

2021 СПЕЦИАЛНО
ИЗДАНИЕ



3 ГОДИНИ GDPR

**БЪЛГАРСКИ
ПРОФЕСИОНАЛИСТИ
КОМЕНТИРАТ
ПРИЛАГАНЕТО НА GDPR**

ДАМЯН ТОДОРОВ

WWW.DAMYAN.TV



Предговор

ОТ ДАМЯН ТОДОРОВ,
АВТОР

Защитата на личните данни изживява възход след като от 25 май 2018 година започна прилагането на Регламент (ЕС) 2016/679 ("GDPR"). Натоварен с множество очаквания, регламентът промени завинаги отношението към личните данни в световен мащаб. Регламентът вдъхнови значими законодателни промени по целия свят, подтикна към технологични и социални брожения. За професионалистите по лични данни последните 3 години бяха изпълнени с надежди, предизвикателства, разочарования и трудности. Какво отговарят професионалистите на въпроси свързани приложението на Регламента?

В това специално издание са събрани мнения и впечатления на български професионалисти по защита на личните данни от различни индустрии с оглед отбелязването на 3 години приложение на GDPR.

ЗА АВТОРА

Дамян Тодоров е магистър по право, дипломиран от СУ "Св. Климент Охридски" и завършил магистърска програма LL.M Law & Technology в Tilburg University. Член на The International Association of Privacy Professionals (IAPP), притежава международния сертификат CIPP/E. Стреми се да допринесе за повишаване на нивото на защитата на личните данни в България чрез работата си в Асоциация на длъжностните лица по защита на данните.

*"Благодаря на всички,
които споделиха своя
опит и размисли за
тригодишния живот на
GDPR.*

*Искрено се надявам
настоящото издание да
допринесе за
утвърждаването на
защита на личните данни
в България като
индивидуално право и
общественозначима
ценност."*

*"Колкото повече научаваме от и за другите,
толкова по-добре разбираме реалността."*

Съдържание

АЛЕКСАНДРА АЙТОВА	03
АТАНАС ЙОРДАНОВ	04
ДЕНИЦА ПЕТКОВА	05
ДИМО ГОСПОДИНОВ	06
ЖУЛИЕТА МАНДАДЖИЕВА	07
ИВО ЕМАНУИЛОВ	08
ИРЕНА ГЕОРГИЕВА	09
КИРИЛ КАЛЕВ	10
МАРТИН ЗАХАРИЕВ	11
ЦВЕТИНА ЛУНГАРОВА	12



Александра Айтова

Александра Айтова се занимава професионално със защита на личните данни и информационната сигурност. Чувства се щастлива от това, което прави. Има страхотен екип и работи в една от най-големите финансови агенции в света.

За връзка:

<https://www.linkedin.com/in/alexandra-aytova/>

Кои са най-значителните промени в защитата на личните данни с оглед прилагането на Регламента?

На първо място това, че защитата на личните данни беше открито като самостоятелно основно право и заслужи своята висока степен на защита на европейско ниво.

На второ място - масовата осъзнатост, че чрез събирането, комбинирането и анализирането на личните данни, може в изключително висока степен на вероятност, да се направят относими изводи и предвидимост за нашето поведение в различни ситуации – било то като потребител, служител, гласоподавател и т.н.

Какви са най-големите предизвикателства пред професионалистите по защита на данните?

Едно от най-големите предизвикателства е свързано с Решението Шремс II, относимо към международния трансфер на лични данни.

Впечатление прави, че непосилният товар за оценяване на адекватността на държави от целия свят, се разпледели от Европейската комисия към специалистите по защита на личните данни, които, не разполагат с финансовия и човешки ресурс на Комисията, за да могат да обезпечат времево реализацията на даден проект. Въпреки това, досегът до индийски държавен вестник остава незабравимо преживяване.

Допълнителна трудност при оценяването на даден продукт или услуга представлява липсата на алтернативно решение, което да попада в териториалния обхват на адекватните държави. В същото време заплахата от глоба, за използването на глобален доставчик или услуга, остава реална.

Защо липсва единен подход на надзорните органи по множество въпроси с оглед приложението на Регламента?

На първо място защото културно-историческо-юридическите постановки на материята са оставили своя отпечатък в различните общества. Това води до различна интерпретация на един и същи въпрос от различните национални правни системи. Така например у нас трите имена на лицето, било то и уникални, не представляват лични данни. Логиката на национално ниво е, че единственият безспорен идентификатор у нас е ЕГН-то, защото чрез него може да бъде кумулирана неограничена информация за даден субект. Не така стоят нещата в Естония, защото там електронната ти идентичност, а не ЕГН-то ти те индивидуализират по несъмнен начин. Затова за България и Естония последиците от загуба на личната ти карта и потенциалът за кражба на идентичност не са еднакви, респективно въпросът не е третиран еднакво от надзорните органи на двете страни.

На второ място различията идват от дискрецията, която Регламента остави на отделните държави членки, по отношение на приложението му. В Испания например делото разпределено на един адвокат в адвокатска кантора, следва да бъде недостъпно от другите адвокати в кантората.

На трето място, значение оказват индивидуалните приоритети за всеки надзорен орган, които много се различават. За едни приоритет е AI и бисквитките, за други – информационна кампания що е лични данни.

На четвърто място разнообразието се определя от организационния подход. Типичен примен за това е Германия с множеството си независими надзорни органи.

Не на последно място, влияние оказва образователната подготовка по материята. Разнообразието е голямо – от държави без специализирано университетско обучение, до такива с идеи за междупланетарен трансфер на лични данни и изучаване на космически кибер-престъпления.



Атанас Йорданов

Атанас Йорданов, технологичен юрист завършил право в Софийския и Лайденския Университети. Специализира в Прайвъси и Защита на личните данни от края на 2016 на регионално (ЕС) и глобално ниво. Прайвъси Офицер за международна корпорация в автомобилния сектор от януари 2019.

Защо липсва единен подход на надзорните органи по множество въпроси с оглед приложението на Регламента?

За разликата в прилагането на GDPR има две основни причини. Първата е в различното разбиране на понятието за върховенство на закона в различните страни членове на ЕС както и на ЕИЗ. Има членове на ЕС, за които спазването на каквито и да било закони и то от всички правни субекти – частни лица и държавни органи, не е задължително и не се отразява в ежедневните им действия. В други членове на ЕС съществува разбирането, че правилата са на мястото си, за да направят живота на всички в обществото по-добър и законите се спазват масово – индивида спазва закона и очаква от околните да правят същото. Приложението на GDPR е до голяма степен резултат от тези по-общии за правото виждания в различните членове на Съюза.

Втората основна причина е различното ниво на залог в различните членове на Съюза. Ирландия например търпи сериозни критики за снизходителното си, граничещо със страхливо отношение по отношение на приложението на GDPR спрямо едни от най-големите дигитални бизнеси в света (Facebook, Google, etc.). Причината вероятно е големият икономически интерес, който Републиката има от това тези големи световни корпорации да останат и продължат да ръководят европейския си бизнес от тяхната държава. Различните национални интереси със сигурност водят до различно ниво на ентузиазъм колко бързо и ефективно и в какви размери да бъде приложен закона (GDPR в конкретния случай).

Какви са най-големите предизвикателства пред професионалистите по защита на данните?

GDPR променя начина, по който се гледа на личните данни на практика – от Американския модел където личните данни са корпоративна собственост към Европейския модел където личните данни са собственост на лицето, за което се отнасят. Самият модел не е нов за Европа, но завишените глоби и по-широкият спектър от правомощия за регулаторните органи в комбинация с практически глобалния териториален обхват на закона доведе до промяна в практиките на някои от най-големите дигитални компании. Например, Microsoft работят в насока за отделянето на европейската част от бизнеса си по такъв начин, че да се гарантира от правно-организационна и технологична перспектива невъзможността на специалните служби в САЩ и други държавни органи извън Европейската Икономическа Зона (ЕИЗ) да могат да принуждават компанията да предава европейски лични данни за масово наблюдение. Освен това, се стимулира преминаването и към по-малки, локални доставчици на услуги (добър пример е Германия).

Кои са най-значителните промени в защитата на личните данни с оглед прилагането на Регламента?

Най-значителните промени дойдоха с отсъждането по делото Шремс II – обявяването на споразумението между ЕС и САЩ за трансфера на лични данни за невалидно; потвърждаването на Стандартните Договорни Клаузи (СДК) за валиден механизъм за трансфер, но само при условие, че се удовлетвори изключително високият стандарт на GDPR. От формално-правна гледна точка това не е нещо ново – то винаги е стояло като правила в GDPR. Новото е това, че институциите на ЕС в лицето на Съда на ЕС, заявиха, че е крайно време да започне да се спазва законът такъв какъвто го е написал законодателят. Това създава сериозни предизвикателства пред всяка организация или лице, които биха искали да спазват правилата в тяхната цялост и до буквата на закона. Имам предвид фактическата обстановка на технологично и организационно ниво, в които се намират най-големите доставчици на дигитални услуги без които начинът на живот на човечеството през последните 10-15 години не би могъл да съществува. Например, ако изведнъж Google, Facebook, Microsoft, Amazon, Apple и други подобни престанат да предлагат каквито и да било услуги в ЕС, повечето електронни бизнеси и системи, включително и тези на държавните органи ще престанат да функционират.



Деница Петкова

Деница Петкова е юрист и Сертифициран експерт на Международната асоциация на професионалистите по защита на личните данни (IAPP), акредитирана към Американския национален институт по стандартизация (ANSI). Притежава сертификат за експерт по защита неприкосновеността на информацията за Европа (Certified Information Privacy Professional/ Europe (CIPP/E)), както и сертификат за мениджър по защита неприкосновеността на информацията (Certified information privacy manager (CIPM)).

Какво влияние оказва Регламентът върху социалния живот?

Неизменна част от съвременния социален живот са социалните медии като средство за социално общуване и за споделяне на съдържание онлайн. Регламентът промени правилата при използване на социалните медии, обемът на данни, които се предоставят и начинът, по който тези данни се обработват и съхраняват.

Всеки от нас оставя следа в интернет, в това число и като предоставя лични данни при използване на социални медии. Макар Регламентът да не се прилага по отношение на физически лица, които използват социални медии за лични цели, то той задължи организациите, които обработват лични данни, получени посредством използването на социални медии, да го прилагат стриктно.

Най-общо казано Регламентът предостави на субектите на данни контрол върху личните им данни и централизира регулаторната среда.

Какви са най-големите предизвикателства пред професионалистите по защита на данните?

Като едно от най-големите предизвикателства, пред които се изправят професионалистите по защита на данните през 2021г., бих открила нарастващия обем на заплахите за сигурността на данните. Дигиталната среда за обработване и съхраняване на данни, както и извършването на все повече дейности от разстояние в условията на пандемия увеличават възможностите за пробиви в сигурността. От професионалистите по защита на данните се изисква да отговорят адекватно на динамично променящите се предизвикателства. Това налага актуализиране и подобряване на процесите, процедурите и политиките, свързани с подsigуряване на сигурността на данните в дадена организация, налага професионалистите по защита на данните да бъдат „крачка пред“ потенциални бъдещи заплахи.

Какво промени в световен мащаб приложението на Регламента?

Приложението на Регламент 2016/679 промени цялостното разбиране на обществото и бизнеса в световен мащаб за значимостта и ценността на личните данни и необходимостта от осигуряване на тяхната защита.

От една страна Регламентът повлия на компаниите като промени начина, по който се организират бизнес процесите- отчита се все по-водещата роля на сигурността на данните, следи се за съответствие още на етапа на проектиране. От друга страна се стимулира значителното увеличаване на отделените от организациите средства за обезпечаване на съответствие с нормативните изисквания. Това в известна степен дава предимство на по-големите компании с възможности да отделят по-съществен времеви, човешки и финансов ресурс за осигуряване на съответствие и за киберсигурност.

Приложението на Регламента даде възможност за засилена защита на правата на субектите на данни, увеличи осведомеността на хората относно възможностите за упражняване и защита на правата им.

В световен мащаб Регламентът изигра ролята на катализатор, който задейства глобална вълна на създаване на регулации за защита на данните.



Димо Господинов

Димо Господинов е адвокат в София, основател и управляващ съдружник в Адвокатско дружество "Господинов и Генчев" (GGlaw). Член на IAPP и CIPP/E, CIPM, както и FIP. Автор на книгата „Privacy by Design – принципи, практики и технологии“. Специалист по електронни доказателства и колективни иски в гражданския процес.

Осъзнава ли обществото значението на личните данни и смисъла от защитата им с оглед прилагането на Регламента?

Краткият отговор е: не съвсем. Но, всъщност положението се е подобрило след началото на прилагането на Регламента, което, ако не друго, имаше много силен информационен ефект. Сега всеки поне е чувал за това, че личните данни са „новият петрол“ и че компаниите правят пари от тях. От друга страна, все повече хора усещат бремето от постоянното наблюдение и дигитална намеса в личния живот, на които са подложени в съвременното ни. Съответно вече по-ясно се осъзнава стойността на личните данни и ценността на „уединението“ (мой любим превод на „privacy“), които държавата и обществото чрез GDPR (и много други актове) са поели ангажимент да им осигурят.

Какви са най-големите предизвикателства пред специалистите по защита на данните?

Професионалистите по защита на данните са хора с различна професионална подготовка. Една част са юристи – като мен, и мога да кажа по наблюденията ми над колегите, че най-голямото им предизвикателство е необходимостта от техническо познание за дейностите и смисъла от обработката на лични данни. В резултат – постоянно се натъкваме на абсурдни решения, които затормозяват ненужно работата на задължените по GDPR лица.

Тъй както юристите, специализирани в търговското право, трябва да имат поне основни познания по икономика и бизнес, така и тези, които се занимават с дигитални правоотношения, трябва да разбират поне повърхностно от информационни технологии.

Кои са най-съществените недостатъци при приложението на Регламента?

Най-същественият недостатък е формализмът. Правилата на Регламента са предназначени най-вече да регулират съвременни дигитални отношения, но неговото прилагане бе посрещнато с добрия стар хартиен подход. Администраторите решиха, че с подписването на всевъзможни декларации и съгласия (често ненужни) са си свършили работата. А истински съществени въпроси като неоторизираното обработване, съхраняването на тонове ненужни лични данни и множеството рискове пред сигурността им бяха negliжирани.



Жулиета Мандажиева

Жулиета Мандажиева е адвокат и активист в областта на цифровите права. Има сертификат CIPP/e от IAPP, както и магистърска степен в областта на правото на компютрите, комуникациите и медиите от Университета Queen Mary в Лондон. Чест гост лектор е в рамките на различни обучения по въпросите на неприкосновеността на личния живот и личните данни.

Защо липсва единен подход на надзорните органи по множество въпроси с оглед приложението на Регламента?

Регламентът е единен правен акт, но практиките по държави са се формирали в продължение на почти четвърт век при действието на Директива 1995/46/ЕО и в контекста на различни административни и съдопроизводствени системи. Също така основен принцип на ЕС правото е този на отстъпления суверенитет, което допълнително дава голяма свобода на националните държави при упражняване на официалните правомощия на техните административни органи и практиката на съдилищата. Като се добавят и значително различаващите се правни традиции на държавите от Източна и Западна Европа и скандинавските държави, от една страна (т.нар. континентални правни системи) спрямо държави като Ирландия, например, разликите се задълбочават. Също така държавите членки имат значително разминаващи се интереси по отношение строгостта на прилагане на стандартите във връзка със защитата на личните данни – едни са съображенията в Германия и Франция, а съвсем в други в Ирландия, където повечето технологични компании са установени в рамките на ЕС. Сближаването ще настъпи под влияние на практиката на СЕС, но това ще отнеме време.

Кои осъществени нарушения на защитата на личните данни определяте като най-значими и защо?

За мен това са мащабните нарушения по отношение на правата на деца или други уязвими групи – например пациенти, хора с увреждания, социално слаби индивиди – този тип нарушения биха могли да имат поразяващ ефект върху субектите на данни предвид тяхната младост или неравностойно положение, в резултат на което да настъпят трайни или дори необратими последици. Още, считам, че с особено внимание трябва да се разглеждат и изследват причините при нарушения от страна на публични структури – като например допуснатият от НАП теч на лични данни. Причината е, че това показва неуважение на законността от страна на призиваните да я опазват институции като цяло – явление, което влиза в противоречие с принципа на правовата държава и опорочава стандартите за прилагане на законите, включително и от страна на частните субекти.

Кои технологии представляват най-голямо предизвикателство пред правилното прилагане на Регламента?

Определено подобно напрежение се чувства най-вече по отношение на технологиите на масово следене. Това проличава изключително ясно, ако вземем предвид многобройните съдебни дела пред Съда на ЕС, свързани с този феномен, срещу който съдилищата в ЕС упорито се съпротивляват, а службите неуморно пробват да прокарат под една ли друга форма. Един от най-пресните примери е опитът за възкресяване на отменените от Конституционния съд на България норми под претекста на пандемията от COVID-19 относно задържането и получаването на трафични данни от най-различни органи, включително МВР в ситуации, различни от непосредствена опасност от извършване на тежко престъпление. Следва да бъдат отбелязани специално и технологиите за лицево разпознаване, използвани на обществени места, както и профилирането на субекти на данни чрез работа с големи данни и изкуствен интелект – последното е особено притеснително предвид факта, че обичайно лицата и не подозират точността и всеобхватността на изводите, които могат да бъдат направени за тях на база анализ на на пръв поглед свършено тривиални данни.



Иво Емануилов

Иво Емануилов е научен сътрудник, програмист и юрист в Центъра по право на интелектуалната собственост и информационните технологии към KU Leuven. Докторант по право и компютърни науки в областта на авторските права върху компютърни програми и модели за машинно самообучение. Практикуващ юрист и изследовател от екипа на Фондация ЛИБРе (България).

Какво промени в световен мащаб приложението на Регламента?

Частично премахна разбирането на компаниите, че „произведеното съгласие“ (по Чомски) е легитимно основание за безконтролно и неограничено обработване на лични данни. Според мен пося и семената на културата на отчетност, макар и в много случаи да я виждаме реализирана в разрез с повелите на регламента, напр. като „отбелязване на кутийки“ или „публикуване на политика за защита на данните“. Често зад които не стоят реални процеси на отчетност, оценки на риска и мерки за неговото ограничаване. Регламентът обаче не успя значително да подобри „потребителското преживяване“ онлайн - все по-често се сблъскваме с незаконни „стени от бисквитки“, които изискват доста усилия, за да бъдат преодолені. В известен смисъл „произвеждането“ на съгласие онлайн стана дори по-агресивно и все още е за сметка на всички нас, като субекти на данни.

Кои са основните препоръки към субектите на данни при упражняването на правата им?

Намалете зависимостите си от централизирани онлайн услуги, предоставяни от големи американски, китайски и др. компании. Използвайте услуги, базирани на свободен софтуер с отворен код.

Използвайте анонимизиращи услуги, на които можете на имате доверие, напр. Tor, Private Internet Access и др. Не ползвайте „умни“ часовници и вещи - те обслужват единствено своите производители. Ползвайте криптография в кореспонденцията си. Упражнявайте правата, които регламентът ни предоставя - ако няма лесен начин да го направите, свържете се с надзорния си орган или потърсете помощ онлайн - общността на хората, които са ангажирани с тези въпроси, расте и винаги ще намерите подкрепа.

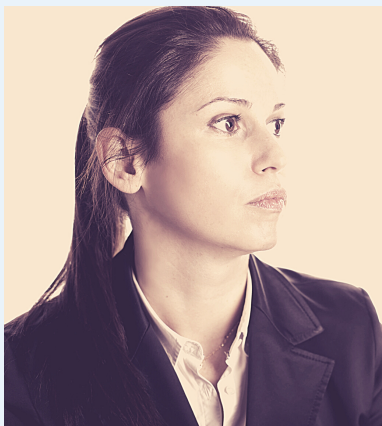
Кои са най-съществените недостатъци при приложението на Регламента?

Най-съществените недостатъци според мен се откриват по три линии.

Първата е липсата на единно интердисциплинарно разбиране за ключови понятия от регламента, като риск за правата и свободите на физическите лица, обхват и адресати на принципите за защита на данните на етапа на изготвяне и по подразбиране и др.

Втората е фрагментацията. От една страна, тя е в режима на прилагане на регламента и произтича от огромните различия във финансовия и човешки ресурс на надзорните органи в държавите-членки. Неизбежно това води и до различен интензитет, с който тези органи осъществяват правомощията си. Втората посока е свързана с „вратичките“, оставени в регламента по отношение на обработване на биометрични данни, както и данни в контекста на трудови правоотношения. С все по-широкото използване на технологии за лицево разпознаване, разпознаване на реч и с внедряването на индустриални колаборативни роботи в производствени предприятия, тези въпроси ще излязат на дневен ред в една силно фрагментирана регулаторна среда.

Третата линия е отговорност колкото на недостатъци (или свърхамбиции) на регламента, толкова и на практиката на Съда на ЕС. Тя се корени в това, което Надежда Пуртова нарече преди време превръщането на правния режим за защита на личните данни в „the law of everything“. Разбирането за това какви категории от данни са „лични“ е толкова широко, че е все по-трудно да се намерят категории от данни, които при определени условия не биха били „лични“ спрямо някого.



Ирена Георгиева

Д-р Ирена Георгиева адвокат, както и основател и управител на PPG Lawyers (ppglawyers.eu) – европейска бутикова кантора, специализирана в разрешаването на специфични регулаторни проблеми. Тя е сертифициран мениджър по поверителност на информацията (CIPM/IAPP). Притежава близо 15 годишна експертиза в областта на защитата на личните данни. Автор е на различни статии и разработки по тази материя и е чест лектор на обучения и семинари, посветени на нуждата от съответствие с правната рамка по защита на личните данни, както и осигуряването на информационна сигурност.

В какви насоки би следвало да се мисли за подобрене на Регламента?

Вече се натрупа не малка практика по приложението на Регламента, като съществуват и достатъчно насоки относно тълкуването на по-спорните му норми (както от страна на Европейският комитет по защита на данните (ЕКЗД), така и от отделните национални надзорни органи). На тази основа би следвало Регламентът да понесе промяна в посока подобряване на клаузите, които ясно да отразяват разбиранията на регулаторите. Така ще се избегне липсата на хармонизация в приложението му и ще бъдат улеснени администраторите, обработващи и субектите на данни, за да няма съмнение в начина на работа с Регламента.

Как виждате ролята на националните надзорни органи?

Националните органи трябва да са в максимална помощ на прилагащите Регламента. Намирам, че след като от администраторите и обработващите се изисква да предоставят информация за обработваните от тях данни в „разбираема и лесно достъпна форма“ (чл. 12 от Регламента),

то на още по-силно основание би следвало надзорните органи да предоставят подробна, ясна и недвусмислена информация на обществото относно приложимостта на нормите на Регламента и тяхната взаимовръзка със спецификите на националното законодателство.

Материята е доста трудна за асимилиране от задължените да се съобразяват с приложимото национално и европейско законодателство. Затова очаквам всеки надзорен орган да демонстрира максимална активност, както по отношение на контакт с други регулатори с цел уеднаквяване на практиката, така и по отношение на изграждането на връзка между обществото, прилагащите нормите и нас – консултантите. Само така ще може да се създаде единодействие в установяването на съответствие и да се намали напрежението от необятността на изискванията по Регламента.

Осъзнава ли обществото значението на личните данни и смисъла от защитата им с оглед прилагането на Регламента?

Тук е от особено значение да дефинираме терминът „общество“ или по-точно дали той се възприема глобално или обхваща гражданите и институциите на държавите-членки на ЕС, или още по-тясно – коментираме само обществото в България. Смятам, че разликата би била от съществено значение. На глобално ниво има държави, които все още се затрудняват в преценката кога и как да прилагат Регламента и кога той има преимущество над националните закони. В Европа голяма част от силните икономики (напр. Германия, Франция, Ирландия, Англия (дори и след Брекзит)) демонстрират сериозно отношение към материята и държат на изграждането на култура по защита на личните данни. Оценява се репутационния риск и риска от загуба на бизнес и партньори, а не само опасността от санкции. В България обществото е разделено много ясно на два противоположни лагера: Големите и средни предприятия (особено тези, които работят и с чужди инвеститори или клиенти) като цяло оценяват необходимостта от организирани действия по опазване на личните данни и осигуряване на информационна сигурност. Създават се политики, които ясно показват симбиозата между техническо и правно обезпечаване на съответствието. Малките предприятия и стартап компаниите обратно – намират Регламента за сериозна пречка и свръхрегулиране на бизнеса, за тях мерките създават единствено разходи и те все още не могат да провидят положителните страни на тази регулация.



Кирил Калев

Кирил Калев се занимава със защита на лични данни от 2014-а година. Завършил е „Право“ в Софийския университет и „Право и технологии“ в Тилбургския университет (Холандия), а понастоящем следва „Киберсигурност“ в Нов български университет. Работи като Мениджър защита на личните данни в Paysafe, съпредседател е на българското KnowledgeNet подразделение на International Association of Privacy Professionals (IAPP).

В какви насоки би следвало да се мисли за подобрене на Регламента?

По мое мнение един от най-явните недостатъци на Регламента, който се откри в последните три години, е твърде честото упражняване на правата на субектите с цел, различна от заложената от законодателя – предоставяне на прозрачност при обработването на лични данни. Въпреки че в Регламента формално са включени механизми против подобни злоупотреби, на практика те не се оказват напълно ефективни и субектите на данни нерядко използват правата си по Глава III единствено за да създадат допълнителна работа и други неудобства за администратора на лични данни. За щастие, вече има съдебна практика, която тълкува закона в посока за преодоляване на някои от тези проблеми. Надявам се, че тази тенденция ще продължи да се развива в правилно направление, за да могат правата на субектите на данни да останат реално защитени в пълна степен без това обаче да се изразжда в злоупотреба с тях и използването им за цели, които са в разрез с духа на Регламента.

Защо липсва единен подход на надзорните органи по множество въпроси с оглед приложението на Регламента?

Макар че въвеждането на Регламента определено беше уместна стъпка в посока на преодоляване на фрагментацията в сферата на защитата на личните данни в рамките на Европейския съюз, е факт, че крайната цел за пълна хармонизация при правоприлагането все още не е постигната. Въпреки сходствата спецификите на правните традиции в отделните държави-членки обуславят и редица различия. Вярвам обаче, че те могат да бъдат постепенно преодоляни, като в този смисъл смятам, че умишленото оставяне на поле за локална интерпретация в определени разумни граници, заложено в Регламента, не е погрешен подход, а напротив – правилна крачка в процеса на сближаване, което като крайна цел ще бъде постигнато в определен момент с достатъчно търпение и целенасочени усилия.

Кои технологии представляват най-голямо предизвикателство пред правилното прилагане на Регламента?

Редица модерни технологии навлизат все по-широко в масова употреба, като голяма част от тях поставят нови трудности за разрешаване задачи пред специалистите в сферата на защитата на личните данни. Като конкретна такава технология бих открил използването на изкуствен интелект (AI), включително и в частност машинното самообучение (machine learning). Когато такива видове обработване се извършват по отношение на биометрични лични данни, предизвикателствата стават още по-големи. В повечето случаи внедряването на подобни технологии се прави с цел подобрене на съществуващи практики, например чрез оптимизиране на използването на корпоративните ресурси посредством автоматизация на съществуващите процеси. Но колкото по-огромен обем от данни използват, толкова по-ефективни са тези технологии. От тази гледна точка е напълно разбираемо защо има засилващ се бизнес интерес от въвеждането им, но тази тяхна характеристика обуславя и необходимостта от още по-внимателна оценка на въздействието им върху правата на субектите на данни. Въпреки предизвикателствата мисля, че възприетият в Регламента подход на технологична неутралност за момента дава добри резултати, постигайки разумен баланс между благоприятна за бизнес развитието регулация на технологичните иновации, от една страна, и защитата на правата на субектите на данни, от друга страна.



Мартин Захариев

Доц. д-р Мартин Захариев е старши адвокат в една от водещите адвокатски кантори в България – „Димитров, Петров и Ко.“ и старши правен експерт във Фондация „Право и интернет“. Специализира в областта на защитата на личните данни, трудовото право, международния арбитраж, регулацията във фармацевтичния сектор и правото на интелектуалната собственост. Автор е на две монографии, учебник и множество статии и анализи в областта на личните данни. Преподава различни дисциплини в областта на правото на ИКТ в УниБИТ и СУ „Св. Климент Охридски“.

Осъзнава ли обществото значението на личните данни и смисъла от защитата им с оглед прилагането на Регламента?

Осъзнаването на значението и смисъла на правилата за защита на личните данни е бавен и труден процес. Много хора виждат в правилата свръхрегулация – поредния административен режим, който хаби ненужни финансов и човешки ресурс в организациите. Но все повече хора постепенно осъзнават важността на този режим и неговата основна функция – да защитава основните права и свободи на хората и да бъде гарант за човешкото достойнство в свят на „умни“ машини и автоматизация, които преобразяват живота ни.

Често срещано е и погрешното разбиране, че личните данни трябва да бъдат държани в тайна и че събирането и обработването им по друг начин трябва да е забранено, за да бъдат данните „защитени“. Това не е така, обществото и бизнесът функционират чрез обмена на лични данни, но това не трябва да става безконтролно, а при спазването на определени правила, гаранции и отчетност.

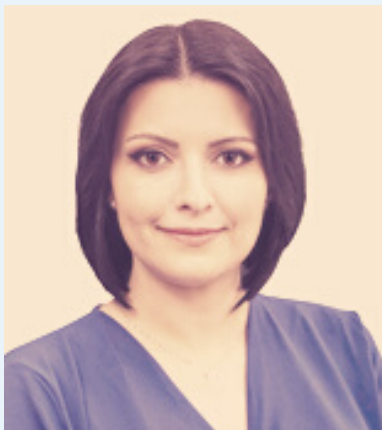
Какво влияние оказва Регламентът върху социалния живот?

GDPR промени съществено социалния живот, доколкото с острота постави въпроса за неприкосновеността на личната сфера и защитата на основните права на хората в един технологичен свят, в който всички социални и бизнес процеси се основават на събирането и обработването на все повече лична информация. Най-същественият принос на GDPR е, че чувствителността на тема защита на личните данни в обществото се засили и много хора започнаха да обръщат внимание на това кой и защо иска техните данни, както и да търсят защита на правата си.

Какви са най-големите предизвикателства пред професионалистите по защита на данните?

Най-голямото предизвикателство пред нас – професионалистите, практикуващи в сферата на защитата на личните данни, е необходимостта да комбинираме знания от множество материи. За да се внедрят ефективно правилата за защита на данните в дадена организация, трябва да познаваме както общата правна рамка на европейско и национално ниво, така и специфичните секторни регулации, приложими към дейността на различните администратори (застрахователи, банки, фармацевтичен сектор, електронни магазини, интернет търсачки и много други). В допълнение, нужно е и определено ниво на техническа експертиза, за да се вникне в процесите по обработване и да се направи правен анализ за съответствие на технологиите с правилата за защита на данните.

Нещо повече, в някои случаи при стартъпи, предлагащи иновативни услуги, действащата регулация не дава отговор на някои от въпросите, които дейността им поставя. Тогава е необходима внимателна преценка и балансиране на рисковете какво може да се регулира в светлината на действащите правила и къде може да възникне потенциален проблем във връзка с обработването на данните – респ. колко целесъобразно е да се поеме и ограничи даден риск. Нерядко тази преценка излиза извън чисто правния съвет, а предполага даването на препоръки за вземането на бизнес и организационни решения, стратегическо планиране и др. под.



Цветина Лунгарова

Цветина Лунгарова е специалист по защита на данните с квалификации по право, икономика и масови комуникации. Има опит като програмен мениджър за югоизточна Европа в известна международна компания, а от 2020г. започва частна практика. Цветина е хоноруван преподавател в СУ и работи върху дисертационен труд „Реструктуриране на бизнес процесите в малки и средни предприятия в България според Общия регламент за защита на данните в условията на Индустрия 4.0“.

Осъзнава ли обществото значението на личните данни и смисъла от защитата им с оглед прилагането на Регламента?

„Значението“ е субективно понятие. Поставям акцент върху икономическите аспекти на този въпрос и по отношение на тях считам, че не. На първо място обаче обществото трябва да разполага с подходяща информация, а засега медиите не му я предлагат. Единици са тези, извън професионалния кръг, които са запознати с решението на съда на ЕС от миналата година относно трансферите на данни към трети страни и по-конкретно към САЩ, известно като „Шремс 2“. То има съществено влияние върху бизнеса и повдига редица въпроси за политическата отговорност на европейско ниво, която следва да бъде ангажирана. В същото време самото ни общество е специфично с това, че е посттоталитарно и по тази причина няма чувствителност по темата до степен, че дори не я разпознава.

Какви са най-големите предизвикателства пред професионалистите по защита на данните?

Въпросът за значението на регламента ме навежда и към темата за предизвикателствата пред професионалистите по защита на данните в смисъл, че осъзнаването в масов план е първият и най-съществен проблем за нас. На този етап сме изправени пред това да обясняваме абстрактни концепции (защото така звучи) предимно на бизнеса. Бизнесът от своя страна, поради практичната си природа, ги определя в своето планиране като проблеми, заплахи, административна тежест, разходи и т.н. и много, много рядко е склонен да ги види като възможност. Също така, традиционно, подобен тип въпроси са разрешавани чрез механично произвеждане на документация, която се оставя да отлежава по папките и с това усилието се изчерпва. GDPR е различен точно с това, че не е т.нар. „хартиен тигър“ и спрямо него описаният подход не работи, а е необходимо защитата на личните данни да бъде интегрирана във всички бизнес процеси. Никой не се радва да научи това. В този смисъл наличието ни само по себе си не „решава проблема“ и се оказва генератор на задачи, които често се възприемат като „излишни“.

Кои технологии представляват най-голямо предизвикателство пред правилното прилагане на Регламента?

От гледна точка на взаимоотношенията между икономическите субекти, според мен това са всички вариации на софтуер или платформа като услуга (SaaS и PaaS), заради текущо доминантната им позиция спрямо малките и средни предприятия, а дори и спрямо големите корпорации. Налице е безпрецедентна зависимост от този тип доставчици, защото дигиталната среда предполага интензивното използване на такива услуги. В резултат от това съответните доставчици се оказват в доминантна роля спрямо своите клиенти и в собствения си отказ да се съобразят с правилата принуждават всички останали по веригата да рискуват. Към настоящия момент рискът от глоба се оказва по-приемлив за фирмите спрямо сигурната загуба на конкурентоспособност (която би настъпила, ако не се възползват от съответните типове услуги). Ключова роля това да се промени имат от една страна органите по защита на данните, които трябва да прилагат ефективно законодателството; специалистите, които трябва да подпомагат бизнеса в намиране на ефективни решения; бизнесът, който следва да прояви корпоративна социална отговорност и държавата – чрез подходящи стратегии за повишаване на общата компетентност на гражданите по тези въпроси. Всичко това ме връща към първия въпрос – за осъзнаването.

"If you have knowledge,
let others light their candles in it."
– *Margaret Fuller*

СПЕЦИАЛНО ИЗДАНИЕ

За обратна връзка:
3gdpr@damyan.tv

3 ГОДИНИ GDPR

БЪЛГАРСКИ ПРОФЕСИОНАЛИСТИ КОМЕНТИРАТ ПРИЛАГАНЕТО НА GDPR

ДАМЯН ТОДОРОВ
WWW.DAMYAN.TV

Всички права запазени © 2021 Дамян Тодоров

Изложените мнения и становища не отразяват
гледната точка на автора и той не носи
отговорност за тях.

Всички права върху отделни текстове и
изображения принадлежат на техните автори.

Изданието се рапространява безплатно и само в
електронна форма.

При споделяне/разпространение на изданието в
Интернет, посочването на първоизточника
www.damyan.tv е задължително.