки на Комисията и EDPB относно взаимодействието между новите режими за данни и GDPR имат за цел да предотвратят размиване на стандартите за защита на личните данни и да ограничат риска от регулаторна фрагментация между държавите членки. Потенциалните изменения в GDPR се вписват в същата логика. Те трябва едновременно да намалят несигурността за администраторите, които оперират в новата рамка за нелични данни, и да запазят ефективността на основните гаранции за субектите на данни, включително правото на прозрачност, контрол и ефективна защита.

В заключение, въздействието на рамката за нелични данни върху защитата на личните данни е двупосочно. От една страна, новите инструменти и таргетираните промени в GDPR могат да създадат по-ясна, предвидима и координирана среда, в която икономиката на данните и защитата на данните съжителстват без формален конфликт. От друга страна, чрез насърчаване на споделянето, агрегиране и повторната употреба на информационни масиви тези политики увеличават натиска върху границата между лични и нелични данни и изискват по-високо ниво на техническа и институционална зрялост, за да се избегне постепенна ерозия на стандарта на защита. Доколко този баланс ще бъде устойчив в дългосрочен план, ще зависи не само от буквата на GDPR и свързаните актове, но и от качеството на тяхното тълкуване, прилагане и ревизия в светлината на развиващата се икономика на данните.

3.2 Оценка

Общата цел на рамката е да се реализира визията на Европейската стратегия за данните за „единен пазар на данни“. Тя намалява фрагментацията, като забранява необоснованите изисквания за локализация на данни, хармонизира правилата за отворени данни и установява оперативно съвместими технически и правни стандарти чрез DGA и Закона за данните. Тези закони създават общи условия за споделяне на публични и частни данни през държавните граници на страните членки и между пазарните сектори. Същевременно рамката се бори с прекомерната концентрация, като задължава мащабните притежатели на данни да предоставят достъп до определени набори от данни на другите. Законът за данните въвежда задължения за фирмите, които контролират индустриални данни или данни от IoT, да ги споделят с потребители и бизнес партньори, докато DMA задължава цифровите гейткипъри да осигурят оперативна съвместимост и преносимост на данните за потребителите и конкурентните услуги.

На теория тези инструменти се допълват взаимно. Фрагментираният данни от публичния сектор стават повторно използвани съгласно последователни правила. Данните от частния сектор стават споделяеми по надеждни и сигурни начини. Затворените екосистеми на доминиращите цифрови платформи се отварят за конкуренция. Този хоризонтален, междусекторен дизайн, обхващащ лични и нелични данни, има за цел да направи цифровата икономика на Европа интегрирана и справедлива. Общи принципи като защита на личните данни, справедлив достъп и оперативна съвместимост са в основата на всички закони, като насърчават равни условия за иновации, основани на данни.

Въпреки че рамката, въведена с Европейската стратегия за данни от 2020 г., на теория предвижда цялостен и амбициозен подход към изграждането на единен европейски пазар на данни, на практика тя се оказва прекалено комплексна и силно регулирана. Паралелното въвеждане на множество хоризонтални и секторни инструменти създава значителна

административна тежест и правна несигурност за бизнеса. Вместо да улесни споделянето на данни, тази свръхрегулация често възпрепятства оперативното прилагане на правилата и не успява да мобилизира реални обеми от данни в икономиката. Именно поради тези практически трудности Европейската комисия предприе в Data Union Strategy 2025 курс към опростяване, консолидиране и рационализиране на съществуващата рамка с цел намаляване на регулаторната сложност, премахване на припокриващи се задължения и осигуряване на по-предвидима, ефективна и икономически устойчива среда за споделяне и използване на данни в ЕС. Балансиране между фрагментация и концентрация

Въпреки двойната си цел, рамката изглежда по-скоро насочена към справяне с концентрацията на данни, отколкото с фрагментацията. Най-строгите и приложими закони (DA и DMA) се фокусират върху ограничаване на пазарната мощ на големите компании, разполагащи с голямо количество данни, като изискват от тях да споделят или да направят данните преносими. За разлика от това, мерките, насочени към фрагментацията, често разчитат на доброволно сътрудничество или инструменти на мекото право, като стандартизация, посредници на данни или механизми за алтруизъм на данни. Те имат за цел да насърчават, а не да налагат споделянето на по-малки или по-разпръснати масиви от данни.

Тази асиметрия отразява политическа и икономическа оценка, че по-належащият проблем на Европа не е липсата на фактически данни, а реалността, че достъпът до тях се контролира от няколко доминиращи участници. Разбиването на монополите върху данните се очаква да доведе до незабавни ползи за конкуренцията и иновациите, като позволи на стартиращи предприятия, МСП и изследователски институции да използват ценни индустриални данни или данни от платформи, които преди това бяха недостъпни. Например, от производител на устройства за интернет на нещата може да се изисква да споделя данни от машините с клиенти, или доминираща онлайн платформа трябва да позволи на потребителите да прехвърлят данните си към конкурентни услуги.

Въпреки това, преодоляването на фрагментацията е също толкова важно, тъй като гарантира, че новодостъпните данни могат действително да се разпространяват ефективно между секторите. В момента рамката на ЕС разчита на заинтересованите страни да прилагат оперативно съвместими стандарти и

да приемат доброволно практики за споделяне на данни. Този подход предполага, че след като бъдат премахнати основните пречки за доминиране на данните, ще се развие органично отворена екосистема за данни. Опитът обаче показва, че за функционирането на икономиката на данните са необходими както регулиране отгоре надолу, така и участие отдолу нагоре. Без силна техническа подкрепа, културни стимули и координация съществува риск да възникнат нови форми на концентрация дори в рамките на формално отворена система.

В този контекст Европейската комисия предприема по-директни интервенции чрез Data Union Strategy 2025, чиято цел е да коригира както прекомерната сложност на съществуващата правна рамка, така и забавеното практическо възприемане на механизмите за споделяне на данни. Стратегията признава, че комбинацията от множество законодателни актове е довела до операционална фрагментация и високи разходи за съответствие, особено за МСП. Ето защо Комисията предлага серия от целенасочени интервенции, които да заменят предходния „мрежов“ модел на взаимно допълващи се инструменти с по-опростена и по-кохерентна архитектура.

Комисията предприема по-активен подход към преодоляване на фрагментацията, като преминава от зависимости от доброволни механизми към инфраструктурно подпомагани форми на координация. Новите Data Labs и AI Factories ще осигуряват не само достъп до висококачествени и оперативно съвместими набори от данни, но и услуги по курация, анонимизация, синтетични данни и правно съответствие. По този начин Комисията признава, че пазарът сам по себе си не може да гарантира достатъчна интероперабилност и качество на данните, особено в сектори с неравномерно цифрово развитие.

Стратегията изрично предвижда пренасочване на зрелите сектори, включително финансовия, към „пазарно движен модел“, при който публичната намеса се свежда до стандартизация, интероперабилност и съвместни инвестиционни рамки. Това отразява теоретичната позиция на Комисията, която гласи че веднъж щом се осигури наличността на публични и високостойностни данни, а основните бариери пред конкуренцията бъдат премахнати чрез Data Act и DMA, пазарът следва сам да развие ефективни екосистеми за споделяне и повторна употреба на данни. С други думи, публичният сектор би трябвало да коригира структурните изкривявания и да предостави необходимите „хоризонтални активатори“, след което да позволи на участниците да изградят устойчиви бизнес модели върху тази основа.

3.3 Заключение

Развитието на европейската рамка за управление на неличните данни показва постепенен преход от силно нормативно ориентиран подход към модел, в който Европейската комисия и като цяло публичният сектор заема по-скоро подпомагаща и оркестрираща роля. Първоначалната фаза, белязана от приемането на FFNPD, Open Data Directive, DGA, Data Act и DMA, се стреми чрез правни задължения да намали фрагментацията и да ограничи концентрацията на данни. На практика обаче натрупването на хоризонтални и секторни инструменти доведе до значителна сложност, разходи за съответствие и „регулаторна умора“, особено за малките и средните предприятия. Именно тази претоварена нормативна среда е в основата на курса към опростяване и консолидиране, формулиран в Data Union Strategy 2025.

Новият подход се характеризира с това, че Комисията се отдръпва от ролята си на централен законодател на данните и се позиционира като доставчик на инфраструктура, хоризонтални улеснителни мерки и координационни механизми. Вместо да налага все по-подробни регулации, тя инвестира в общи платформи и инструменти, като общи европейски пространства за данни, Data Labs, AI Factories, стандартизирани формати, отворени API, референтни архитектури, модели на договорни клаузи и „one-click compliance“ решения. Така Data Union Strategy 2025 представлява пренастройване на ролята на публичната власт спрямо двата основни структурни риска в европейската икономика на данните: фрагментацията и концентрацията. От една страна, Комисията продължава нормативно да ограничава концентрацията чрез инструменти като DMA и Data Act, които принуждават доминиращите участници да отворят затворени екосистеми и да осигуряват достъп до данни. От друга страна, вместо да се опитва да регулира детайлно всички форми на обмен.

Европейската комисия преминава към инфраструктурно ориентиран подход за преодоляване на фрагментацията, които да улесняват интероперабилността и между-съюзническия поток от данни. Този преход към подкрепяща рамка почива на предпоставката, че след като концентрацията бъде удържана, а инфраструктурните бариери пред споделянето премахнати, пазарът сам ще бъде способен да намали остатъчната фрагментация и да предотврати възникването на нови центрове на прекомерна концентрация. Успехът на модела ще се измерва именно по това дали предоставените инструменти ще доведат до реално намаляване на фрагментацията и до по-равномерно разпределение на стойността, произтичаща от неличните данни в ЕС.

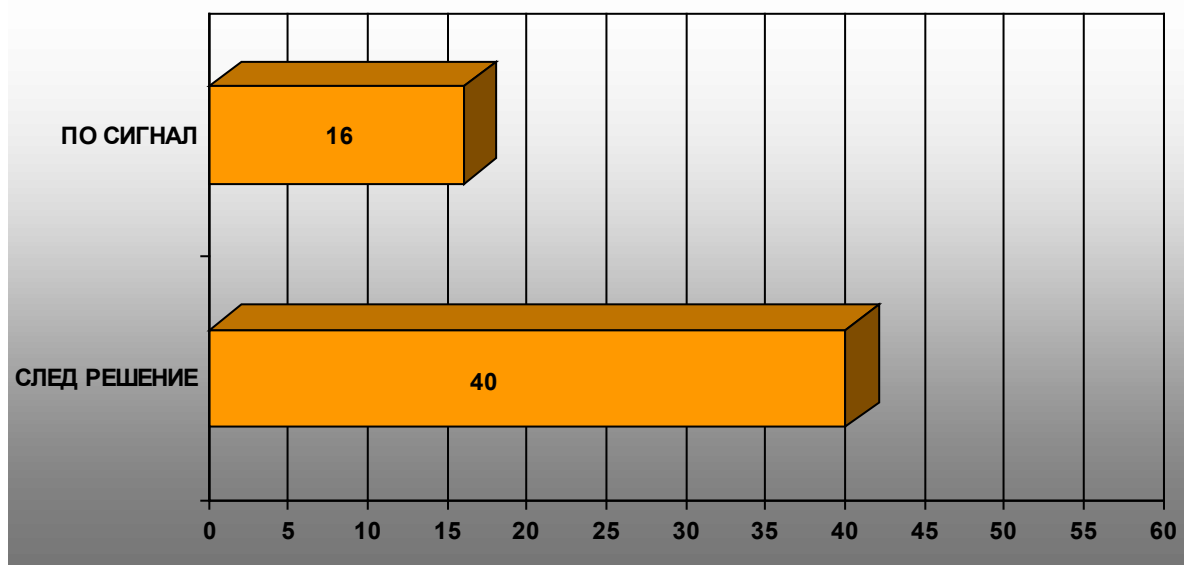
Библиография

1. Bristows LLP. “Two Worlds Collide: The Data Act Proposal v GDPR.” Lexology, 14 June 2022. <https://www.lexology.com/library/detail.aspx?g=7ef051bc-f5e6-4948-8d60-b7ce4ffed02c>.
2. Blomstein. “Data on Demand? Access to Gatekeeper Data under the DMA.” Briefing, April 2024. <https://www.blomstein.com/en/news/data-on-demand-access-to-gatekeeper-data-for-business-users-under-the-digital-markets-act>.
3. BusinessEurope. “Council Should Not Exempt the Free Flow of Data.” Press release, 18 December 2017. <https://www.buinessurope.eu/publications/council-should-not-exempt-the-free-flow-of-data/>.
4. European Commission. A European Strategy for Data. Communication COM(2020) 66 final, 19 February 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>.
5. “Free Flow of Non-Personal Data.” Digital Strategy Policy Page. Accessed October 2025. <https://digital-strategy.ec.europa.eu/en/policies/non-personal-data>.
6. “European Data Governance Act (DGA).” Digital Strategy Policy Page. Accessed October 2025. <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>.
7. European Data Protection Board and European Data Protection Supervisor. Joint Opinion 2/2022 on the EU Data Act Proposal, 4 May 2022.
8. Regulation (EU) 2018/1807 of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union. Official Journal of the European Union L 303, 28 November 2018. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>.
9. Directive (EU) 2019/1024 of 20 June 2019 on Open Data and the Re-use of Public Sector Information. Official Journal of the European Union L 172, 26 June 2019.
10. Regulation (EU) 2022/868 of 30 May 2022 on European Data Governance (Data Governance Act). Official Journal of the European Union L 152, 3 June 2022.
11. Regulation (EU) 2022/1925 of 14 September 2022 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act). Official Journal of the European Union L 265, 12 October 2022.
12. European Commission. Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act). Final compromise text, political agreement 2023 (publication pending).
13. Schnurr, Daniel. “Introducing Daniel Schnurr.” CERRE Interview, 2022. <https://cerre.eu/news/introducing-daniel-schnurr/>.
14. Schauer, Andreas, and Daniel Schnurr. “Data Brokers: Intermediaries for More Efficient Data Markets?” CPI TechReg Chronicle, October 2023.
15. U.S. Chamber of Commerce. The EU Data Act: A Misguided Policy. Washington, DC: U.S. Chamber of Commerce, 2022. <https://www.uschamber.com/assets/documents/US-Chamber-EU-Data-Act-Report.pdf>.

КОНТРОЛНА ДЕЙНОСТ

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА НОЕМВРИ-ДЕКЕМВРИ 2025 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета за м. ноември и декември 2025 г. са извършени общо 56 проверки – 16 след постъпили в КЗЛД сигнали и 40 след решение на КЗЛД.



Разгледани са 120 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 9 Разпореждания, отправено е 1 Предупреждение, 2 Официални предупреждения, наложени са 2 Временни забрани за обработване, съставен е 1 Акт за установяване на административно нарушение и е издадено 1 Наказателно постановление.



Комисия за защита на личните данни

Председател: Борислав Божинов
Членове: Василка Рангелова
Ивайло Станев
Цветана Червенякова- Илиева
Цветелин Софрониев

Информационен бюлетин № 1 (118) 2026 г.
Издава се съгласно чл. 10, ал. 3 от ЗЗЛД
Уеб сайт на КЗЛД: www.cpdp.bg

Разпространява се в електронен вид