DOI: http/doi.org/10.370.75/BAL.2021.03.03

Защита на личните данни на етапа на проектирането и по подразбиране и оценка на въздействието върху защитата на данните като способи за обезпечаване сигурността на личните данни

Privacy by Design, Privacy by Default and Data Protection Impact Assessment as Methods for Ensuring Personal Data Security

Анита Борисова[1]

SUMMARY

The main goal of the right to personal data protection turns out to be their security. Various instruments of the legislation can achieve this task. EU law requires the data controllers to put in place measures to implement effectively the principles of protection and necessary safeguards' integration in compliance with the

[1] Анита Борисова е адвокат и докторант в катедра „Публичноправни науки" на Университета за национално и световно стопанство, e-mail: a.ev.borisova@unwe.bg, a.ev.borisova@gmail.com (Anita Borisova is an attorney-at-law and a PhD student at the Department of Public Law at the University of National and World Economy, e-mail: a.ev.borisova@unwe.bg, a.ev.borisova@gmail.com).

requirements of the GDPR protecting the data subjects. These safeguards should apply both during processing and planning the processed activity including the means of their managing. To this end it is important to consider the state of the art, the costs of implementation, the nature, the scope and the objectives of the personal data processing, and the risks and their burden on the rights and freedoms of the data subjects, as well. Another way to ensure the data security is to carry out the protection impact assessment and to find where the processing could lead to a risk for the rights and freedoms of individuals. The GDPR does not specify how to make the risk assessment, but rather contains a list of processing operations that are considered to pose a high risk and for which a preliminary impact assessment is particularly necessary.

KEY WORDS

Data Privacy; Privacy by Design; Privacy by Default; Data Protection Impact Assessment

1. „Защита на личните данни на етапа на проектирането и по подразбиране“ (privacy by design and privacy by default)

Съгласно правото на ЕС се изисква администраторите на лични данни да въведат мерки за ефективно прилагане на принципите за защита и да интегрират необходимите гаранции, за да се спазят изискванията на ОРЗД[2] и да се защитят правата на субектите на данни. Тези мерки следва да се прилагат както по време на обработването, така и при планиране на дейността по обработването и определянето на средствата за обработване. За тази цел се взимат предвид

[2] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. 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 (Общ регламент относно защитата на данните).

достиженията на техническия прогрес, разходите за прилагане, естеството, обхватът и целите на обработването на личните данни, както и рисковете и тяхната тежест за правата и свободите на субектите на данни. Освен това администраторите и обработващите лични данни са длъжни да проектират обработването на данни по такъв начин, че да предотвратят или да сведат до минимум риска от намеса в правата и свободите и да въведат технически и организационни мерки, съобразени с последиците върху правото на защита на личните данни на всички етапи от обработването.

Така се оказва, че защитата на данните на етапа на проектирането и по подразбиране е „фундаментът, върху който се гради философията на защита на личните данни“[3]. Споделям изказаното в литературата мнение, че гореспоменатите концепции следва да се възприемат в по-широк план от предвиденото в чл. 25 от ОРЗД задължение, а именно те следва да се приемат като цялостна „политика на всеобхватно и законосъобразно планиране и реализиране на процесите по обработване на лични данни, по начин, който обезпечава тяхната сигурност“[4]. В основата на разглежданата защита на личните данни на етапа на проектирането и по подразбиране стоят принципите, свързани с тяхното обработване, на които тук няма да се спираме.

Защитата на етапа на проектирането изисква към момента на определяне на целите на обработването администраторът да анализира и планира всички релевантни аспекти на самата дейност по обработване, така че да осигури механизми и мерки на защита, които да действат в рамките на целия процес – от стартирането му със събирането на личите данни до неговия край с тяхното заличаване. В случай че съществуват пречки за изпълнението на предвидения план и има каквото и да било съмнение, че сигурността на личните данни може да бъде застрашена, или че някой от принципите по член 5 от ОРЗД не може да бъде подсигурен или има опасност за неговото нарушаване, обработването не следва изобщо да започва.

---

[3] Н. Фети, Д. Тошкова-Николова. *Прилагане на защитата на личните данни.* София, ИК „Труд и право“, 2020, с. 22.

[4] Пак там.

Защитата на данните по подразбиране изисква от своя страна практическо прилагане на предвидения набор от механизми, технически и организационни мерки по начин, който взема предвид и съобразява принципите за законосъобразно обработване и защита на личните данни, предвидени в ОРЗД.

Планирането или осъществяването на обработването на лични данни не подлежи на стандартизиране и унифициране, поради различните типове бизнеси, дейности и контекст, в който те се обработват. Възможно е обаче изготвянето на модел, по който да се ръководят администраторите с цел осъществяване на концепциите за защита на етапа на проектирането и по подразбиране, който да е съответно сходен за всяка дейност по обработване на лични данни. Най-общо казано, подобен модел би могъл да включва следните стъпки[5].

- Анализ на принципните положения при планиране на обработването – в тази фаза се преценява наличието или неналичието на обработване на лични данни, приложимата правна уредба, правното основание за законосъобразно обработване, приложимостта на принципите по ОРЗД, евентуален трансфер на личните данни, необходимостта от назначаване на длъжностно лице по защита на данните (ДЛЗД) и др. Определят се също целите и средствата на обработването. Анализират се последиците за правата на субектите на данни и способите за тяхното осъществяване.
- Дейности по управление на риска за защита на личните данни, които могат да включват, но не се изчерпват до: анализ на риска, подходящи технически и организационни мерки, оценка на въздействието върху защитата на данните, консултации с надзорния орган, процедури за своевременна реакция при нарушаване сигурността на данните.
- Гарантиране на правата на субектите на данни, което се осъществява чрез предоставяне на прозрачна, разбираема, достъпна и актуализирана информация при спазване изискванията на чл. 13 и чл. 14 от ОРЗД, разработване и прилагане на процедури за навременно разглеждане на исканията на субектите на данни, надлежно уведомяване на субектите при

[5] В подобен ред и вид стъпките са представени във Фети, Тошкова-Николова (2020), с. 25 – 30.

настъпили нарушения в сигурността на данните им, съобразно регулаторните изисквания.

• Контрол върху лицата, обработващи лични данни от името на администратора, чрез определяне на отговорности по равнища в организацията, входящо и последващо обучение по въпросите на защитата на данните и пр.

• Отчетност – осъществявана съобразно принципа на отчетност, изразяваща се в изпълнението на редица задължение по ОРЗД, като създаване на регистри за дейностите по обработване, назначаване на ДЛЗД, изготвяне на оценка на въздействието, внедряване на вътрешни правила, политики, процедури и пр.

2. Оценка на въздействието върху защитата на данните (ОВЗД)

Операциите по обработване винаги имат потенциал да създадат рискове за правата на физическите лица. Личните данни могат да бъдат загубени, разкрити на неупълномощени страни или обработени в разрез със закона, а рисковете се различават в зависимост от естеството и обхвата на обработването. В този смисъл мащабните операции, които включват обработване на чувствителни данни например, носят много по-висок риск за субектите на данни в сравнение с обработването на минимални данни като адреси и личните телефонни номера в компания с малък брой служители.

Появата на нови технологии води до все по-комплексни операции по обработка, поради което администраторите следва да проучват възможното въздействие, а това ще даде насока за планираното обработване, преди да започнат операциите по него. Така компаниите ефективно и целесъобразно могат да установят, преодолеят и ограничат рисковете предварително, като значително редуцират вероятността за негативно въздействие върху субектите на данни.

Извършването на оценки на въздействието върху защитата на данните е предвидено в член 35 от ОРЗД, съгласно който, ОВЗД е необходима при вероятност обработването да

доведе до висок риск за правата и свободите на лицата. В ОРЗД не е определено как трябва да се оценява вероятността от настъпване на риска, а по-скоро се съдържа списък на операциите по обработване, за които се смята, че създават висок риск и за които е особено необходимо да се извърши предварителна оценка на въздействието. Такива са случаите, когато:

- личните данни се обработват с цел вземане на решения относно физически лица след систематична и обстойна оценка на личните аспекти, свързани с физически лица (профилиране);
- се извършва мащабно обработване на чувствителни данни или лични данни, свързани с присъди и нарушения;
- обработването включва широкомащабно, систематично наблюдение на публично достъпни зони.

Националните надзорни органи, в т.ч. и Комисията за защита на личните данни (КЗЛД), следва да приемат и публикуват списък на видовете операции по обработване, за които се изисква ОВЗД, но също така са оправомощени да съставят и списък на операциите по обработване, освободени от това задължение. Българският надзорен орган е приел такъв списък през февруари 2019 г., който може да бъде открит на уебсайта на КЗЛД[6].

Ако ОВЗД е задължителна за конкретни операции по обработване, администраторите трябва да оценят необходимостта и пропорционалността на тези операции и възможните рискове за правата на субектите на данни. При това ОВЗД следва да съдържа и планираните мерки за сигурност с цел преодоляване на установените рискове. За съставянето на списъците надзорните органи на държавите членки си сътрудничат помежду си, както и с Европейския комитет по защита на данните (ЕКЗД). С това се цели последователен

[6] Комисия за защита на личните данни. *Съобщение за публикуване на Списък на видовете операции по обработване на лични данни, за които се изисква извършване на оценка за въздействие върху защитата на данните*, [онлайн] https://www.cpdp.bg/index.php?p = news_view&aid = 1370 [достъпен на 17.11.2021 г.]; *Списък на видовете операции по обработване на лични данни, за които се изисква извършване на оценка за въздействие върху защитата на данните съгласно чл. 35, пар. 4 от Регламент (ЕС) 2016/679* [онлайн] https://www.cpdp.bg/index.php?p = element&aid = 1186 [достъпен на 17.11.2021 г.].

подход в целия ЕС по отношение на операциите, които изискват ОВЗД, както и еднакви изисквания към администраторите независимо от държавата на установяването им. В случай че след извършената оценка на риска може да се заключи, че обработването ще доведе до висок риск за правата на субектите на данни, но не са въведени подходящи мерки за неговото ограничаване, администраторът е длъжен да се консултира със съответния надзорен орган преди започване на операциите по обработване[7].

За осъществяване на ОВЗД няма разработена единна методика. ОРЗД изяснява основните изисквания и допуска администраторите да изберат правилния за себе си подход, който да бъде в съответствие с изискуемите критерии[8]. Така ОВЗД може да е свързана с единствена операция по обработване на данни или да обхваща повече от един проект едновременно например при наличие на множество операции по обработване, които са сходни по своето естество, обхват, контекст, цел и рискове. В действителност ОВЗД целят систематичното проучване на нови ситуации, които биха могли да доведат до високи рискове за правата и свободите на субектите на данни. Не е нужно да се извършва ОВЗД в случаите, когато подобни операции с много близки параметри вече са проучени.

Ако операцията по обработване включва съвместни администратори, те трябва да определят прецизно своите задължения и разпределението помежду им. Необходима е яснота в ОВЗД кой администратор отговаря за различните мерки за третиране на рисковете, както и за защитата на правата и свободите на субектите на данни.

---

[7] European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law.* Luxembourg, Publications Office of the European Union, 2018, pp. 179 – 181.

[8] П. Биолчева, Г. Средков. Оценка на въздействието при обработване на лични данни в съответствие с Регламент (ЕС) 2016/679 (GDPR). *Предизвикателства пред индустриалния растеж в България, сборник от конференцията.* 2018, с. 283, [онлайн] https://www.industrialgrowth.eu/wp-content/uploads/2018/11/29.pdf [достъпно на 17.11.2021 г.].

В тази връзка Работната група по член 29 е издала насоки[9] относно ОВЗД, които съдържат критериите за определяне на вероятността обработването да породи висок риск. Поради факта, че регулацията в ОРЗД подлежи на широко тълкуване по повод случаите, в които ОВЗД е необходима, а споменатите списъци на надзорните органи не са и не могат да бъдат изчерпателни, поради многообразието от операции за обработвана на лични данни, насоките на Работната група по член 29 предоставят девет критерия, за да подпомогнат решението на администраторите дали в конкретен случай се изисква ОВЗД или не.

• Оценка или точкуване – включва аспекти, свързани с поведението на субекта на данни (икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността местоположението или движенията). Примери могат да бъдат финансови институции, които извършват справки за своите клиенти в референтна база данни за кредити, за борба срещу изпирането на пари или финансирането на тероризма, или за борба с измамите.

• Автоматизирано вземане на решения с правни последици или подобни сериозни последици – например обработването може да доведе до изключване или дискриминация на физически лица.

• Систематично наблюдение – обработване, което се използва за наблюдение или контрол на субектите на данни, включително данни, които се събират чрез мрежи или „систематично мащабно наблюдение на публично достъпна зона“. Възможно е да се събират лични данни при обстоятелства, когато субектите на данни може да не осъзнават кой събира техните данни и как ще бъдат използвани. Освен това за физическите лица може да е невъзможно да избегнат подлагането на такова обработване в публична (или публично достъпна) зона.

[9] Работна група по член 29. *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, прието на 4 април 2017 г., последно преработени и приети ня̀а 4 октомври 2017 г.,* [онлайн] https://www.cpdp.bg/userfiles/file/WP29/wp248% 20rev_01_bg.pdf [достъпно на 17.11.2021 г.].

• Чувствителни данни – в тази връзка може да е от значение дали данните вече са обявени публично от съответното физическо лице или от трети страни. Фактът, че личните данни са публично достъпни, може да се разгледа като фактор в оценката, ако се е очаквало данните да се използват допълнително за определени цели.

• Мащабно обработване на данни – в ОРЗД не се определя какво означава мащабно обработване, въпреки че съображение 91[10] съдържа известни насоки. Във всеки случай Работната група по член 29 препоръчва да се проучат по-специално следните фактори, когато се определя дали извършваното обработване е мащабно:

а. броят на засегнатите субекти на данни като конкретна цифра или като дял от съответното население;

б. обемът на данните и/или обхватът на различните видове данни, които се обработват;

в. продължителността или непрекъснатостта на дейността по обработване на данните;

г. географският обхват на дейността по обработване.

• Търсене на съвпадение или съчетаване на набори от данни – например с произход от две или повече операции по обработване на данни, извършени за

[10] Съображение 91 ОРЗД: „…Оценка на въздействието върху защитата на данни следва да се извършва и когато личните данни се обработват с цел вземане на решения относно конкретни физически лица след систематична и обстойна оценка на личните аспекти, свързани с физически лица, въз основа на профилирането на тези данни или след обработването на специални категории лични данни, биометрични данни или данни за присъди и нарушения или свързани с това мерки за сигурност. Оценка на въздействието върху защитата на данните се изисква също за широкомащабно наблюдение на публично достъпни зони, особено когато се използват оптично-електронни уреди, или за всякакви други операции, когато компетентният надзорен орган счита, че има вероятност обработването да доведе до висок риск за правата и свободите на субектите на данни, по-специално поради това, че възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор, или поради това, че се извършват систематично в голям мащаб. Обработването на лични данни не следва да се счита за широкомащабно, ако засяга лични данни на пациенти или клиенти на отделен лекар, друг здравен работник или адвокат. В такива случаи оценката на въздействието върху защитата на данните не следва да бъде задължителна“.

различни цели и/или от различни администратори, по начин, който надхвърля разумните очаквания на субекта на данни.

• Данни относно уязвими субекти на данни – обработването на този вид данни е включено като критерий поради увеличената неравнопоставеност на правомощията между субектите на данни и администратора, което означава, че физическите лица може да не са в състояние лесно да се съгласят или да възразят срещу обработването на техните данни, или да упражнят своите права. Уязвимите субекти на данни могат да включват деца, служители, по-уязвими сегменти от населението, които се нуждаят от специална защита (психично болни лица, търсещи убежище лица или възрастни лица, пациенти и др.) и всички други субекти на данни, при които може да се установи неравнопоставеност в отношенията с оглед на положението на субекта на данни и това на администратора.

• Иновативно използване или прилагане на нови технологични или организационни решения – например съчетаване на използването на пръстови отпечатъци и разпознаване на лица с цел подобряване на контрола на физическия достъп и пр. В действителност личните и социалните последици от внедряването на нова технология може да не са известни, а ОВЗД ще помогне на администратора да разбере и да третира тези рискове.

• Операциите по обработването сами по себе си „възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор“ – включва операции по обработване, чиято цел е да се позволи, измени или откаже достъпът на субектите на данни до услуга или сключването на договор. Пример за това са банки, които извършват справки за своите клиенти в референтна база данни за кредити, за да решат дали да им предложат кредит.

Въведено е практическото правило от Работната група по член 29, че операциите по обработване, които отговарят на по-малко от два критерия, представляват по-нисък риск и за тях не се изисква оценка на въздействието върху защитата на данните, докато за тези, които отговарят на два и повече от горните критерии, се изисква такава оценка. Въпреки

това в някои случаи администраторът може да заключи, че обработване, което отговаря само на един от тези критерии, изисква ОВЗД. От друга страна, дадена операция по обработване може да отговаря на няколко от посочените случаи и все пак администраторът да стигне до извода, че не съществува вероятност същата да породи висок риск. Важното в всички случаи е администраторът да обоснове и документира причините, поради които не извършва ОВЗД, и да включи/отбележи възгледите на ДЛЗД в тази връзка.

Когато не е ясно дали се изисква ОВЗД, Работната група по член 29 препоръчва все пак да се извърши такава оценка, тъй като тя представлява „полезен инструмент, който помага на администраторите да спазват законодателството в областта на защитата на данните“. Важно е въвеждането на нова технология за обработване на лични данни винаги да бъде съпроводено с ОВЗД. Въпреки това самият факт, че не са налице условията, при които извършването на ОВЗД е задължително, не намалява общото задължение на администраторите да въведат мерки, за да управляват по подходящ начин рисковете за правата и свободите на субектите на данни. На практика това означава, че 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“.

Освен всички останали функции, които има, ОВЗД представлява важен инструмент за отчетност, тъй като помага на администраторите на лични данни не само да спазят изискванията на ОРЗД, но и да демонстрират това спазване. Съгласно добрата практика ОВЗД следва постоянно да се преразглежда и да подлежи на редовна повторна оценка във времето.

Консултация с надзорния орган се изисква всеки път, когато администраторът не може да предприеме достатъчни мерки за намаляване на рисковете до приемливо равнище, т.е. остатъчните рискове продължават да бъдат високи. Освен това е възможно да има хипотези, когато правото на държавата членка изисква от администраторите да се консулти-

рат с надзорния орган и/или да получават предварително разрешение от него, във връзка с обработването от администратор в полза на обществения интерес, включително по повод на обработване, свързано със социалната закрила и общественото здраве (член 36, параграф 5 от ОРЗД). Тази концепция е възприета от българския законодател в чл. 12, ал. 2 от ЗЗЛД[11].

Съгласно ОРЗД неспазването на изискванията за провеждане на ОВЗД може да доведе до налагане на имуществени санкции от компетентния надзорен орган. Ако не бъде извършена оценка на въздействието, когато обработването подлежи на ОВЗД, ако ОВЗД бъде извършена неправилно или ако не бъде проведена консултация с компетентния надзорен орган, когато това се изисква, може да се стигне до налагането на административна глоба в размер до 10 милиона евро или, в случай на предприятие, до 2% от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока.

Съгласно правната доктрина ОВЗД надхвърля основното си предназначение да служи за управление на високите рискове, които операциите по обработване пораждат за субектите на данни, а е видяна като важен инструмент за отчетност, който безспорно допринася за обезпечаване сигурността на личните данни[12].

Любопитно е да отбележим, че макар ОВЗД да се счита за нов инструмент, възприет с ОРЗД, някои автори приемат[13], че подобна оценка е била изготвяна и съобразно регулирания

[11] ЗЗЛД: Чл. 12 (2) (Отм. – ДВ, бр. 103 от 2005 г., изм. – ДВ, бр. 91 от 2006 г.; изм., бр. 17 от 2019 г.) Освен в случаите по чл. 36, параграф 1 от Регламент (ЕС) 2016/679 предварителни консултации се извършват и когато се обработват лични данни в изпълнение на задача в обществен интерес, включително обработване във връзка със социалната закрила и общественото здраве. В този случай комисията може да разреши обработването преди изтичането на срока по чл. 36, параграф 2 от Регламент (ЕС) 2016/679.

[12] В този смисъл Фети, Тошкова-Николова (2020), с. 202.

[13] В този смисъл А. Александров. *Защита на личните данни на работниците и служителите*. София, ИК „Труд и право“, 2016, с. 94.

в българското законодателство правен режим, създаден вследствие на Директива 95/46/ЕО[14].

Заключение

Накрая следва да отбележим, че със съвременното развитие на компютрите, интернет и услугите на информационното общество се появяват все повече нови рискове, свързани с правото на зачитане на личния живот, както и със събирането и използването на лична информация, затова и обезпечаването на нейната сигурност следва да има приоритет за администраторите и обработващите лични данни. Препоръчваме прилагането на максимален брой инструменти, които предлагат законодателството и практиката, с цел съхраняване на интересите на субектите на личните данни.

Цитирани източници

European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*. Luxembourg, Publications Office of the European Union, 2018.

Александров, А. *Защита на личните данни на работниците и служителите*. София, ИК „Труд и право“, 2016 г. (Aleksandrov, A. *Zashtita na lichnite danni na rabotnitsite i sluzhitelite*. Sofia, IK „Trud i pravo“, 2016).

Биолчева, П. и Средков, Г. Оценка на въздействието при обработване на лични данни в съответствие с Регламент (ЕС) 2016/679 (GDPR). *Предизвикателства пред индустриалния растеж в България, сборник от конференцията, 2018* [онлайн] https://www.industrialgrowth.eu/wp-content/uploads/2018/11/29.pdf [достъпно на 17.11.2021 г.] (Biolcheva, P. i Sredkov, G. Otsenka na vazdeystvieto pri obrabotvane na lichni danni v

[14] Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни.

saotvetstvie s Reglament (ES) 2016/679 (GDPR). *Predizvikatelstva pred industrialnia rastezh v Bulgaria, sbornik ot konferentsiyata,* 2018 [online] https://www.industrialgrowth.eu/wp-content/uploads /2018/11/29.pdf [access 17.11.2021]).

Фети, Н. и Д. Тошкова-Николова. *Прилагане на защитата на личните данни.* София, ИК „Труд и право“, 2020 г. (Feti, N. i Toshkova-Nikolova, D. Prilagane na zashtitata na lichnite danni. Sofia, IK „Trud i pravo“, 2020.