Комисия за Защита на Личните Данни

ИНФОРМАЦИОНЕН БЮЛЕТИН

Брой 1 (112), януари 2025 г.

ТЕМИТЕ В БРОЯ

(бюлетинът отразява периода ноември и декември 2024 г.)

СЪБИТИЯ И ИНИЦИАТИВИ

ЗА ПОРЕДНА ГОДИНА КЗЛД ЩЕ ОТБЕЛЕЖИ ДЕНЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

На 28 януари 2025 г. Комисията за защита на личните данни традиционно отбелязва Денят за защита на личните данни. Възникнал като европейски, Денят за защита на данните вече се празнува в световен мащаб и извън Европа и за 19-ти пореден път в България. Основната цел на този празник е насърчаване на осведомеността и формиране на разбиране за значението на личните данни в цифрови свят и глобален обмен на информация – дейности вече превърнали се в част от ежедневието на всеки един от нас.

Прилагайки съвременен подход в провеждането на обучение в сферата на защита на данните КЗЛД завърши цялостно въвеждащо онлайн обучение в сферата на защитата на личните данни, насочено към публичния сектор. По повод на празника и със специалното сътрудничество с Института по публична администрация, обучението е достъпно за всички държавни служители.

За втора поредна година, Комисията обявява инициативата: годишна награда „Длъжностно лице по защита на данните на годината“. Тя цели затвърждаване на функциите на длъжностното лице по защита на данните и мотивиране на самите лица, които изпълняват тези функции. С инициативата КЗЛД се стреми да даде публичност и по-висока разпознаваемост на ежедневните усилия на усилията на длъжностните лица по защита на данните сред граждани, бизнеса и всички заинтересовани организации. Подборът на номинираните ще бъде извършван от КЗЛД въз основа на конкретни мотиви за всяка отделна номинация и при отчитане на следните критерии:

– наличие на политика за защита на личните данни и нейното съответствие с изискванията в тази област (ОРЗД и/или ЗЗЛД);

– наличие/липса на уведомления за нарушения на сигурността на личните данни, настъпили при администратора/обработващия лични данни, когото номинираното длъжностно лице по защита на данните подпомага;

– наличие/липса на корективни мерки и/или наказания на администратора/обработващия лични данни когото номинираното длъжностно лице по защита на данните подпомага.

При спазване на вече установената институционална традиция, КЗЛД ще реализира и следните разяснителни мероприятия:

- Обявяване на студентски конкурс за есе на актуална тема, свързана с предизвикателствата пред защитата на личните данни. Съгласно вече утвърдената практика класираните на първо, второ и трето място да бъдат включени в програма на КЗЛД за платен стаж в Комисията.
- Открита приемна в КЗЛД за администратори на лични данни и граждани (13:00-15:00 ч., заседателна зала на КЗЛД).

Надяваме се, че ще се възползвате от предоставените възможности да се запознаете с нашите инициативи и да участвате в тях!

ЗАСЕДАНИЕ НА ЕВРОПЕЙСКИЯ КОМИТЕТ ПО ЗАЩИТА НА ДАННИТЕ

По време на пленарното си заседание през ноември Европейският комитет по защита на данните (ЕКЗД) прие доклад относно първия преглед на Рамката за защита на личните данни между ЕС и САЩ (DPF), както и изявление относно препоръките на групата на високо равнище относно достъпа до данни за ефективно правоприлагане.

ЕКЗД приветства усилията на органите на САЩ и Европейската комисия за прилагане на DPF и взема под внимание няколко събития, настъпили след приемането на решението относно адекватното ниво на защита през юли 2023 г.

По отношение на търговските аспекти, т.е. прилагането и изпълнението на изискванията, приложими за дружества, които са самостоятелно сертифицирани съгласно тази рамка, ЕКЗД отбелязва, че Министерството на търговията на САЩ е предприело всички съответни стъпки за прилагане на процеса на сертифициране. Това включва разработване на нов уебсайт, актуализиране на процедурите, ангажиране с дружествата и провеждане на дейности за повишаване на осведомеността.

Освен това механизмът за правна защита на физическите лица от ЕС беше приложен и от двете страни на Атлантическия океан. Бяха публикувани изчерпателни насоки за разглеждане на жалби. Въпреки това, малкият брой жалби, получени досега в рамките на DPF, подчертава необходимостта американските органи да предприемат активни мерки за наблюдение на съответствието на сертифицираните по DPF дружества със съществените принципи на Рамката.

ЕКЗД насърчава разработването на насоки от американските органи, които да изяснят изискванията за сертифицираните по DPF дружества при предаване на лични данни, получени от износители в ЕС. Особено ценни биха били насоки, свързани с обработката на данни за човешките ресурси. ЕКЗД изразява готовност да предостави обратна връзка по тези насоки.

По отношение на достъпа на публичните органи на САЩ до лични данни, предавани от ЕС на сертифицирани организации, ЕКЗД насочи вниманието си към ефективното прилагане на гаранциите, въведени с Указ 14086 в правната рамка на САЩ. Това включва принципите за необходимост и пропорционалност, както и новия механизъм за правна защита. Комитетът счита, че елементите на механизма за правна защита са налице, но същевременно призовава Европейската комисия да наблюдава практическото функциониране на тези гаранции, включително прилагането на принципите за необходимост и пропорционалност. ЕКЗД също така препоръчва Комисията да следи бъдещите развития, свързани със Закона за наблюдение на външното разузнаване на САЩ, като обръща специално внимание на разширения обхват на раздел 702 след повторното му одобрение от Конгреса на САЩ по-рано тази година.

Заместник-председателят на ЕКЗД Здравко Вукич заяви: „Радваме се, че след приемането на решението относно адекватното ниво на защита е постигнат напредък благодарение на ползотворното сътрудничество между органите на САЩ, Европейската комисия и ЕКЗД. В същото време все още има място за подобрение и следва да продължим да работим заедно, за да поддържаме високо равнище на защита на данните и да защитаваме правата и свободите на физическите лица от ЕС.“

И накрая, Комитетът препоръчва следващият преглед на решението относно адекватното ниво на защита на данните между ЕС и САЩ да се извърши в рамките на три години или по-малко.

В изявлението относно препоръките на Групата на високо равнище относно достъпа до данни за ефективно правоприлагане се подчертава, че основните права трябва да бъдат гарантирани, когато правоприлагащите органи имат достъп до личните данни на физическите лица. Въпреки че ЕКЗД подкрепя целта за ефективно правоприлагане, той посочва, че някои от препоръките на групата на високо равнище биха могли да доведат до сериозна намеса по отношение на основните права, по-специално зачитането на неприкосновеността на личния живот и семейния живот.

Макар че ЕКЗД отбелязва положително, че препоръката може да доведе до създаване на равнопоставени условия за запазване на данни, той счита, че едно широко и общо задължение за запазване на данни в електронна форма от всички доставчици на услуги би създало значителна намеса в правата на физическите лица. Поради това ЕКЗД пита дали това би отговаряло на изискванията за необходимост и пропорционалност на Хартата на основните права на ЕС и на съдебната практика на Съда на ЕС.

В своето изявление ЕКЗД подчертава също така, че препоръките относно криптирането не следва да възпрепятстват използването му или да отслабват ефективността на предоставяната от него защита. Например въвеждането на процес от страна на клиента, позволяващ отдалечен достъп до данни, преди те да бъдат криптирани и изпратени по комуникационен канал или след като бъдат дешифрирани при получателя, на практика би отслабило криптирането. Запазването на защитата и ефективността на криптирането е важно, за да се избегне отрицателното въздействие върху зачитането на личния живот и поверителността и да се гарантира, че свободата на изразяване и икономическият растеж, които зависят от надеждни технологии, са защитени.

По време на пленарно заседание през месец декември Европейският комитет по защита на данните (ЕКЗД) публикува насоки относно чл. 48 от ОРЗД относно предаването на данни на органи на трети държави и одобри нов Европейски печат за защита на данните.

ЕКЗД помага на организациите да оценяват исканията за предаване на данни от органи на трети държави.

В един силно взаимосвързан свят организациите получават искания от публични органи в други държави за споделяне на лични данни. Споделянето на данни може например да помогне за събиране на доказателства в случай на престъпление, за проверка на финансови транзакции или за одобряване на нови лекарства.

Когато европейска организация получи искане за предаване на данни от орган на „трета държава“ (т.е. неевропейски държави), тя трябва да спазва Общия регламент относно защитата на данните (ОРЗД). В своите насоки ЕКЗД разширява обхвата на чл. 48 от ОРЗД и пояснява как организациите могат най-добре да преценят при какви условия могат законно да отговорят на такива искания. По този начин насоките помагат на организациите да вземат решение дали могат законно да предават лични данни на органи на трети държави, когато бъдат помолени да направят това.

Съдебни решения или решения на органи на трети държави не могат автоматично да бъдат признавани или изпълнявани в Европа. Ако дадена организация отговори на искане за лични данни от

орган на трета държава, този поток от данни представлява предаване и се прилага ОРЗД. Международното споразумение може да предвижда както правно основание, така и основание за прехвърляне. В случай че няма международно споразумение или ако споразумението не предвижда подходящо правно основание или гаранции, могат да бъдат разгледани други правни основания или други основания за прехвърляне, при изключителни обстоятелства и за всеки отделен случай.

Насоките подлежат на обществена консултация до 27 януари 2025 г.

Комитетът също прие и становище, с което одобрява критериите за сертифициране на съответствието на марките по отношение на дейностите по обработване от страна на администраторите или обработващите лични данни. През септември 2023 г. Комитетът вече прие становище относно одобряването на националните критерии за сертифициране на съответствието на марките, което ги превръща в официално признати критерии за сертифициране в Нидерландия за обработване на данни от организациите. Одобрението на новото становище означава, че тези критерии вече ще се прилагат в цяла Европа и като европейски печат за защита на данните.

Европейският комитет по защита на данните (ЕКЗД) прие изявление по втория доклад на Европейската комисия относно прилагането на Общия регламент относно защитата на данните (ОРЗД).

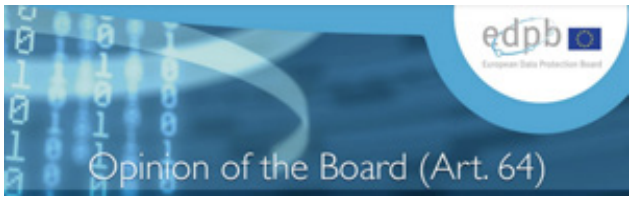
В изявлението си ЕКЗД приветства докладите на Европейската комисия и Агенцията за основните права.

Важно е да се отбележи, че ЕКЗД подчертава значението на правната сигурност и съгласуваността на законодателството в областта на цифровите технологии с ОРЗД и припомня някои от текущите си инициативи за изясняване на взаимодействието на ОРЗД в областта на правоприлагането със Законодателния акт за изкуствения интелект, стратегията на ЕС за данните и пакета за цифровите услуги.

Освен това ЕКЗД обявява, че ще увеличи производството на съдържание за неексперти, малки и средни предприятия (МСП) и други групи.

Накрая, Комитетът подчертава истинската необходимост от допълнителни финансови и човешки ресурси, за да се помогне на ОЗД и ЕКЗД да се справят с все по-сложни предизвикателства и допълнителни правомощия.

ЕКЗД ПРИЕ СТАНОВИЩЕ СЪС ЗАДЪЛЖИТЕЛЕН ХАРАКТЕР ПО ЧЛ. 64, ПАР. 2 ОРЗД ОТНОСНО МОДЕЛИТЕ ЗА ОБУЧЕНИЕ НА ИЗКУСТВЕН ИНТЕЛЕКТ



ЕКЗД прие становище със задължителен характер по чл. 64, пар. 2 ОРЗД относно моделите за обучение на изкуствен интелект

Европейският комитет по защита на данните (ЕКЗД) прие становище относно използването на лични данни за разработването и внедряването на модели на изкуствен интелект.

В настоящото становище се разглежда: 1) кога и как моделите с ИИ могат да се считат за анонимни, 2) дали и как легитимният интерес може да се използва като правно основание за разработване или използване на модели на ИИ и 3) какво се случва, ако модел на ИИ е разработен с използване на лични данни, които са били обработени незаконосъобразно. Разглежда се и използването на данни на първа и трета страна.

Становището беше поискано от ирландския орган за защита на данните (DPA) с цел постигане на хармонизация на нормативната уредба в цяла Европа. За да събере информация за настоящото становище, в което се разглеждат бързо развиващите се технологии, които имат важно въздействие върху обществото, ЕКЗД организира събитие за заинтересованите страни и проведе обмен с Европейската служба за ИИ.

Председателят на ЕКЗД, Талус, заяви: „Технологиите в областта на ИИ могат да донесат много възможности и ползи за различните отрасли и области на живота. Трябва да гарантираме, че тези иновации се осъществяват етично, безопасно и по начин, който е от полза за всички. ЕКЗД иска да подкрепи отговорните иновации в областта на ИИ, като гарантира, че личните данни са защитени и всичко се извършва при пълно спазване на Общия регламент относно защитата на данните.“

Що се отнася до анонимността, в становището се посочва, че органите по защита на данните (ОЗД) следва да преценяват дали даден модел на ИИ е анонимен за всеки отделен случай. За да бъде даден модел анонимен, следва да е много малко вероятно: (1) пряко или косвено да се идентифицират лицата, чиито данни са били използвани за създаването на модела, и (2) да се извличат такива лични данни от модела чрез запитвания. Становището предоставя незадължителен и неизчерпателен списък на методите за доказване на анонимност.

По отношение на легитимния интерес, в становището се съдържат общи съображения, които ОЗД следва да вземат предвид, когато преценяват дали легитимният интерес е подходящо правно основание за обработването на лични данни за разработването и внедряването на модели на ИИ.

Тест от три стъпки помага да се оцени използването на легитимния интерес като правно основание. ЕКЗД дава примери за разговорно средство (conversational agent) за подпомагане на потребителите, както и използването на ИИ за подобряване на киберсигурността. Тези услуги могат да бъдат от полза за физическите лица и могат да се позовават на легитимния интерес като правно основание, но само ако се докаже, че обработването е строго необходимо и се спазва баланс на правата.

Становището включва и редица критерии, които помагат на ОЗД да преценят дали физическите лица могат основателно да очакват определени употреби на техните лични данни. Тези критерии включват: дали личните данни са публично достъпни или не, естеството на връзката между физическото лице и администратора, естеството на услугата, контекстът, в който са събрани личните данни, източникът, от който са събрани данните, потенциалното по-нататъшно използване на модела и дали физическите лица действително са наясно, че личните им данни са онлайн.

Ако балансиращият тест покаже, че обработването не следва да се извършва поради отрицателното въздействие върху физическите лица, смекчаващите мерки могат да ограничат това отрицателно въздействие. Становището включва неизчерпателен списък с примери за такива смекчаващи мерки, които могат да бъдат от техническо естество, да улеснят упражняването на правата на физическите лица или да повишат прозрачността.

И накрая, ако даден модел на ИИ е разработен с незаконно обработени лични данни, това може да окаже въздействие върху законосъобразността на неговото внедряване, освен ако моделът не е надлежно анонимизиран.

Като се има предвид обхватът на искането на ирландския ОЗД, голямото разнообразие от модели на ИИ и тяхното бързо развитие, становището има за цел да предостави насоки относно

различни елементи, които могат да се използват за извършване на анализ на всеки отделен случай.

Освен това, ЕКЗД понастоящем разработва насоки, обхващащи по-специфични въпроси, кат например web scraping-а.

ЗАСЕДАНИЕ НА КОНСУЛТАТИВНИЯ КОМИТЕТ НА КОНВЕНЦИЯ 108

През ноември 2024 г. в Страсбург, Франция, се проведе 47-то заседание на Консултативния комитет на Конвенция 108 на Съвета на Европа за защита на лица при автоматизираната обработка на личните данни.

Сред основните акценти на заседанието бе напредъкът в подписването и ратифицирането на Конвенцията 108+, като Комитетът насърчи държавите да ускорят своите вътрешни законодателни процеси. Освен това бяха разгледани примерни договорни клаузи за предаване на данни, целящи улесняване на свободното движение на данни, като България представи своите усилия за популяризиране на приетия модел.

На заседанието бяха обсъдени актуализации по тълкуването на член 11 от модернизираната Конвенция 108, като делегациите бяха приканени да представят коментари и предложения за подобрения.

Друга ключова тема бяха проектите за насоки за защита на данните в контекста на невронауките. Значително внимание бе обърнато и на технологии за подобряване на поверителността (като синтетични данни и големи езикови модели), разгледани в контекста на подобряване на поверителността и защитата на личната информация. На заседанието бе избрано и ново ръководство на Комитета, което ще координира работата през следващия период.

ЗАСЕДАНИЕ НА КОМИТЕТА ЗА КООРДИНИРАН НАДЗОР

ККН е създаден в рамките на Европейския комитет за защита на данните (ЕКЗД) и представлява структура, чиято основна цел е да осигури координиран надзор над широкомащабните информационни системи, функциониращи на територията на ЕС, които се използват от органи, служби и агенции на ЕС в съответствие с член 62 от Регламент (ЕС) 2018/1725 или с друг правен акт на ЕС за създаване на конкретната система. В рамките на своята цел да осигури координиран надзор на широкомащабните системи и институции на ЕС, ККН: Обменя определена информация с институциите; подпомага надзорните

органи при извършване на одити и проверки; изготвя хармонизирани предложения за решения на проблемите и др.

В рамките на заседанието бе представено мобилното приложение „Пътуване към Европа“ (Travel to Europe), разработено от FRONTEX, което ще се ползва от граждани на трети страни извън ЕС.

За да се регистрират в приложението, пътниците ще трябва да заснемат пътните си документи, да направят снимка на лицето си и да попълнят кратък въпросник преди пристигането си на граничния контролно-пропускателен пункт. Снимката на лицето на пътуващия се верифицира спрямо образа, съхранен в чипа на паспорта.

Целта на доброволната предварителна регистрация в EES е да се намали времето за обработка на документите на границата, което е от полза както за националните органи, така и за пътниците. Тя не замества процедурите за граничен контрол, а има за цел да ги направи по-гладки и бързи.

Държавите членки ще бъдат администратори на лични данни, а FRONTEX – обработващи лични данни. FRONTEX няма да имат достъп до обработваните данни.

Повече информация можете да намерите на сайта на FRONTEX тук.

МЕЖДУВЕДОМСТВЕН КООРДИНАЦИОНЕН МЕХАНИЗЪМ КЪМ ОИСР

На 14 ноември 2024 г. в Министерството на външните работи се проведе редовно заседание на Междуведомствения координационен механизъм (МКМ) за присъединяването на България към ОИСР. В срещата участва делегация от дирекция „Правна“ на ОИСР, водена от координатора на процеса по разширяване на Организацията, г-жа Гита Котари.

Заместник-министър Мария Ангелиева, която ръководи заседанието, подчерта отличното взаимодействие между България и Секретариата на ОИСР. Тя заяви, че пълноправното членство в Организацията остава ключов национален приоритет, като през последните месеци българското правителство е работило активно и е засилило усилията си в този процес. Присъединяването към ОИСР не е само стратегическа цел, но и значим ангажимент за привеждане на българските политики и практики в съответствие с водещите международни стандарти. То цели постигането на по-висок стандарт на живот за гражданите и по-ефективно управление в икономическата, социалната и екологичната сфера.

Представителите на Секретариата на ОИСР представиха обобщение на постигнатия до момента напредък и изразиха готовност да подкрепят българските институции. Те също така разясниха предстоящите стъпки, необходими за постигането на пълноправно членство. Участниците в заседанието от страна на МКМ имаха възможност да зададат въпроси и да дадат обратна връзка относно процеса.

Делегацията на ОИСР е на двудневно посещение в България, като в рамките на визитата са планирани срещи на политическо и експертно ниво. Основната цел на тези срещи е да бъдат обсъдени в детайли напредъкът в процеса на присъединяване, предизвикателствата и следващите стъпки. Двете страни са обединени около амбицията техническите преговори да приключат до края на 2025 г., а България да стане пълноправен член на ОИСР през 2026 г

БЪЛГАРИЯ ИЗПОЛЗВА ВСИЧКИ ДОСТИЖЕНИЯ НА ШЕНГЕНСКОТО ПРОСТРАНСТВО

На 12 декември 2024 г. Съветът на Европейския съюз взе историческо решение, като одобри пълноправното членство на България и Румъния в Шенгенското пространство. Това означава, че от 1 януари 2025 г. ще бъдат премахнати граничните проверки по всички вътрешни граници – сухопътни, въздушни и морски – между тези две страни и останалите членки на Шенген.

Решението бе взето единодушно от вътрешните министри на държавите членки на ЕС по време на заседание в Брюксел. Унгарският вътрешен министър Шандор Пинтер, чиято страна председателстваше Съвета, заяви: "Това е исторически момент, в който най-накрая приветстваме България и Румъния в Шенген."

Присъединяването на България и Румъния към Шенген бе дългоочаквано, след като двете страни изпълниха техническите критерии още през 2010 г. Въпреки това, различни опасения, свързани с миграцията и сигурността, забавиха процеса. През последните години Австрия изразяваше резерви, но в навечерието на гласуването във Виена обявиха, че няма да наложат вето, след като България се съгласи да засили граничния контрол по границата си с Турция.

Пълноправното членство в Шенген носи значителни ползи за България. Премахването на граничния контрол ще улесни свободното движение на хора и стоки, което се очаква да стимулира икономическата активност и туризма. Освен това, българските граждани ще могат да пътуват без проверки по вътрешните граници на Шенгенското пространство, което ще улесни бизнес контактите и личните пътувания.

Въпреки тези предимства, България поема и отговорността да гарантира сигурността на външните граници на Шенген. Това включва засилен контрол и сътрудничество с други държави членки за предотвратяване на нелегалната миграция и трансграничната престъпност.

Решението за присъединяване на България и Румъния към Шенген бе приветствано от европейските институции и лидерите на двете страни. Те го определиха като важна стъпка към по-голяма интеграция и сътрудничество в рамките на Европейския съюз.

С това решение България затвърждава своето място в европейското семейство, като допринася за сигурността и стабилността на континента. Очаква се пълноправното членство в Шенген да донесе нови възможности и предизвикателства, които страната е готова да посрещне

УЧАСТИЕ НА КЗЛД В МИСИЯ ПО ОЦЕНКА ПО ШЕНГЕН

В периода от 10 до 15 ноември 2024 г. се проведе мисия за оценка по Шенген на Чешката република в областта на защитата на личните данни. Част от екипа на тази проверка бе представител на българския надзорен орган по защита на данните.

Оценката по Шенген в областта на защитата на личните данни се провежда на основание чл. 19 от Регламент (ЕС) 2022/922 от 9 юни 2022 година за създаването и функционирането на механизъм за оценка и наблюдение с цел проверка на прилагането на достиженията на правото от Шенген и за отмяна на Регламент (ЕС) 1053/2013. Проверката се извършва в съответствие програма, изготвена от страна на Европейската комисия и на оценяваната държава.

На проверки за оценка по Шенген подлежат държавите, които са членки на Шенген. Съществуват няколко вида оценки: периодична (включена е в многогодишната, както и в годишната програма за оценка), внезапна (не е включена в многогодишните и годишните програми за оценка, а целта е да се провери прилагането на достиженията на правото от Шенген от една или повече държави членки в една или повече области на политиката) и тематична оценка (включена е в годишната програма за оценка, като целта е да се осигури анализ на законодателството или практиките на държавите членки при прилагането на достиженията на правото от Шенген или на прилагането на определени части от тези достижения в няколко държави членки). Подлежащите на оценка области са: управление на външни граници, връщане, обща визова политика, полицейско сътрудничество, шенгенска информационна система и защита на личните данни.

В рамките на проверката на Чешката република, националният надзорен по защита на данните проведе редица срещи, насочени към оценка на структурите и процедурите, свързани с Шенгенската информационна система (ШИС) и Визовата информационна система (ВИС) в Чешката република. Първоначалната среща се проведе с националния надзорен орган по защита на личните данни в Чешката република. В хода на дискусиите бяха представени презентации, свързани със структурата, независимостта, бюджета и човешките ресурси на органа, както и неговите правомощия по надзора върху ШИС и ВИС. Освен това беше обсъдено повишаването на осведомеността и правата на физическите лица. На следващия ден екипът посети Полицейския президиум на Република Чехия. Бяха направени презентации относно организационната инфраструктура и мерките за защита на личните данни, свързани с ШИС и ВИС, както и презентации, свързани с Бюрото СИРЕНЕ. Длъжностното лице по защита на личните данни в полицията представи допълнителна информация за правната рамка, вътрешните правила и обученията, свързани с повишаване на осведомеността относно тези системи. Посещението включваше и международното летище в Прага, където бе демонстриран процесът на издаване на визи на границата. Екипът проведе среща с експерти на местно полицейско управление. Заключителната среща се проведе с представители на различни институции, като бе изготвен всеобхватен доклад за оценка на съответствието на Чешката република с изискванията на правото на Шенген. Докладът включва препоръки и заключения относно бъдещи подобрения, като всички документи са класифицирани съгласно изискванията на ЕС.

Оценката по Шенген приключва с проект на доклад, съдържащ информация, предоставена в рамките на мисията, както и заключения и препоръки на проверяващия екип. В последствие се изготвя един подробен доклад за оценка на приложението на достиженията на правото на Шенген във всички оценявани области.

Участието на представители на КЗЛД в мисиите за оценки по Шенген е предпоставка за споделяне на добри практики в областта на защитата на личните данни и възможност за повишаване на авторитета на институцията в областта на достиженията на правото от Шенген.

74-ата СРЕЩА НА МЕЖДУНАРОДНАТА РАБОТНА ГРУПА ПО ЗАЩИТА НА ДАННИТЕ В ТЕХНОЛОГИИТЕ

На 18-19 ноември 2024 г. Европейският надзорен орган по защита на данните (ЕНОЗД) беше съорганизатор на 74-ата среща на Международната работна група по защита на данните в технологиите. Известен също като Берлинската група, към която ЕНОЗД поема дългогодишен ангажимент. Този международен форум събира органи за защита на данните и експерти по защита на неприкосновеността на личния живот от целия свят, за да проучат последиците за защитата на данните от нововъзникващите технологии.

От създаването си през 1983 г. в Берлин, Германия, Групата и нейните членове разработват препоръки и насоки за защита на данните, за да развият стандартите за защита на личните данни в областта на технологиите и телекомуникациите. ЕНОЗД винаги е бил активен участник в екипа на този международен форум. Напоследък той има голям принос за издаването на работни документи, по-специално ЕНОЗД е съавтор на този за цифровата валута на централните банки (2024 г.).

Подготовката за нововъзникващите технологии на международно равнище е от ключово значение. Берлинската група създава условия за подкрепа на колективни и последователни глобални усилия, които целят извличане на ползите от технологичния напредък, управление на рисковете и защита на хората и техните права, включително личната неприкосновеност и защитата на данните. Техниките за прогнозиране, както и споделянето на знания и добри практики, са основополагащи за този процес.

За тази цел тази двудневна среща беше възможност за членовете на Берлинската група да споделят своите виждания, опит и предизвикателства относно еволюцията на технологиите и потенциално голямото им въздействие върху хората, като например невротехнологиите и разширената реалност.

Двудневната среща предостави възможност на членовете на Берлинската група да обменят виждания, опит и предизвикателства, свързани с развитието на технологиите и значителното им въздействие върху хората – като например невротехнологиите и разширената реалност.

По време на обсъжданията ЕНОЗД използва възможността да представи наскоро публикувания си TechSonar (докладите TechSonar са свързани с наблюдението на технологиите), акцентиращ върху различни технологии в областта на изкуствения интелект (ИИ), включително увеличено поколение, изкуствен интелект на устройството, мултимодален ИИ, машинно обучение и невро-символичния ИИ. Изследването за тази публикация потвърждава, че бързият напредък в ИИ, съчетан с висок потенциал за възвръщаемост на инвестициите, подхранва глобалната надпревара в областта, което може да доведе до значителни рискове за хората, ако не бъдат правилно управлявани.

Обща отговорност е да гарантираме, че човешкото достойнство остава в центъра при разработването на ИИ решения. Технологиите могат да разширят хоризонта, но защитата на правата и свободите на хората трябва да бъде водещ принцип.

ВТОРА МЕЖДУНАРОДНА СРЕЩА ПО ПРОЕКТ OPWHI

На 11 – 13 ноември 2024 г. се проведе втората международна среща по изпълнението на проект „OPWHI – Open the Whistle: Protecting Whistleblowers Through Transparency, Cooperation and Open Government Strategies“ по програма „Граждани, равенство, права и ценности“ на Европейския съюз.

В срещата взеха участие представители на организациите, участващи в проектния консорциум – Комисия за защита на личните данни, Асоциация „Прозрачност без граници“ – клон Испания, Центъра за изследване на демокрацията, Асоциация LiBERA – Италия, надзорния орган за борба с корупцията на Италия, университета в Пиза и службата за борба с измамите в Каталуня. Водещ партньор в проектния консорциум е Асоциацията „Прозрачност без граници“ – клон Испания.

По време на срещата се обсъдиха финансовото отчитане на изпълнението на проекта и осъществяването на комуникацията между партньорите в проектния консорциум, като сред основните теми бяха предстоящите през 2025 г. дейности.

През ноември 2024 г., КЗЛД и партньорите в консорциума, проведоха редица интервюта в България, Испания и Италия с представители на публичния и частния сектор с цел да се идентифицират нуждите в различните сфери и структури по отношение на защитата на лицата, подаващи сигнали или публично оповестяващи информация за нередности. През следващата календарна година ще бъдат завършени дейностите, залегнали в основата на проекта, пряко приложими, както за лицата подаващи сигнали за нередности и публично оповестяващи информация, така и за частния и публичния сектор при изпълнение на задълженията им в сферата и гарантирането на защитата на тези лица. Дейностите, които ще бъдат завършени, включват:

- Инструменти за почтеност в подаването на сигнали за нередности, по който в първата половина на 2025 г. предстои да бъде публикуван наръчник включващ, както разяснения, така и най-добри практики, които могат да бъдат заимствани от организациите в публичния и частния сектор в тяхната дейност в сферата на защитата на лицата, подаващи сигнали или публично оповестяващи информация за нарушения.
- Обучителни програми за специализирано обучение, включително подход за обучение на обучаващи, адаптиран за националните и регионалните органи, държавните служители и частните организации, участващи в прилагането на Директива (ЕС) 2019/1937. Тези обучения ще насърчават обмена на знания и опит, като помагат на органите и организациите да преразгледат, подобрят и адаптират своите процедури, за да включат най-добрите практики.
- Комуникационна кампания, в рамките на която ще бъдат адресирани нуждите на задължените лица по Директива (ЕС) 2019/1937 и по Закон за защита на лицата, подаващи сигнали или публично оповестяващи информация за нарушения. Кампанията ще има за цел, както да повиши осведомеността по темата и да предостави информация по дейностите на проекта, така и да предложи решения и най-добри практики за изграждане на вътрешни и външни комуникационни канали за организа организациите.

Съфинансирано от Европейския съюз

КЗЛД Е НОВИЯТ ПРЕДСЕДАТЕЛ НА ИЗПЪЛНИТЕЛНИЯ КОМИТЕТ НА ГЛОБАЛНАТА АСАМБЛЕЯ ПО ВЪПРОСИТЕ НА НЕПРИКОСНОВЕНОСТТА

На извънредно заседание на Изпълнителния комитет на Глобалната асамблея по въпросите на неприкосновеността, проведено на 20 декември 2024 г., бе взето единодушно решение Комисията за защита на личните данни (КЗЛД) да поеме председателството на Изпълнителния комитет на организацията. С този избор КЗЛД, нарежда България сред водещите държави, които играят ключова роля в управлението на защитата на данните, ставайки едва третият европейски председател на Асамблеята след надзорните органи на Франция и Германия от 1979 година насам. Повече от четири десетилетия международната Асамблея функционира като платформа за среща на лидерите в областта на защитата на личните данни. Това се постига чрез обединените усилия на организации от публичния и неправителствения сектор не само от Европа, но и от Азия, Африка, Австралия и Северна и Южна Америка – общо сто и петдесет акредитирани членове и близо четиридесет наблюдатели.

Комисията за защита на личните данни е единственият представител от държава-членка на Европейския съюз към настоящия момента в Изпълнителния комитет. В качеството си на председател, КЗЛД ще има възможността не само да определя дневния ред на Глобалната асамблея до края на октомври 2025 година, като ръководи заседания на Изпълнителния комитет, но и координира темите на закритата и откритата сесия на годишните издания на най-големия световен форум по защита на неприкосновеността на личния живот и личните данни.

Освен административните и организационни отговорности, председателството предоставя на КЗЛД възможността да представлява Асамблеята пред международни форуми, като същевременно насърчава глобалното сътрудничество в областта на защитата на данните и допринася за формирането на нови, глобални тенденции и политики в областта на неприкосновеността. В своето изказване, председателят на КЗЛД – г-н Венцислав Караджов, благодари за гласуваното персонално доверие и увери, че Комисията ще има ключова роля в развитието на стратегически инициативи, като обработването на лични данни чрез новите информационни технологии, включително системите с елементи на изкуствен интелект, в социалните медии, видеонаблюдението, невронауките и цифровото образование.

Този значим избор отразява активното участие и принос на КЗЛД в глобалните усилия за гарантиране на правото на неприкосновеност и защитата на личните данни.

РЕШЕНИЕ НА КЗЛД ПОТВЪРДЕНО ОТ ВАС

На свое редовно заседание, проведено на 06.07.2022 г., Комисията за защита на личните данни (КЗЛД) прие Решение № ПНМД-01-53/2022 г. по искане на „Топлофикация София“ ЕАД по чл. 106, ал. 1, т. 3 от Закона за гражданската регистрация (ЗГР). Решението на Комисията беше обжалвано пред АССГ, след което, с негово Решение № 741/01.02.2024 г., постановено по адм. дело № 7310/2022 г., беше

оставено в сила. Като касационна инстанция Върховният административен съд (ВАС), със свое Решение № 12677/22.11.2024 г. по адм. дело № 2862/2024 г., остави окончателно в сила решението на АССГ.

В своите мотиви решението на КЗЛД, както и съдебните решения, съдържат принципните разбирания относно предоставянето на данни от ЕСГРАОН, основанията, спазването на основните принципи за обработване на лични данни и съответствието с останалите изисквания на Регламент (ЕС) 2016/679. Посочената практика е от значение за дейността на доставчиците и на редица други услуги.

С решението си ВАС потвърди изводите на предходните инстанции, че искането на дружеството да бъде предоставен на „Топлофикация София“ ЕАД достъп до регистрите на ЕСГРАОН, не отговаря на изискванията на Регламент (ЕС) 2016/679 (GDPR) и представлява прекомерно и непропорционално обработване на лични данни. Съдът отбеляза, че обработването на лични данни може да бъде законосъобразно само ако отговаря на изискванията на чл. 6, § 1 от GDPR. В случая искането на „Топлофикация София“ ЕАД не отговаря на условията, определени в букви „б“, „в“ и „д“. В мотивите си ВАС подчерта, че предоставянето на достъп до регистрите би обхванало прекомерно широк кръг лица, включително такива, които не са клиенти на дружеството, което е несъвместимо с принципа на пропорционалност.

ВАС също така акцентира, че необходимостта от обработване на лични данни за изпълнение на задачи от обществен интерес не се покрива в настоящия случай, тъй като събирането на вземания на „Топлофикация София“ ЕАД не представлява обществен интерес, а по-скоро частен търговски интерес. Съдът отбеляза, че дружеството разполага с други механизми за набавяне на информация, като използване на процедурите, предвидени в Гражданския процесуален кодекс. В мотивите си ВАС изрази становище, че правото на защита на личните данни не е абсолютно и трябва да бъде съобразено с принципа на баланс между интересите на администратора и правата на субектите на данни. Липсата на доказателства за обществен интерес и легитимна цел, които да оправдаят искането, потвърждава правилността на отказа на КЗЛД и решението на АССГ.

ПРОВЕДЕ СЕ ЕВРОПЕЙСКИ WORKSHOP ПО РАЗГЛЕЖДАНЕ НА ЖАЛБИ В ЕСТОНИЯ

В периода 4 – 6 декември 2024 г. експерти на Комисията за защита на личните данни (КЗЛД) взеха участие в Европейски семинар за разглеждане на жалби от надзорните органи по защита на данните. Събитието се проведе в град Талин, Република Естония, и бе фокусирано върху обмена на добри практики и споделянето на казуси от надзорните органи.

В семинара участваха представители от 30 страни, сред които държави членки на Европейския съюз (ЕС) и Европейското икономическо пространство (ЕИО), както и Грузия, Косово и Украйна. В инициативата се включиха също представители на Европейския комитет за защита на данните (ЕКЗД) и Европейския надзорен орган по защита на данните (ЕНОЗД).

По време на семинара експертите на КЗЛД участваха активно в различни панели, сред които:

- Разглеждане на жалби относно камери в сгради в режим на етажна собственост.
- Изкуствен интелект и ролята на надзорните органи по защита на данните.
- Оценка на въздействието върху защитата на данните (DPIA): методи за оценяване, легитимен интерес и права на субектите на данни.
- Разглеждане на казуси с правна и фактическа сложност: социални медии, дефиниции за лични данни.
- Правоотношения между администратори и обработващи лични данни и договори между тях.

Семинарът предостави платформа за обмен на знания и опит между представителите на надзорните органи от различни европейски държави. Участниците обсъдиха иновативни подходи и общи предизвикателства, с които се сблъскват в своята практика при разглеждане на жалби и защита на правата на субектите на лични данни.

ПРЕСПЕКТИВИ ЗА ЦИФРОВАТА ИКОНОМИКА НА ОИСР 2024 . (ТОМ 2)

Инициативата потвърждава ангажимента на КЗЛД за активно участие в международното сътрудничество и за прилагане на най-добрите практики в защита на личните даннПерспективите на ОИСР за цифровата икономика (Том 2): Укрепване на свързаността, иновациите и доверието е водеща публикация, в която се анализират тенденциите в технологиите, цифровите политики и цифровите резултати в държавите членки на ОИСР и икономиките на партньорите.

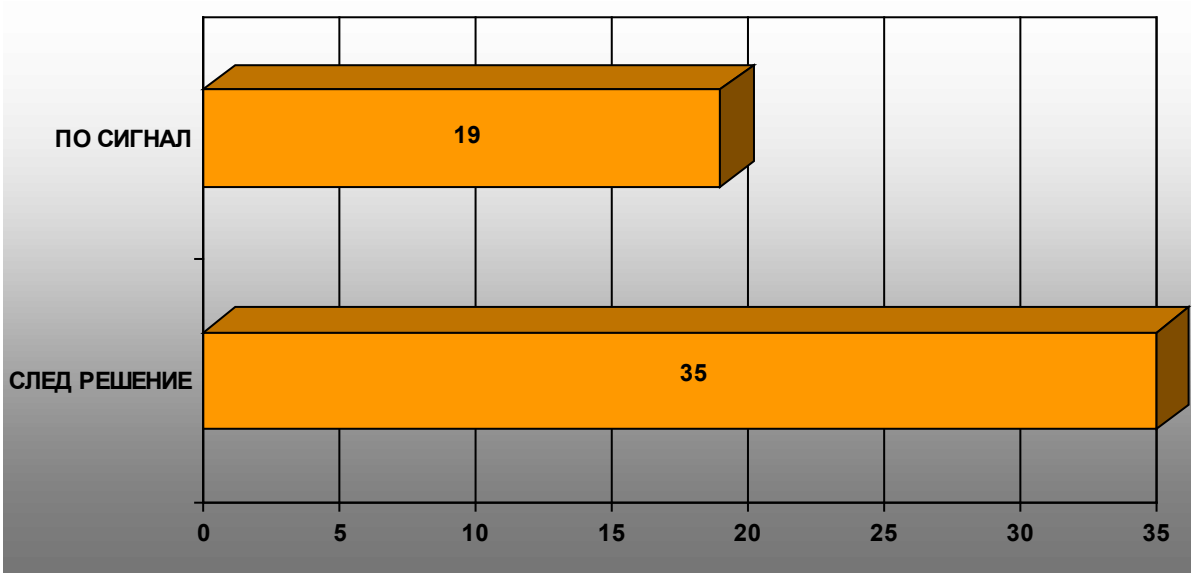
Бързите технологични промени характеризират най-новата фаза на цифровата трансформация, създавайки възможности и рискове за икономиката и обществото. В том 2 от перспективите на ОИСР за цифровата икономика за 2024 г. са разгледани нови аспекти в цифровите приоритети, политики и управление във всички държави. В него допълнително се анализират развитията във фондациите, които подкрепят цифровата трансформация, стимулират цифровите иновации и насърчават доверието в цифровата ера. Томът оценява тенденциите в достъпа и свързаността, както и уменията, необходими за успех в цифровата икономика и общество. Проучва се как цифровите технологии могат да разгърнат неизползвания потенциал на жените. Освен това се разглежда как технологичните иновации могат да допринесат за постигането на нулеви нетни емисии и как да опазим планетата.

Накрая, томът анализира развитието на цифровата сигурност, тенденциите в потреблението и доверието в медиите, отношението към неприкосновеността на личния живот и управлението на данни. Разглежда се също как допълнителният контекст влияе върху способността на хората да разпознават достоверна информация онлайн. Изданието завършва със статистическо приложение.

Целият доклад може да видите на следния линк: OECD Digital Economy Outlook 2024 (Volume 2).

СТАТИСТИКА И АНАЛИЗ НА КОНТРОЛНАТА ДЕЙНОСТ ЗА ПЕРИОДА НОЕМВРИ-ДЕКЕМВРИ 2024 Г.

На основание чл. 58, § 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета, през месеците ноември и декември 2024 г. са извършени общо 29 проверки – 14 след постъпили в КЗЛД сигнали и 15 след решение на КЗЛД.



Разгледани са 97 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 6 бр. Разпореждания и са отправени 4 бр. Предупреждения и 1 бр. Официално предупреждение. В отчетния период с решение на КЗЛД е наложена и 1 бр. Имуществена санкция.

ПРЕПОРЪКИ НА КЗЛД

ПРЕПОРЪКИ НА КЗЛД

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

Препоръки към администраторите на лични данни при възлагане на обработване на лични данни

При осъществяване на контролната си дейност и направени проверки на множество администратори на лични данни, КЗЛД е установила значителен брой на случаи на формален подход при дефиниране на условията за регламентиране на взаймоотношенията при възлагане на дейности на обработващи лични данни, съгласно изискванията чл.28 от Регламент (ЕС)2016/679. В тази връзка, на свое заседание на 18.12.2024г., Комисията прие "Препоръки към администраторите на лични данни при възлагане на обработване на лични данни".

Тези препоръки се основават на „Насоки 07/2020 относно понятията „администратор" и „обработващ лични данни" в ОРЗД" (Насоките) на Европейския комитет по защита на данните (ЕКЗД), налични тук. Насоките, които приема ЕКЗД, са задължителни за всички надзорни органи по защита на личните данни в ЕС и като такива се взимат изцяло предвид от Комисията за защита на личните данни (КЗЛД, комисията) при осъществяването на надзорната ѝ дейност. В този смисъл и администратор/и на лични данни (администратор/и) и обработващ/и лични данни (обработващ/и) следва добре да ги познават и да се съобразяват с изложените в тях принципни правила. С настоящите препоръки КЗЛД иска още веднъж да обърне специално внимание на някои конкретни акценти, които следва да се вземат пред вид, при възлагане на обработване на лични данни на обработващ/и лични данни.

Действия на администратора преди да избере обработващия.

1.1. В случаите, когато администратор реши да възложи обработването на лични данни на обработващ, той следва на първо място да направи преценка за това – кои лични данни, в какъв вид и обем ще се обработват от негово име. Това е от изключително значение, защото възлагането на операции по обработване на лични данни на обработващ, не освобождава по никакъв начин администратора от носенето на отговорността му по ОРЗД (чл.5, пар.2 от ОРЗД). Задължително е администраторът да извърши първоначален анализ на риска с оглед преценка на рисковете от предстоящото възлагане на обработването и съответно да вземе предвид резултата от този анализ при последващите си действия.

На този етап администраторът следва да определи границите на достъпа, който обработващият следва да има, като се изключи достъп до лични данни, обработвани от администратора, които не са свързани конкретно с предстоящото възлагане на обработване. Два са често използваните принципи в тази насока:

„необходимо е да знае“, като се предоставя достъп само до лични данни, от които обработващият има нужда, за да изпълни задълженията си;

„необходимо е да ползва“, когато се предоставя достъп само до средства за обработване на лични данни, от които обработващият има нужда, за да изпълнява задълженията си.

1.2. На следващо място администраторът трябва да направи оценка дали гаранциите, които обработващият предоставя, са достатъчни, за да се гарантира спазването на всички изисквания на ОРЗД. („„…администраторът използва само обработващи лични данни, които предоставят достатъчни гаранции…“ – чл. 28, пар. 1 от ОРЗД). Тази оценка на администратора по отношение на гаранциите е форма на оценка на риска, която в голяма степен зависи от вида обработване, което ще се възложи на обработващия. (пар. 96 от Насоките).

Администраторът следва да вземе предвид следните елементи (съображение 81 от ОРЗД и пар. 97 от Насоките), за да оцени дали гаранциите са достатъчни:

експертните познания на обработващия (напр. технически и експертен опит по отношение на мерките за сигурност и нарушенията на сигурността на данните);

надеждността на обработващия, вкл. репутацията, която има на пазара;

ресурсите на обработващия.

В допълнение, с оглед спазването на принципа за отчетност по чл.5, пар.2 от ОРЗД, администраторът следва да може да представи извършването на този анализ/оценка на риска и изводите от него, свързани с избора на обработващ.

Изпълнението на този етап (т.1.2) е постоянно задължение на администратора и следва на подходящи интервали от време да се извършва отново преценка на гаранциите на обработващия, вкл. чрез одити и проверки (чл. 28, пар. 3, б. “з“ от ОРЗД и пар. 99 от Насоките).

Действия на администратора преди сключване на договор с обработващия.

2.1. На този етап администраторът следва да се увери, че обработващият ще спазва изискванията за обработване на лични данни съгласно ОРЗД. Обработващият трябва да докаже по удовлетворителен за администратора начин (пар. 95 от Насоките), че ще прилага конкретни правила (политики) във връзка със сигурността на лични данни:

конкретно за категориите лични данни, които ще се обработват;

физическо местонахождение на регистрите (сървърите);

гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

начините на достъп и предоставяне на лични данни;

механизми за контрол, включително контрол на достъпа, мониторинг, докладване и одит;

изричен списък на служителите на обработващия, оторизирани за достъп или получаване на информация, вкл. декларации, че са поели ангажимент за поверителност (чл.28, пар.3, б. “б“ от ОРЗД);

процедури за управление на нарушения на сигурността на лични данни (уведомяване и сътрудничество за възстановяване след инцидент).

2.2. Важен момент тук е и конкретното уточняване на взаимоотношенията между администратора и обработващия:

ОЛД обработва лични данни само по документирано нареждане на администратора (чл.28, пар.3, б. “а“ от ОРЗД);

конкретно посочване на личните данни, които ще се обработват (естеството, обхвата, контекста и целите на обработването);

начинът на предоставяне на личните данни;

избор на подходящи технически и организационни мерки, за да може да се гарантира и докаже спазване на Регламент (ЕС) 2016/679 и ЗЗЛД (напр. псевдонимизация или криптиране на лични данни) – след анализ на рисковете (чл.28, пар.3, б. “в“ от ОРЗД);

водене на журнални записи (logs) на дейностите по обработване на данни в системите за автоматизирано обработване;

обучение на служители;

процеси и процедури за мониторинг на спазването на уговорените изисквания за сигурност на обработването;

нормативните изисквания за конкретното обработване и описание на това как се осигурява тяхното спазване;

условия и действия при промяна на договора;

задължения след прекратяване на договора – връщане, унищожаване, съхраняване;

преносимост – как и колко време се съхраняват данните след прехвърляне;

задължение за информираност на администратора, вкл. да го подпомага да отговори на искания за упражняване на правата на субектите на данни (чл.28, пар.3, б. “д“ от ОРЗД);

задължение за информираност и сътрудничество с надзорния орган;

действия при нарушения на сигурността, вкл. възстановяване на наличността на ЛД.

одити/проверки на обработващия (чл.28, пар.3, б. “з“ от ОРЗД);

основания за прекратяване на договора.

Необходимо е да се уточни и дали обработващият ще извършва обработването самостоятелно или ще използва и подизпълнители, за които следва да се прилагат всички посочени по-горе изисквания (чл.28, пар.3, б. “г“ от ОРЗД) Това може да се случи само след изрично предварително съгласие на администратора, защото и в този случай администраторът запазва главната си роля в обработването (пар.152 от Насоките).

2.3. При реализация на техническа услуга следва да се определи нивото на услугата (Service Level Agreement (SLA)), което да включва:

Описание на предоставяната услуга;
Канали за комуникация;
Ефективност/качество на услугата;
Обем на услугата – разработка, тест, производство и др.;
Наличност – времеви период и време за обслужване на отказ;
Архивираща политика;
Управление на промените;
Мерки за сигурност и нива на сигурност;
Инциденти и нарушения;
Мониторинг и одити;
Прекратяване на услугата;
Изтриване и унищожаване;
Санкции за неспазване на SLA;
Преглед на SLA.

Правно основание за уреждане на взаимоотношенията между администратор и обработващ – чл. 28 от ОРЗД.

Отношенията между администратор и обработващ, съгласно чл. 28, пар. 3 от ОРЗД, се уреждат „с договор или с друг правен акт съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни спрямо администратора, и който регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора.“. В него следва да се разпишат всички елементи, които са разгледани в т. 1 и т. 2 по-горе (пар. 100-160 от Насоките).

За изясняване на някои други аспекти от взаимоотношенията между администратор и обработващ, може да се ползват и „Становище 22/2024 относно определени задължения, произтичащи от използване на обработващ(и) и подобработващ(и)“ на ЕКЗД, налично тук и „Решение за изпълнение (ЕС) 2021/915 на Комисията от 4 юни 2021 година относно стандартни договорни клаузи между администратори и обработващи лични данни съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета и Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета“, налично тук

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

АВТОМАТИЗИРАНО ВЗЕМАНЕ НА РЕШЕНИЕ- ПРЕСЕЧНА ТОЧКА МЕЖДУ НОВИЯ РЕГЛАМЕНТ НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ И ОРЗД

ЖАНИН ФАХД АЛ-ШАРГАБИ, СТУДЕНТ V КУРС В СПЕЦИАЛНОСТ "ПРАВО" ЮРИДИЧЕСКИ ФАКУЛТЕТ, СОФИЙСКИ УНИВЕРСИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ".

Автоматизираното вземане на решения - пресечна точка между новия Регламент за изкуствен интелект и ОРЗД

1. Въведение

С развитието на новите технологии и нарастващото влияние на изкуствения интелект('ИИ'), общественото внимание все повече се фокусира върху възможните рискове, до които това ще доведе. Това кара и европейските законодателни органи също да се насочат към създаване на ясна законодателна уредба на изкуствения интелект, проявявайки се и като пионери на световно ниво в тази сфера. Не само бе приет Регламент (ЕС) 2024/1689,1 който създава общата рамка за създаването и оперирането на системи с ИИ в рамките на Съюза, ами предстои да се обсъдят и други значими законодателни инициативи, като тази за директива за извъндоговорната отговорност за вреди от системи с ИИ.2 Това показва далновидността на европейския законодател, но също така отваря вратата за по-строга регулация в рамките на много други юрисдикции.

В академичните среди вече се е наложил терминът 'Брюкселски ефект', именно покрай тенденцията други правни сфери да следват примера на Европа за регулиране на различни значими обществени отношения.3 Може да се наблюдава и известно саморегулиране от страна на частноправните субекти, отново под влиянието на европейските изисквания и желанието им да се развиват на този пазар безпроблемно. Това е ясно видимо в сферата на защита на личните данни, където в следствие на ОРЗД, темата за защита на неприкосновеността на данните до ден днешен продължава да расте по важност. Личните данни и тяхното значение не само станаха разпознаваеми в рамките на обществените дебати и дискусии, но и уредбата относно защитата им продължава да се детайлизира и усложнява спрямо нуждите на обществото.

Подобно развитие трябва да се очаква и като става дума за ИИ и мястото му в живота на гражданите на Съюза. Темата за регулацията на ИИ изглежда няма скоро да напусне полезрението на европейския законодател, а колкото повече се усложняват и по-често се имплементират системи с ИИ, толкова по-детайлна уредба ще бъде създадена. Тази тенденция неимоверно ще последва и в рамките на други юрисдикции.

1 Регламент (ЕС) 2024/1689 на Европейския парламент и на Съвета от 13 юни 2024 година за установяване на хармонизирани правила относно изкуствения интелект и за изменение на регламенти (ЕО) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и директиви 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828, PE/24/2024/REV/1, OB L, 2024/1689, 12.7.2024.

2 Proposal for a directive of the European Parliament and of the Council on adapting non- contractual civil liability rules to artificial intelligence (AI liability directive), COM(2022) 496 final 28.9.2022.

3 Bradford, A. "The Brussels effect", <https://scholarship.law.columbia.edu/faculty_scholarship/271>, последно посетено: 12 януари 2025.

По-интересен стои въпросът за пресечните точки между ИИ и защитата на личните данни. Както се вижда и в актовете на съюзния законодател, при регулирането на тези системи, особено внимание се обръща на влиянието им върху основните права и свободи на човека. Това показва детайлен поглед, който цели да постави ИИ и регулацията му в общата съюзна законодателна рамка и да осигури кохерентност между отделни законодателни актове и по-генералните приоритети на Съюза. С оглед на това трябва да се обърне особено внимание и как системите с ИИ се вписват с оглед защитата на лични данни.

Това е една пространна тема с множество рискове, несигурности и неуредени аспекти. Настоящата разработка цели да се фокусира върху едно тясно проявление на системите с ИИ, което подлежи на детайлна регулация и от страна на ОРЗД - автоматизираното вземане на решения. Все по-често гражданите на Съюза ще се сблъскват с това явление. Въвличането на усложнени алгоритми, които следва да улеснят вземането на решения, е неизбежно развитие в съвременните обществени отношения. На първо място, много бизнеси биха видели в това начин да спестят разходи, защото това би позволило намаляване на работната ръка.4 На второ място, това дава обещания и за съкращаване на времето, което различни операции изискват.5 На последно място и по-генерална полза не само с оглед на икономическите интереси на отделни лица, автоматизираното вземане на решения е приветствано от някои като начин да се избегнат предразсъдъците, които са присъщи на хората.6 В този смисъл, един алгоритъм, захранен с критерии, изглежда по-евтин, по-бърз и по-справедлив в преценката си от хората. Но автоматизираното вземане на решения крие и много рискове - от неясни решения, през риск от дискриминация до рискове за сигурността и злоупотребата с лични данни.7

ОРЗД има ясни правила относно автоматизираното вземане на решения, предвиждат се и определени механизми, които следва да бъдат възприети, за да се митигират потенциалните рискове. Но нарастващото влияние на ИИ би могло да създаде нови рискове и въпроси, затова е необходимо да се разгледа още веднъж действащата уредба, практиката около нея, както и новите законодателни решения, възприети в Регламента за ИИ. Тази разработка ще разгледа двата релевантни законодателни акта, след което ще обсъди съществуващите проблеми относно автоматизираното вземане на решения и полето за развитие на тази тема.

2. Обща уредба и обхват на двата правни акта

Основните актове, които регулират автоматизираното вземане на решения на европейско ниво са два - ОРЗД, който от няколко години предвижда конкретни изисквания към това явление, и от скоро и Регламента за ИИ, който също има разпоредби, влияещи на уредбата на този въпрос. Тъй като двата акта едновременно създават изисквания към автоматизираното вземане на решения, защитата на лични данни се пресича с регулацията на ИИ. За да може да се разбере по-добре взаимодействието на тези два правни режима, следва да се разгледа подробно действието и обхвата на тези два акта.

ОРЗД стъпва на предходни законодателни инициативи на съюзно ниво за регулиране на защитата на личните данни. Той влиза в сила през 2018 г. и има огромно влияние върху обществените отношения не само на общоевропейско, а и на световно ниво. Обхватът му е върху всички лица в рамките на ЕС, както и върху лица от Трети страни, в ясно определени случаи, където най-общо дейността им оказва влияние и в границите на Съюза.8 Успешното имплементиране на този регламент се базира на два фактора. На първо място, ОРЗД предвижда високи глоби за нарушения - те стигат до 20 милиона евро или 4% от глобалния годишен оборот, спрямо това кое е по-високо.9 Неимоверно подобни тежки санкции са силно ефективни при създаването на култура на съответствие с изискванията на ОРЗД. На второ място, обществената осъзнатост относно значението на защитата на лични данни също расте и създава обществен натиск върху икономическите оператори да спазват изискванията на регламента. Тези два фактора способстват успешното имплементиране на регламента и възможността практиката в сферата на защитата на лични данни да се разраства и детайлизира.

4 Mezina, N.A., Tikhonov, G.V. (2024). Automation of Decision-Making Processes: Opportunities and Risks, Russ. Engin. Res, 44, 400–404.
5 Пак там.
6 Пак там.
7 Пак там.

Регламентът за ИИ е иновативно постижение на европейския законодател с оглед липсата на предходни успешни инициативи за регулирането на ИИ. В този смисъл може да се каже, че това е един пръв по рода си акт. Това от своя страна би могло да доведе до много правни празноти, тъй като възможните рискове и притеснения в сферата на ИИ не само досега не са били регулирани, може въобще да не са били осъзнавани и дискутирани в детайли. Въпреки това този акт плод на продължителни обсъждания и консултации, като финалната му версия обхваща широк кръг системи с ИИ и адресира много от рисковете, които са били повдигани в рамките на академични дискусии, както и от представители на бизнеса и обществеността.

Регламентът за ИИ също има широк обхват - той засяга не само лица, разположени в рамките на ЕС, но отново и такива, които най-общо с дейността си оказват влияние и в границите на ЕС.10 В този смисъл полето му се припокрива с това на ОРЗД. Санкциите, които се предвиждат при неспазване на Регламента за ИИ също са изключително високи - могат да стигнат до 35 милиона евро или 7% от годишния глобален оборот.11 Тук е интересно да се направи сравнение с ОРЗД. От една страна, европейският законодател явно е осъзнал успеха, който подобни санкции имат, като стане на въпрос на имплементиране на законодателни рестрикции и задължения. От друга страна, това че предвидените санкции са дори по-високи, може да сочи към още по-голямата важност, която регулирането на ИИ има за ЕС.

3. Автоматизираното вземане на решения - същност и практика досега

Автоматизираното вземане на решения е явление, което ще продължава да се разраства. Причините за това вече бяха отбелязани с цел да се акцентира върху актуалността на дискутирания проблем. С оглед на това, доколкото изглежда безспорно значението на автоматизираното вземане на решения, по-трудно се оказва даването на ясна дефиниция за това какво представлява автоматизираното вземане на решения, както и изследването на правната му регулация.

На първо място, дефинирането на автоматизирано вземане на решения трудно би могло да се направи чрез описание на дейностите, които попадат под този термин. Дълго време като автоматизирано вземане на решение се е разбирало единствено използването на алгоритъм, който да извършва механична обработка на данни и да стига до крайни решения. Например ако се захрани алгоритъм с данни за финансовото състояние на лица, той да излезе с крайно решение кое от тях да получи одобрение за кредит и на кое да му бъде отказан такъв. С оглед на подобен прочит на явлението автоматизирано вземане на решения, много компании на пръв поглед са избягвали задълженията си да създадатмеханизми за митигиране на рискове, като са включвали човешки елемент някъде по веригата на вземане на решения. С оглед примера по-горе, това би изглеждало като служител, който да има крайна дума дали лице да получи кредит с оглед решението на алгоритъма.

В последната практика на СЕС обаче може да се види рязка промяна във възприятията относно автоматизираното вземане на решения и въпроса това какво обхваща. В делото SCHUFA,12 СЕС коментира това какво се разбира под ‘решение’. Оказва се, че дори на пръв поглед подготвителни действия, като създаването на оценка от страна на алгоритъм за потенциален кредитополучател, може да се счете за автоматизирано вземане на решения, ако тази оценка оказва значително влияние върху човекът, който в крайна сметка решава дали да отпусне кредит на съответното лице.

8 Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО, Член 3.

9 Пак там, Член 83.

10 Регламент (ЕС) 2024/1689, бел. 1, Член 2.

11 Пак там

Този подход следва да се разгледа като позитивно развитие в контекста на регулирането на автоматизираното вземане на решения. На първо място, то взима в предвид често повдиган проблем, дискутиран в академичните среди, когато става дума за системите с ИИ - предразсъдъкът към технологии.13 Този термин описва склонността на хората да се доверяват прекомерно много на решенията, дадени от система с ИИ, защото им е казано, че те се базират на обективни критерии, че има нисък риск от даване на грешка и т.н. С оглед на това, хората са по-малко склонни да са критични към решенията на системата с ИИ и често дори не биха ги поставили под въпрос. От друга страна, дори там където хората се съмняват в дадено решение на система с ИИ, те пак не са склонни да се противопоставят, защото не биха искали да носят отговорност, ако се окаже че оригиналното решение на системата с ИИ е било по-подходящо. Тези два фактора отслабват влиянието, което оказва крайната дума от страна на човек, в цялостния процес по вземане на решения, там където има оценки от системи с ИИ. В този смисъл, там където има оценки, давани от ИИ, дори да има човек, който взима крайното решение, често на практика се прилагат решенията на самата система с ИИ, без особени отклонения. В крайна сметка един механизъм за вземане на решения с привидно добавен човешки елемент не се различава особено от напълно автоматизиран механизъм. Затова съдът разумно отчита, че при решаващото влиение на оценките от ИИ, следва да се счита, че има автоматизирано вземане на решения.

На второ място, както и съдът сам отбелязва, подобен прочит създава повече гаранции за правата на индивидите. Там където оценките от системи с ИИ имат решаващо влияние върху крайните решения, следва да се приема, че има автоматизирано вземане на решения, за да могат индивидите, които са подложени на оценяването да се възползват изцяло от правата си да искат информация, да решават дали да бъдат подлагани на подобна система за вземане на решения и т.н.14

С оглед на това, много практики, особено във финансовия сектор, а и в други обществени сфери, ще се окаже, че попадат под регулацията на автоматизираното вземане на решения. Автоматизираното преглеждане и отхвърляне или оценяване на автобиографии при кандидатстване за работа, оценяването на потенциални кредитополучатели, оценяването на кандидати за университет или гимназия, оценяването на кандидати за социални помощи, това са малко от хипотезите, в които системи с ИИ може да бъдат използвани за оптимизиране на работния процес, те биха попаднали и под дефиницията на автоматизирано вземане на решения и биха подлежали на по-сериозен контрол с оглед на настоящото законодателство на ЕС.

В случай, че дейността на лице, което е задължено по ОРЗД, попада под дефиницията автоматизирано вземане на решения, то ще бъде в противоречие с чл. 22 от регламента, който забранява автоматизираното вземане на решения, които биха имали значително правно влияние върху субекта на данни.15 Изключенията за тази забрана са ограничени до необходимост за изпълнението на договорно задължение, изрично, информирано и свободно дадено съгласие, както и при овластяване за това от националното или съюзното законодателство.16 Както са отбелязвали вече автори, с оглед доктрината за съответстващ дизайн, тази забрана и уредбата ѝ трябва да бъдат вземани в предвид още при самото създаване и настройване на системи с ИИ, за да се осигури наистина пълно съответствие с европейските изисквания.

Второ ниво на регламентиране на автоматизираното вземане на решения може да бъде видяно и в самия Регламент за ИИ. На първо място, регламентът изрично забранява дадени дейности, които биха попаднали под разбирането за автоматизирано вземане на решения.

12 Judgment - 07/12/2023 - SCHUFA Holding (Scoring), Case C-634/21, ECLI:EU:C:2023:957.

13 Tewell, E. (2016). 'Toward the Resistant Reading of Information: Google, Resistant Spectatorship, and Critical Information Literacy', Johns Hopkins University Press, 16(2)

14 Judgment - 07/12/2023 - SCHUFA Holding (Scoring), Case C-634/21, ECLI:EU:C:2023:957.

15 Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО, Член 22

16 Пак там.

17 Artificial Intelligence and automated individual decision making, including profiling, under Art. 22 GDPR, <https://www.fieldfisher.com/en/insights/artificial-intelligence-and-automated-individual-decision-making>, последно посетено: 12 януари 2025.

Това ще обхваща системи с ИИ, които оценяват или класифицират индивиди или групи на база тяхното поведение или други характеристики и им поставят социална оценка, която може да доведе до неблагоприятно отношение или е несправедливо и диспропорционално.18 Подобни системи наподобяват сценарии от някои дистопични художествени произведения, но биха могли да станат реалност под автократичен режим на управление и европейския законодател далновидно ги е забранил изцяло. Следва да се отбележи, че подобна абстрактна дефиниция следва да бъде развита по-задълбочено с натрупването на повече практика и тълкувания на новото законодателство в сферата на ИИ. Интересно ще е да се види дали дадени граничи хипотези не биха попаднали тук, особено с нарастващата употреба на ИИ и от страна на самите държави членки. На второ място, системи с ИИ биха попаднали под дефиницията за високорискови, когато могат да навредят на лицата, особено с оглед на тяхното материално положение.19 Това би обхванало със сигурност системи с ИИ, които водят до автоматизирано вземане на решения във финансовия сектор. Класифицирането на системи с ИИ като високорискови би създало допълнителни задължения за прозрачност, осигуряване на високо ниво на киберсигурност, защита на данните, осигуряване на човешки надзор и т.н.20

Макар конкретните законодателни изисквания да не са обвързани дотолкова с темата за защита на личните данни, от интерес е наличието на пресечна точка между двата законодателни акта. Възможността лице да бъде подведено под отговорност под два акта със сурови санкции има потенциал да повиши още повече нивото на изпълнение на законодателните изисквания. На второ място, показва законодателен импулс да се обръща все повече внимание на рисковете от автоматизираното вземане на решения и да се митигират те преди да доведат до реални вреди за лицата. На трето място, създава възможност и за натрупване на повече практика относно това какво би било възприето като автоматизирано вземане на решения и как да се ограничат рисковете от него.

4. Нови проблеми с нарастващото влияние на изкуствения интелект

Когато става дума за автоматизираното вземане на решения от страна на системи с ИИ могат да се отбележат нови проблеми, които ще изискат нови решения, за да се ограничат рисковете от тях. На първо място, вече беше спомената нарастващата зависимост на хората от тези системи. Колкото по-разпространени са системите с ИИ иколкото повече се подобряват, ще намалява критичността на хората към тях. Това води до два основни проблема при автоматизираното вземане на решения. От една страна, хората стават по-склонни да споделят широк набор от данни с тези системи, без да имат достатъчно информация къде отиват тези данни, как се ползват, дали се споделят с трети лица, какви мерки са предприети за съхранението им, дали обработката е в съответствие с европейските изисквания и т.н. Това е особено опасно с оглед споделянето и на данни с по-особен статус, например данни относно здравословното състояние, расата, религията на лица и т.н., споделянето на които към системи с ИИ за оценяване и даване на решаващи заключения може да доведе и до дискриминация. От друга страна, зависимостта и доверието към системи с ИИ, както беше отбелязано, намалява и ефективността на човешката намеса, когато хората се окажат по-малко склонни да се намесват в решенията на тези системи и са безкритични към функционирането им. Този проблем изисква повече осведоменост към рисковете от ИИ. Решаването му се крие в осигуряването на повече информационни кампании, целенасочени осведомителни материали и други подобни инициативи. Вменяването на задължения към самите създатели и оператори на системи с ИИ да предоставят ясна и прозрачна информация за рисковете от техните системи също е от значение.

Друг проблем на системите с ИИ е така наречения ефект на черната кутия.21 Както беше отбелязано, при автоматизираното вземане на решения трябва да може да се предостави ясна информация на субектите на данни как се ползват техните данни и как се стига до крайните решения. Това е особено важно и там, където обработката на лични данни за автоматизираното вземане на решения става на основание изрично, свободно и информирано даване на съгласие.

18 Регламент (ЕС) 2024/1689, бел. 1 .
19 Пак там.
20 Пак там.

Това обаче се затруднява с трудната проследимост на резултатите, давани от ИИ. Често и самите оператори и създатели на подобни системи не са напълно наясно как те стигат до дадени решения и изводи. Самият механизъм на ИИ не способства пълно проследяване на неговите решения, като този проблем засега остава висящ. Тук следва да се спомене и въпросът за разпределяне на риска при вреда от системи с ИИ. В момента има висящи инициативи от страна на европейския законодател за уреждане на извъндоговорната отговорност за вреди от системи с ИИ.22 Подходът, който е взет, е създаване на презумпции за вина от страна на оператори иликолкото повече се подобряват, ще намалява критичността на хората към тях. Това води до два основни проблема при автоматизираното вземане на решения. От една страна, хората стават по-склонни да споделят широк набор от данни с тези системи, без да имат достатъчно информация къде отиват тези данни, как се ползват, дали се споделят с трети лица, какви мерки са предприети за съхранението им, дали обработката е в съответствие с европейските изисквания и т.н. Това е особено опасно с оглед споделянето и на данни с по-особен статус, например данни относно здравословното състояние, расата, религията на лица и т.н., споделянето на които към системи с ИИ за оценяване и даване на решаващи заключения може да доведе и до дискриминация. От друга страна, зависимостта и доверието към системи с ИИ, както беше отбелязано, намалява и ефективността на човешката намеса, когато хората се окажат по-малко склонни да се намесват в решенията на тези системи и са безкритични към функционирането им. Този проблем изисква повече осведоменост към рисковете от ИИ. Решаването му се крие в осигуряването на повече информационни кампании, целенасочени осведомителни материали и други подобни инициативи. Вменяването на задължения към самите създатели и оператори на системи с ИИ да предоставят ясна и прозрачна информация за рисковете от техните системи също е от значение.

На последно място, друг актуален риск, който създават системите с ИИ, е свързан със защитата на интелектуалната собственост.25 Тук съществуват два правни режима, които биха могли да влязат в противоречие. От една страна, създателите или ползвателите на системи с ИИ, които извършват автоматизирано вземане на решения, имат задължение да предоставят информация на субектите на данни относно това какви данни се събират, как се обработват, особено с оглед това как се вземат дадени решения. От друга страна, създателите на системи с ИИ може да се ползват със защита над информация, която се смята за търговска тайна или дори попада под по-строги режими на защита, сред които дори защита на патенти. Тук вече има разрешения в рамките на европейската юриспруденция. Като че ли е намерен баланс, където собствениците на системи с ИИ са задължени да споделят достатъчно информация за изграждане на представа как функционира алгоритъмът, без обаче да се споделят самите технически данни, за да се осигури все пак защита и на съответните икономически интереси.26 Подобни съображения са важни с оглед това Европа да не изостане на фона на други юрисдикции, които може би са по-активни в култивирането на иновации и технологично развитие. На пръв поглед, достигнатите решения успешно балансират обществените интереси с икономическите интереси на големите играчи в сферата на ИИ. Все пак следва да се следи развитието на практиката в тази сфера, а и частноправните субекти в противоречие. От една страна, създателите или ползвателите на системи с ИИ, които извършват автоматизирано вземане на решения, имат задължение да предоставят информация на субектите на на лични данн

21 Rawashdeh, S. 'AI's mysterious 'black box' problem, explained', <https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained>, последно посетено: 12 януари 2025.

22 Proposal for a directive of the European Parliament and of the Council on adapting non- contractual civil liability rules to artificial intelligence (AI liability directive), COM(2022) 496 final 28.9.2022.

23 Пак там. 24 Vellinga, N. E. (2024). Rethinking compensation in light of the development of AI. International Review of Law, Computers & Technology, 38(3), 391–412.

25 Caforio, V. & Paolluci, F. "The Rise of Automated Decision-Making and Its Legal Framework", <https://www.medialaws.eu/the-rise-of-automated-decision-making-and-its-legal-framework/>, последно посетено: 12 януари 2025.

26 Пак там.

5. Заключение

Автоматизираното вземане на решения не е ново явление, а е практика, която вече активно се ползва от редица сектори в рамките на ЕС. С нарастването на влиянието на системи с ИИ и потенциалните ползи, които те обещават, може да се очаква и бум в технологиите, базирани на автоматизираното вземане на решения. Това ще доведе и до усъвършенстване на тези системи. Също така би могло да доведе до много ползотворни нововъведения в рамките на обществения живот. Вече може да говорим за ИИ, който помага на шофьори да се движат по-безопасно по пътищата,27 за ИИ, който съпътства лекарските решения и води до по-таргетирана терапия на болести,28 както и много други полезни развития за обществото.

От друга страна, това създава и много нови рискове и би могло да доведе до вреди за субектите на лични данни. Съществуват и редица ограничения при този тип обработване на данни, които не бива да бъдат игнорирани, с оглед улеснение и спестяване на разходи.

Изглежда, че европейският законодател е наясно с рисковете от автоматизираното вземане на решения. Новият Регламент за ИИ също предвижда разпоредби, които засягат това явление. От друга страна СЕС също е по-активен в дефинирането и детайлизирането на изискванията по ОРЗД относно автоматизираното вземане на решения. Вероятно може да очакваме още практика по тези въпроси и дори по-строги изисквания към подобен тип дейност. Това предполага и по-активна и осъзната роля на националните надзорни органи в тази сфера, за да се осигури съответствие в отделните държави членки и равна защита на правата на субектите на лични данни, които засега може дори да не са наясно с рисковете, които крие бъдещето за тях.

27 Liu, Q., Li X., Yuan, S. & Li Z. “Decision-Making Technology for Autonomous Vehicles: Learning-Based Methods, Applications and Future Outlook”, IEEE International Intelligent Transportation Systems Conference, 2021.

28 Орманджиева, А. “Изкуственият интелект и персонализираната медицина”, <https://www.toest.bg/izkustveniyat-intelekt-i-personaliziranata-meditsina/>.

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

Информационен бюлетин № 1 (112) 2025 г.
Издава се съгласно чл. 10, ал. 3 от ЗЗЛД
Уеб сайт на КЗЛД: www.cpdp.bg
Разпространява се в електронен вид

ISSN 2367-7759