„Предизвикателства пред индустриалния растеж в България“, сборник от конференцията, 2018, стр. 280-288

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ В СЪОТВЕТСТВИЕ С РЕГЛАМЕНТ (ЕС) 2016/679 (GDPR)

Автор: Петя Биолчева[1] , Георги Средков[2]

Резюме

Въвеждането на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета е сред най -значителните промени в европейското законодателство през последните две десетилетия. Поддържането на съответствие с него е важна задача за всички администратори на личи данни в ЕС. Важна част от защитата на лични данни се отдава на оценката на въздействието за сигурността на данните. Настоящият доклад илюстрира как може да бъде извършена спомената оценка на базата на два утвърдени метода и вяжданията на българският регулативен орган.

Ключови думи: *GDPR, Управление на риска, Методи за оценка на въздействието, Лични данни*

1. Въведение

С приемането на 27 април 2016 г. на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (по-известен като GDPR) относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, на всички страни, членки на Европейския съюз бе даден

[1] *гл. ас. д-р Петя Биолчева ,УНСС, Катедра Индустриален бизнес, p.biolcheva@unwe.bg*

[2] *Георги Средков; Information Consulting Office Ltd, office@icobg.eu*

Електронно копие налично на: http://www.industrialgrowth.eu/wp-content/uploads/2018/11/29.pdf

двугодишен период за адаптиране към неговите изисквания. Сега, след влизането му в сила на 25 май 2018 година, се налага прилагането на новия комплексен набор от правила за защита на личните данни. Важна част от защитата на личните данни заема т.нар. „оценка на въздействието“. Тя е свързана с необходимостта да се вземат адекватни мерки по отношение на управлението на риска свързан със защитата на лични данни.

Оценката на въздействието върху личните данни представлява процес, чиято цел е да опише обработването, да оцени неговата необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработването на лични данни, като ги оцени и определи мерки за справяне с тези рискове. Тази оценка е важен инструмент за отчетност, тъй като помага на администраторите на лични данни не само да спазят изискванията на регламента, но и да демонстрират, че са предприети подходящи мерки за защита на данните.

В GDPR оценката на въздействието е засегната в няколко основания (75,84,91) и членове (35,36). Основание 75 обръща внимание на видовете последици, които могат да се проявят в следствие на обработването на лични данни, а именно: материални или нематериални вреди в следствие на дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация, или други значителни икономически или социални неблагоприятни последствия; или когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни; когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили; когато се обработват лични данни на уязвими лица, по-специално на деца; или когато обработването включва голям обем лични данни и засяга голям брой субекти на данни.[3] От основанието изпъква многоаспекността на гамата от рискови проявления на обработката на лични данни, което е и основание за необходимостта от управление на този риск.

На следващо място оценката на въздействието е засегнато и в Основание 84. Тук се акцентира по-скоро върху необходимостта от изготвяне на оценката на риска по-специално: произходът, естеството, спецификата и степента на риск. Резултатите от

[3] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, основание 75

оценката следва да бъдат взети предвид, когато се определят съответните мерки, за да се докаже, че обработването на лични данни отговаря на изискванията на регламента.[4]

За осъществяване на процеса по оценка на въздействието е необходимо да се определи кога всъщност е нужно да не извърши тя. Според нормативната уредба на Регламент 2016/679, оценка на въздействието се извършва в случаите, когато съществува вероятност обработването на лични данни „да породи висок риск за правата и свободите на физическите лица“.[5] Този риск се засилва, когато се въвежда нова технология за обработка на данните; освен това при мащабно обработване на специални категории данни; автоматично обработване, включително и профилиране. Надзорният орган, от своя страна трябва да състави списък на всички видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните. Въпреки, че са определени специфични случаи, при които се извършва оценка на въздействието, задължение на всеки администратор е да въведе мерки и да управлява по подходящ начин рисковете за правата и свободите на субектите на данни. В тази връзка администраторите трябва непрекъснато да оценяват рисковете, които се пораждат от техните дейности по обработване, за да идентифицират кога съществува вероятност определен вид обработване „да породи висок риск за правата и свободите на физическите лица“.

Характерно за процеса по оценка на въздействието е, че той може да се приложи на веднъж за множество операции по обработване, които се сходни по естество, обхват, контекст и цел. Оценката на въздействието цели анализ на нови ситуации, които биха могли да доведат до високи рискове, което прави ненужно провеждането му в случаите, които вече са познати. Такъв може да бъде случаят, когато се използва сходна технология за събирането на един и същ вид данни за едни и същи цели. Специфичното тук е, че една оценка на въздействие може да бъде приложима към сходни операции по обработване, извършвани от различни администратори. В такива случаи следва да бъде споделена оценката или тя да бъде направена публично достъпна, като описаните мерки трябва да бъдат изпълнени и да бъде представена обосновка за извършването само на една-единствена оценка на въздействието. Поради факта, че обработването на лични данни често засяга съвместни администратори, то те трябва да определят прецизно своите задължения. Ясно трябва да дефинират, коя страна отговаря за различните мерки за третиране на рисковете и за защита на правата и свободите на субектите на данни. Всеки администратор следва да посочи своите потребности и да споделя полезна информация, без да разкрива тайни (като например търговски тайни, интелектуална собственост, поверителна търговска информация) или да оповестява слабости.

2. Същност на процеса по оценка на въздействието

Оценката на въздействието на личните данни е необходимо да бъде проведена преди да започне процеса по обработка на данните[6]. По този начин тя се явява

[4] Пак там, основание 84
[5] Пак там, чл.35
[6] Пак там, чл.35, параграф 1 и 10, Съображение 90 и 93

инструмент, който подпомага вземането на решения относно обработването. Извършването на оценка на въздействието следва да започне на възможно най-ранен етап от проектирането на операцията по обработване, дори ако някои от операциите по обработване все още не са известни. Освен това трябва да се има предвид, че то е периодичен процес и е необходимо неговото регулярно провеждане. Особено важно е да се прави, когато обработката на данни е динамична и подлежи на текущи промени. Така извършването на оценка на въздействието се явява важен и постоянен процес, а не еднократно действие на администратора.

За извършването на ефикасна и адекватна оценка на въздействието са необходими добри, задълбочени познания при отчитане на различните бизнес процеси на администратора. По тази причина администраторите на лични данни често избират да работят с екип от членове от организацията на администратора, длъжностното лице по защита на данните (ако има такова) и/или специалисти в областта извън организацията. По този начин може да се получи по-пълна картина на всички рискове застрашаващи обработката на личните данни от администратора. Важно е да се има предвид, че администратора носи пълната отговорност да гарантира съответствие на изискванията на Регламент (ЕС) 2016/679.

В основата на процеса по оценка на въздействието са заложени елементите от ISO 31000 Управление на риска. Управлението на риска по отношение на личните данни е насочено към „управление на рисковете“ за правата и свободите на физическите лица.

В обобщение може да се каже, че при планиране процеса по обработване на лични данни с вероятност от висок риск, администраторът трябва:

- да избере методология за оценка на въздействието, която да е интегрирана в съществуващите процеси и да включва съответните заинтересовани страни и ясно определя техните отговорности;
- да предостави доклада от оценката въздействието на компетентния надзорен орган;
- да се консултира с надзорния орган, когато не успее да определи достатъчни мерки за ограничаване на високите рискове;
- да извършва периодичен преглед на оценката на въздействието на личните данни и на обработването, което се оценява чрез нея, най-малкото когато настъпи промяна на риска, породен от операцията по обработване;
- да документира взетите решения.

3. Методи за оценка на въздействието

За осъществяване на оценката на въздействието на личните данни няма разработена единна методика. GDPR изяснява основните изисквания и допуска администраторите да изберат правилният за тях подход, който да бъде в съответствие с изискуемите критерии.

Според Европейски съвет за защита на данните (European Data Protection Board, бивша работна група по член 29) е удачно специфични методики за бъдат разработвани за отделните сектори на икономиката. По този начин ще бъдат

отразени специфични особености на конкретни видове обработка. Така оценката на въздействието може да бъде насочена към въпроси, които възникват в даден икономически сектор или при използването на конкретни технологии или извършването на конкретни видове операции по обработване.

В настоящият доклад ще бъдат разгледани две от утвърдените методики, които се ползват с приоритет. Първата е наречена SDM MODEL и е дело на екип от Германски експерти, а втората GDPR DATA PROTECTION IMPACT ASSESSMENTS, разработена от експертен международен екип на специалистите от ISACA.

3.1. SDM Model

SDM моделът предлага методика за оценка на въздействието при обработката на лични данни. Разработен е от експерти за нуждите на Германия, но може да бъде използван, като основа и добър пример върху, която може да се стъпи в целия ЕС.

Моделът, е разработен, както в услуга на администраторите на лични данни, така и за надзорните органи. По този начин се постига цялостност, включваща планиране, изпълнение и непрекъснато наблюдение на необходимите функции и мерки за защита от страна на администраторите и прозрачност и надеждност на процедурата от страна на надзорният орган.

SDM, като цялостна концепция цели да осигури хармонизирана, прозрачна и правдоподобна система за оценка на защитата на личните данните. От една страна SDM осигурява систематично и подлежащо на проверка сравнение между регламентацията, стандартите, договорите, декларациите за съгласие и организационните правила и от друга страна, прилагането на тези изисквания в организационните, техническите процедури и в процедурите базирани на ИТ.[7]

В най-общи линии SDM модела дава информация за:

- Законовите изисквания за защита на личните данни;
- Структурира на процедури;
- Класифицира данните в нива на защита;
- Осигурява набор от стандартизирани мерки за защита на данните[8]

Целите на защита на лични данни са насочени към: минимизиране на данните, наличност, цялостност, поверителност, несвързаност, прозрачност, интервенция.

За всеки от компонентите на SDM (данни, системи и процеси) референтните мерки са посочени и описани за всяка от целите за защита. За всяка от мерките се вземат предвид и ефектите от прилагането на други цели за защита, които не са пряко засегнати от съответната мярка. По този начин конкретните мерки могат да допринесат индивидуално за постигането на няколко цели за защита.

Моделът дава яснота за това, как могат да бъдат постигнати съответните цели. Те се свеждат до: минимизиране на данните, наличност, цялостност, поверителност, несвързаност, прозрачност, интервенция.[9] Постигането на тези цели

[7] The Standard Data Protection Model, V1.0-Trial Version, Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016, pp5.
[8] Пак там с.8
[9]Пак там, с.27-30

е добър гарант за постигане на стабилно ниво на защита на данните на физическите лица.

Освен конкретните препоръки за постигане на целите в SDM е отделено специално място за оценката на риска. При SDM от решаващо значение е нивото на защита на личните данни. В теорията на риск мениджмънта е характерно нивото на риска да се измерва, чрез тежестта на щетите и честотата на проявление. Според SDM моделът за защитата (на основните права) на хората се изисква друга, различна оценка. Моделът налага изпълнението на определена специфична процедура, чиито основни реквизити включват съответното правно основание, нивото на защита, продължителността на съхранението, вида и броя на евентуалните получатели на обработените данни. Поверителността на личните данни играе специална роля при определянето на нивото на защита. Тя се гарантира, чрез подходящи мерки, дори ако нивото на потенциално вмешателство е ниско.

SDM разграничава три категории на защита "нормални", "високи" и "много високи" за процедурите за обработка на лични данни. Трябва да се има предвид, че данните с „нормално“ ниво на защита могат да изискват „високо“ ниво на защита, ако се обработват в големи количества ("Натрупване на голям брой данни"). Данните с нормално ниво на защита могат да изискват висока степен на защита, ако се обработват от лица, които имат различни роли, с различни права за различни цели ("Натрупване на голям брой права").

SDM налага да бъде извършен анализ на риска, с цел да се оцени вероятността организацията да не спазва правилата за защита на личните данните, въпреки предприетите мерки. Въз основа на анализът е възможно да се наложат допълнителни защитни мерки. Анализът на риска за защита на личните данните трябва да обхване и аспектите на информационната сигурност.

Анализ и оценка на риска се извършват в следните направления:

1. Склонността на организацията да променя целта на използването на данните по неразрешен начин.

2. Оперативните възможности на дадена организация да извърши промяна на целите на обработката на лични данни.

3. Трябва да се вземат предвид ефектите от прехвърлянето на лични данни към трети държави. Независимо от определеното равнище на защита на данните в национален контекст, трябва да се проучи кои допълнителни защитни мерки биха били необходими за такова прехвърляне и евентуално за обработка в трети страни.

4. Обхватът на приетите мерки за информационна сигурност, включително процесите за разрешаване на конфликти между защитата на информационната сигурност на бизнес процесите и оперативното запазване на нормативната уредба.

Оценката на риска се основава на определянето на фактическите обстоятелства свързани с обработката на личните данни. Тя налага да бъде даден отговор на редица въпроси свързани с отговорност, договорни взаимоотношение между администратори, съгласие на субектите, цели на обработка, инфраструктура и др. Целта на тези въпроси е да се определят фактическите обстоятелства.

Оценката по същество след определянето на фактическите обстоятелства се съсредоточава върху това дали разглежданата или планираната обработка е общо допустима. Последващото прилагане на метода изисква даването на отговори на нова серия от въпроси. Те са насочени към: легитимност на целите на обработка, допустимост на промяна в целите на обработка, прехвърляне на данни между субекти и трети страни, специални изисквания, технически и организационни мерки.[10]

Оценката на риска включва и дефинирани качествени характеристики на целите за защита. В основни линии те са свързани с: дефиниция на данните, които трябва да са актуални, на кого трябва да бъдат разкрити или отказани данни, в какъв размер, за кого обработката трябва да е прозрачна, какви промени са допустими и т.н.

След като целите за защита са определени от гледна точка на качеството, трябва да се дефинира ниво на защита. На това място следва да се отчетът и остатъчните рискове и да се отчете в каква степен застрашават постигането на целите на защита. Трябва да се има в предвид, че всяко изменение в бизнес процесите ще даде отражение върху заплахите свързани с личните данни. Това прави оценката на въздействието необходимост.

Като цяло SDM моделът дава една добра рамка върху, която може да се стъпи при провеждане на детайлна оценка на въздействието върху личните данни.

3.2. GDPR DATA PROTECTION IMPACT ASSESSMENTS

ISACA е независима, нестопанска, глобална асоциация занимаваща се с разработването, приемането и използването на глобално приети разработки и практики за информационни системи. Персонала на ISACA наброява 450 000 професионалисти в областта на информацията и кибернетичното пространство сигурността, управлението, риска и иновациите. ISACA има присъствие в 188 държави, с 217 главни офиси включително в САЩ и Китай.

ISACA разработва GDPR Assessment, като предоставя на потребителите „пътна карта“ за внедряване на GDPR въз основа на отговорите на редица въпроси. Получената персонализирана оценка предлага данни за това, къде организация трябва да съсредоточи своите усилия за защита на данните. С течение на времето потребителите могат да направят нова оценката, за да преценят напредъка по спазването на GDPR.

Документа предоставя информация за GDPR, ползите от използването на принципите за поверителност на ISACA за извършване на оценки на въздействието, изисквани по GDPR за защита на данните (DPIAs), които са специфичен тип оценка на въздействието върху неприкосновеността на личния живот (PIA) и как да се постигне GDPR DPIA, използващи принципите за поверителност.

GDPR изисква всеки администратор и обработващ на лични данни да изпълнява DPIAs. Процесът на DPIAs е предназначен да се: опише обработката; прецени необходимостта и пропорционалността на обработката; определи съответствието с изискванията на GDPR; подпомага управлението на риска за правата и свободите

[10] The Standard Data Protection Model, V1.0-Trial Version, Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016, pp38-40

на физическите лица, произтичащи от обработката на лични данни и определят подходящи мерки за преодоляване или минимизиране на този риск.

С DPIAs също се поддържа отчетност, като се подпомагат администраторите и обработващите лични данни, не само да спазват всички изисквания на GDPR, но и да демонстрират, че организацията предприема съответните действия, за да гарантира постоянно съответствие.

Организациите могат да използват принципите на ISACA за поверителност като рамка за техния DPIA, като групират GDPR и други изисквания в рамките на всеки от 14-те принципа за поверителност. Освен това отговарят на изискванията за GDPR чрез въпроси, които се отнасят до DPIA. Рамката позволява въпросите да се коригират така, че да се отнасят към подобни изисквания от други нормативи.

Принципите за поверителност, които предлага ISACA са могат да се обобщят в следните: 1. Избор и съгласие; 2. Законови основания и специфични ограничения; 3. Лични данни и чувствителни данни. Цикъл на живот на данните; 4. Прецизност и качество на данните; 5. Откритост и прозрачност при обработката/права за прозрачност на данните/; 6. Индивидуалност на организацията / достъп до данни/; 7. Отговорност; 8. Мерки за сигурност; 9. Мониторинг, оценка и докладване; 10. Превенция на вреди; 11. Управление на трети лица / контрагенти; 12. Управление недопускането на нарушения; 13.Сигурност и поверителност на обработката на ЛД; 14.Свободен поток от информация и законови ограничения.

Организациите могат да използват четиринадесетте принципа за поверителност на ISACA, за да оценят риска. Методът подробно илюстрира същността на всеки един от принципите, като подпомага определянето на риска за неприкосновеност на личните данни, чрез дефинирането на множество въпроси по всички принципи. По този начин администраторите на лични данни контролират политиките и процедурите си по отношение на обработката на лични данни.

След приключването на процеса по DPIA, администраторите на лични данни трябва да намалят идентифицирания риск, след което да поддържат съответствие, чрез постоянни дейности по спазване и управление на риска. Организациите следва да установят план за корективни действия, за да отговорят по подходящ начин на идентифицирания риск. При одит от надзорния орган се прави проверка не само дали организацията е извършила DPIA, но и дали съществуват документирани действия за въздействие върху риска. Надзорният орган проверява времевата рамка за смекчаване на всяка от констатациите на DPIA и наблюдава напредъка на организацията в това отношение.

И двата представени метода дават достатъчно информация и са добра основа за провеждане на цялостна оценка на въздействието за всеки един администратор на лични данни. Трябва да се има предвид, че оценката на въздействие освен от широкия набор от дейности, които предлагат и двата метода зависи в голяма степен от сферата на дейност, отрасъла и спецификата на всяка една организация.

3.3. Оценка на въздействието върху защитата на личните данни, прилагана в практиката в България

Методиката за оценка на въздействието, препоръчана от българският регулатор "Комисия за защита на личните данни" се основава на NIST 800-53 „Security and Privacy Controls for Information Systems and Organizations" на националния институт по стандарти и технологии на САЩ и се използва още от въвеждането на Наредба №1 от 2013 г.

Нива на въздействие, които могат да бъдат установени в нашата практика са както следва: изключително високо, високо, средно, ниско.

За определяне на въздействието е необходимо да се специфицират и оценят: типовете лични и данни, възможните заплахи.

Типовете личните данни могат да бъдат разделени условно на лични данни и чувствителни лични данни, които са специфичните лични данни, отговарящи на новата технологична среда и предизвикателства: произход; убеждения; членство в политически партии или организации; сдружения; здраве, сексуална ориентация и човешки геном; други.

Нивото на въздействие, според българският регулатор се определя на база отговори на въпроси, свързани с дефинирането и описанието на параметрите на регистъра имащи отношение към сигурността на данните; с определяне на нивото на въздействие за всеки регистър; с групиране на регистрите и определяне на общото им ниво на въздействие.

Нивото на въздействие се определя както следва:

{Регистър} x {Тип лични данни} x {Заплаха} x{ Цел} x {Последствие} x {Обхват}

Във всяка една организация, средно ниво на въздействие върху личните данни, като минимум има в регистрите на „Човешки ресурси". Лечебните заведения, лабораториите и фирмите, в чиято дейност се обработват чувствителни лични данни имат повече регистри с високо ниво на въздействие върху личните данни. Такива могат да бъдат и маркетинговите и социологически компании, извършващи автоматично профилиране или систематично наблюдение. В тази категория са и учебните заведения, като тук допълнителен фактор, който следва да се отчита е риска и респективно въздействието от обработката на данни на непълнолетни субекти.

4. Емпирични наблюдения и изводи

След влизането в сила на GDPR всички администратори на лични данни трябва да покажат съответствие, част от което изисква и извършването на оценка на въздействието при обработката на данни. След първоначалният анализ за постигнатото съответствие данните на фирма Information Consulting Office Ltd[11], резултатите показват, че значителна част от организациите в България са постигнали добра степен на съответствие по отношение на изискванията на Регулацията. По отношение на оценката на въздействие наблюденията сочат

[11] Information Consulting Office Ltd е консултантска компания с основен предмет на дейност защита на данни и информационна сигурност

повишаване на общата риск култура и осведоменост по въпросите за защитата на личните данни. Оценката на риска и на въздействието върху различните категории лични данни става по точна и обоснована, а мерките за защита според нивото на въздействие все по адекватни и ефективни.

Оценката на въздействието при защитата на лични данни представлява ключова част от спазването на GDPR, когато се планира или се извършва обработване с висок риск. Администраторите на лични данни следва стриктно да оценяват риска, така че да не допускат злоупотреби и да гарантират в голяма степен сигурността на защитата при обработката на лични данни. В настоящият доклад бе представена рамка на два различни, но допълващи се метода, които дават добра основа за извършване на процеса по оценка на въздействието. Успешното им прилагане от администраторите на лични данни следва да доведе до повишено доверие и увереност от страна на субектите на данни и другите администратори на данни.

Използвана литература

1. Кога е необходимо да се изготви оценка на въздействието върху защитата на данните (ОВЗД)?, Европейска комисия, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_bg
2. Комисия за защита на личните данни, https://www.cpdp.bg/index.php
3. Насоки относно оценката на въздействието върху защитата на данни (ОВЗД) и определяне дали съществува вероятност обработването „да породи висок риск“ за целите на Регламент 2016/679, Работна група за защита на личните данни по чл.29,17/BG WP 248 rev. 01, 2017
4. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни
5. GDPR DATA PROTECTION IMPACT ASSESSMENTS, ISACA,2017,pp11
6. The Standard Data Protection Model, V1.0-Trial Version, Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016