ЗАЩИТАТА НА ПРАВАТА НА ФИЗИЧЕСКИТЕ ЛИЦА В МОДЕЛА НА ВЗАИМОДЕЙСТВИЕ „ЕЛЕКТРОННА МЕДИЯ – ПОСРЕДНИК – ФИЗИЧЕСКО ЛИЦЕ“

Проф. д.т.н. Веселин Целков, Катедра „Национална сигурност“, Факултет „Информационни науки“, Университет по библиотекознание и информационни технологии
Докторант Камен Алексиев, Катедра „Национална сигурност“, Факултет „Информационни науки“, Университет по библиотекознание и информационни технологии

Резюме:
В настоящия доклад е разгледана защитата на физическите лица при взаимодействието „електронна медия – посредник – физическо лице“ в контекста на изискванията на Общия регламент за зашита на личните данни. Дефиниран е общ модел на взаимодействие и са изследвани въпросите за обработваните лични данни, защитата на правата и личните данни на физическите лица.
Ключови думи: *Общ регламент за защита на личните данни, електронни медии, права на физическите лица, модели на взаимодействие.*

PROTECTION OF THE RIGHTS OF INDIVIDUALS IN THE MODEL OF INTERACTION "ELECTRONIC MEDIA – INTERMEDIARY – INDIVIDUAL"

Professor D. Sc.Veselin Tselkov, Department of National Security, Faculty of Information Sciences, University for Library Studies and Information Technologies
PhD student Kamen Alexiev, Department of National Security, Faculty of Information Sciences, University for Library Studies and Information Technologies

Abstract:
This report examines the protection of individuals in the "electronic media - intermediary - individual" interaction in the context of the requirements of the General Data Protection Regulation. A general model of interaction is defined and the issues of processed personal data, protection of the rights and personal data of individuals are studied.
Key words: *General regulation for personal data protection, electronic media, rights of individuals, interaction models.*

ВЪВЕДЕНИЕ

Регламент (ЕС) 2016/679 на Европейския парламент и 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 (Общ регламент за защита на личните данни, Регламент (ЕС) 2016/679, GDPR) [1] е развитие на правната рамка и изисква много по-стриктно опазване на личната информация. За пробив в защитата ѝ санкциите са огромни за мащаба и възможностите на повечето администратори на лични данни. Общия регламент променя и философията на защитата на личните данни, а именно:

- основно внимание се отделя на защита на правата на субекта (физическото лице), на данните, а не на организационните и технически мерки за защита;
- проблемът със сигурността на данните се вменява изключително на администратора на личните данни.

Част от основните причини за приемането на Регламента са [2, 3]:

- бързото технологично развитие и глобализацията създадоха нови предизвикателства пред защитата на личните данни; значително нарасна мащабът на обмена и събирането на лични данни;
- технологиите позволяват и на частните дружества, и на публичните органи да използват лични данни в безпрецедентни мащаби, за да упражняват дейността си;
- физическите лица все по-често оставят лична информация, която е публично достъпна и в световен мащаб.

Всичко това е особено валидно и се отнася за взаимодействието ***„електронна медия – посредник – физическо лице“***. Методите на системния анализ са основа на това изследване. Използван е конструктивен подход за дефиниране на модела за взаимодействия и спецификация на функциите за защита на правата и данните на физическите лица.

ДЕФИНИРАНЕ НА ОБЩ МОДЕЛ НА ВЗАИМОДЕЙСТВИЕ

Общият модел на взаимодействие, моделът ***„електронна медия – посредник – физическо лице***“ обхваща:

- структурни елементи на модела;
- взаимодействия в модела;
- базови въпроси в светлината на GDPR.

Структурни елементи ма модела

Структурните елементи на модела „***електронна медия – посредник – физическо лице***“ са:

- ***електронна медия*** – администратор на лични данни, предоставящ за публичен и свободен достъп информационни ресурси;
- ***посредник*** – администратор на лични данни, предоставящ множество от средства на физическите лица за достъп до информационните ресурси;
- физическо лице.

Взаимодействия в общия модел

В основата на общия модел на взаимодействието ***„електронна медия – посредник- физическо лице“*** са:

- електронната медия предоставя собствените си електронни ресурси (електронни страници (уебсайт), бази данни и др.) за публичен и свободен достъп на физическите лица, използвайки инструменти (услуги), предоставени от посредника;
- посредникът предоставя множество от инструменти за взаимодействие (достъп, търсене, специализирани приложения и др.) до електронните ресурси;
- физическото лице използва определени услуги (използвайки някой от инструментите) за свободен и без ограничения достъп да предоставените електронни ресурси;
- за всяко физическо лице електронната медия и посредникът за достъп притежават технологични възможности за записване и анализ на различни характеристики на действията на физическото лице.

Забележка. ***Представеният модел на взаимодействие е без ограничения на достъпа до електронните ресурси от физическите лица.***

Базови въпроси

Следвайки изискванията на GDPR, в представения модел на взаимодействие възникват следните базови въпроси:

- Какви са целите за записване и анализ на различните характеристики на действията на физическото лице в електронната среда?
- Каква информация за физическото лице се записва и анализира и каква част от нея попада в категорията лични данни?
- Как са защитени данните и правата на физическите лица в съответствие с GDPR?

ОБРАБОТВАНИ ДАННИ НА ФИЗИЧЕСКИТЕ ЛИЦА

Цели за използване на събраните данни

Събраните данни се използват за:

- подобряване на съществуващите и създаване на по-добри услуги за физическото лице;
- измерване на ефективността на услугите;
- комуникация с физическото лице;
- гарантиране на сигурността, предотвратяване на измами и отстраняване на грешки.

Подобряване на съществуващите и създаване на по-добри услуги

- *Предоставяне на услугите* – информацията се използва за предоставяне на услугите, например за обработване на думите за търсене, за извеждане на резултати или за споделяне на съдържание с получатели от контактите.
- *Поддръжка и подобряване на услугите* – информацията се използва за гарантиране, че услугите работят нормално, например проследяване на прекъсванията или отстраняване на проблемите, за които е сигнализирано. Използва се също за подобряване на услугите, помага да усъвършенстване на функциите за проверка на правописа, използвани в съответната услуга.
- *Разработване на нови услуги* – информацията, която се събира в съществуващите услуги, помага да разработване на нови услуги.
- *Предоставяне на персонализирани услуги, включително съдържание и реклами* – информацията, която се събира, може да се използва за персонализиране на услугите, включително за предоставяне на препоръки, персонализирано съдържание, персонализирани реклами и персонализирани резултати от търсенето. (Пример – Google Play използва информация като кои приложения са инсталирани и кои видеоклипове са гледани в YouTube, за да предлага нови приложения, които може да се харесат.)

Измерване на ефективността

Данните се използват с цел анализ и измерване, за да се разбере как се ползват услугите. Например, анализира се информацията за посещенията на сайтовете, за да се направи оптимизиране на продуктовия дизайн. Също така се използват данните за рекламите, с

които взаимодейства физическото лице, за да се помогне на рекламодателите да разбират каква е ефективността на рекламните им кампании.

Комуникация с физическото лице

Събираната персонална информация, като имейл адрес, телефон и др., може да се използва за директно взаимодействие с физическото лице с цел:

- *изпращане на известие,* например, ако е открита подозрителна активност като опит за влизане в профила ви от необичайно местоположение;
- *възможно е също да се използва за уведомяване* за предстоящи промени или подобрения в услугите*;*
- *за заявка от физическото лице* за решаване на възникнали проблеми.

Гарантиране на сигурността, предотвратяване на измами и отстраняване на грешки:

- *гарантиране на сигурността на данните;*
- *откриване, предотвратяване и вземане на мерки при измами и злоупотреби;*
- *откриване, предотвратяване и вземане на мерки при технически проблеми.*

Типове съхранявана информация

„Бисквитки“

„Бисквитката“ е малък файл, съдържащ низ от знаци, който се поставя на компютъра ви, когато посещавате уебсайт. Когато посетите сайта отново, „бисквитката“ му позволява да разпознае браузъра ви. В „бисквитките“ може да се съхраняват предпочитания на потребителя и друга информация. Можете да конфигурирате браузъра си да отказва всички „бисквитки“ или да показва, когато се изпраща „бисквитка“. Някои функции или услуги на уебсайта обаче може да не функционират правилно без „бисквитки“.

Кеш за данни на приложенията

Кешът за данни на приложенията представлява хранилище в дадено устройство. С негова помощ, например, уеб приложенията могат да работят без връзка с интернет и да подобрят ефективността си благодарение на по-бързото зареждане на съдържанието.

Лични данни

Това е информация, която физическото лице предоставя и която го идентифицира лично, като например име, имейл адрес или данни за плащане, или други сведения, които логично могат да се свържат с подобна информация, например информацията, която свързваме с личния профил.

Чувствителни лични данни е категория лична информация, свързана с теми, като например поверителни медицински сведения, расов или етнически произход, политически или религиозни убеждения или сексуална ориентация.

Пример: профил в Google. Можете да получите достъп до някои от услугите на Google, като си регистрирате профил в Google и предоставите определена лична информация (обикновено името си, имейл адрес и парола). Тази информация за профила се използва за удостоверяването ви, когато ползвате услугите на Google, и за защита на профила ви от неупълномощен достъп от страна на други лица. Можете да редактирате или да изтриете профила си по всяко време чрез настройките му.

Непозволяваща лично идентифициране информация

Това е информация, която се записва за потребителите по такъв начин, че вече не отразява или не препраща към потребител, който може да бъде лично идентифициран.

Пикселен маркер

Пикселният маркер се поставя на уебсайт или в основния текст на имейл с цел проследяване на определена активност, като например преглежданията на даден сайт или отварянето на имейл. Пикселните маркери често се използват в комбинация с „бисквитки“.

Препращащ URL адрес

Препращащият URL (единен ресурсен локатор) адрес е информация, която се изпраща от уеб браузъра до целевата страница, обикновено когато кликнете върху връзка към нея. Тази информация съдържа URL адреса на последната уеб страница, посетена от браузъра.

Сървърни регистрационни файлове

Повечето сървъри на уебсайтовете автоматично записват заявките за страници, направени, когато се посещават сайтовете. Тези „сървърни регистрационни файлове“ обикновено включват заявката за мрежата, IP адрес, тип на браузъра, език на браузъра, дата и час на заявката ви и една или повече „бисквитки“, чрез които еднозначно може да се идентифицира използваният браузър.

Уеб хранилище на браузъра

Уеб хранилището на браузъра дава възможност на уебсайтовете да съхраняват данни в браузър на дадено устройство. Когато се използва в режим „локално хранилище“, то позволява информацията да се

съхранява между сесиите. Така тя може да се извлече дори след затваряне и повторно отваряне на браузъра. HTML 5 е една от технологиите, улесняващи уеб хранилището.

Уникални идентификатори

Уникалният идентификатор представлява низ от знаци, който може да се използва за еднозначното идентифициране на браузър, приложение или устройство. Тези идентификатори се различават по това доколко са постоянни, дали могат да се задават повторно от потребителите и как се осъществява достъп до тях.

ЗАЩИТА НА ПРАВАТА НА ФИЗИЧЕСКИТЕ ЛИЦА

Важните въпроси, които произтичат от изискванията на Общия регламент във взаимодействието „***електронна медия – посредник – физическо лице***“, са спазването на принципите при обработка на данните и осигуряване на правата на физическите лица [4, 5].

Принципи

Принципите на Общия регламент при обработка на личните данни изискват (Глава II от GDPR):

- законосъобразност, добросъвестност и прозрачност;
- ограничение на целите;
- свеждане на данните до минимум;
- точност;
- ограничение на съхранението;
- цялостност и поверителност.

Права на физическите лица

Основните права на физическите лица при обработка на личните данни (Глава III от GDPR) включват:

- информация и достъп до личните данни;
- коригиране и изтриване;
- ограничаване на обработването;
- преносимост на данните;
- възражение.

Управление на събираните от *посредника* и *електронната медия* данни

В контекста на Общия регламент ***електронната медия*** и ***посредникът*** обработват данните на физическите лица и следователно те са администратори (обработващи) на лични данни. В този случай в

предлаганите инструменти и услуги трябва да бъдат интегрирани функции, които да позволяват информираност на физическото лице и достъп и управление на събираните личните (поверителни) данни, по-съществените от които са:

- функции за преглед и коригиране на настройките за поверителност;
- функции за управление, преглед и актуализиране на личните данни;
- функции за управление, преглед и актуализиране на поверителната информация;
- функции за управление на „бисквитките“;
- функции за контролиране на активността и типовете активност;
- функции за настройка на рекламите;
- функции за персонализиране на търсенето;
- функции за експортиране, премахване и изтриване на информацията;
- функции за споделяне на информация.

Защита на личните данни

За осигуряване на адекватна защита на личните данни е необходимо да се осигури:

- сигурност на обработването;
- защита на данните на етапа на проектирането и по подразбиране;
- отчетност.

Сигурност на обработването

Сигурността на обработването (чл.32 от GDPR) изисква от администраторите и обработващите:

- да прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица. Мерки за сигурност на данните могат да бъдат:
  - псевдонимизация и криптиране на личните данни;
  - способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

- способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;
- процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

- При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.
- Да предприемат стъпки всяко физическо лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до лични данни, да обработва тези данни само по указание на администратора.

Защита на данните на етапа на проектирането и по подразбиране

Защита на данните на етапа на проектирането и по подразбиране (*Data Protection by Design and Default*, или „Поверителност по дизайн“ и „Поверителност по подразбиране“) са често обсъждани теми, свързани със защитата на данните.

Поверителност по дизайн

„Поверителност по дизайн“ (чл.25 от GDPR) означава, че техническите и организационните мерки трябва да бъдат предприети още по време на планирането на система за обработка за защита на безопасността на данните. Терминът „поверителност по дизайн“ не означава нищо повече от „защита на данните чрез технологичен дизайн“. Зад това стои мисълта, че защитата на данните в процедурите за обработка на данни се спазва най-добре, когато вече е интегрирана в технологията, когато е създадена, като трябва да се вземат предвид видът, обхватът, обстоятелствата и целта на обработката.

Поверителност по подразбиране

„По подразбиране“, както обикновено се определя в цифровия свят, се отнася до вече съществуващата или предварително избраната стойност на настройка, която е присвоена на софтуерно приложение, компютърна програма или устройство. Такива настройки се наричат още „предварително зададени“ или „фабрични настройки“, особено за електронни устройства. „Поверителност по подразбиране“ при обработката на лични данни се отнася до вземане на решение относно

конфигурационни стойности или опции за обработка, които са зададени или предписани в система за обработка, като например а софтуерно приложение, услуга или устройство, или процедура за ръчна обработка, която влияе върху размера на събрани лични данни, степента на тяхната обработка, периода на тяхното съхранение и тяхната достъпност. Администраторът трябва да избере и да бъде отговорен за прилагането на настройките за обработка по подразбиране и опции по начин, по който само обработката, която е строго необходима за постигане на поставената законна цел, е извършва по подразбиране. Основното изискването е защитата на данните да е вградена в обработката по подразбиране.

Отчетност

Администраторът носи отговорност и трябва да е в състояние да докаже спазването на принципите и да обоснове предприетите необходими технически и организационни мерки за защита на данните (чл. 5 от GDPR). Отчетността е един от основните принципи и едно от решенията за защита на данните в цифровия свят. Отчетността може да бъде разгледана в тринадесет основни направления, както следва:

- поддържане на управленската структура;
- поддържане на описите с данни;
- поддържане на политиката за неприкосновеност и защита на личните данни;
- поддържане на операционните политики и процедури;
- повишаваща се трениране и съзнание (убеждение);
- поддържане на контролите за сигурност;
- поддържане на договорите;
- поддържане на бележките;
- управление на въпросите, оплакванията и дискусиите;
- мониторинг (непрекъснато наблюдение) за новите операционни (оперативни) практики;
- мониторинг (непрекъснато наблюдение) за нарушенията на личните данни;
- мониторинг (непрекъснато наблюдение) на практиките за управление на личните данни;
- следене на външните критерии.

ЗАКЛЮЧЕНИЕ

В представения доклад са отразени вижданията и опитът на авторите по прилагане на правната рамка за защита на личните данни и

развитието на електронните медии. Основните моменти само са маркирани и до пълното им осмисляне и въвеждане в практиката предстои нелек път. Необходими са съвместни усилия на Националния надзорен орган, научните организации, електронните медии, физическите лица и бизнеса за еднаквото разбиране и тълкуване на изискванията на Регламента, за постигане на обща убеденост и практически действия за защита на правата и неприкосновеността на гражданите.

Представените модели ще бъдат в основата на изграждане на цялостна система за защита на данните в електронните медии, апробиране на резултатите и доказателство за адекватност с изискванията на Регламента.

Литература:

1. Reglament (ES)2016/679 na Evropejskiya parlament i syveta ot 27 april 2016 godina [Регламент (ЕС) 2016/679 на Европейския парламент и 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 Конвенцията на Съвета на Европа за защита на гражданите по отношение на автоматичната обработка на личните данни].

2. **Tselkov**, V., D. Petkow, G. Sredkov i Pl. Georgiev, Zashtita na dannite. Printsipi I praktiki, Vtoro prereboteno izdanie, Akademichno izdatelstwo „Za bukvite – O pismeneh“, 2020 g., 333 str., ISBN 978-619-185-441-7. [Целков, В., Д. Петков, Г. Средков и Пл. Георгиев, Защита на данните. Принципи и практики, Второ преработено издание, Академично издателство „За буквите – О писменехь“, 2020 г., 333 стр., ISBN 978-619-185-441-7]

3. **Tselkov**, V., S. Denchev I Ir. Peteva, Sigurnost na informacionnite resursi, Akademichno izdatelstwo “Za bukvite – O pismeneh”, 2020 g., 268 str., ISBN: ISBN 978-619-185-432-5. [Целков, В., С. Денчев и Ир. Петева, Сигурност на информационните ресурси, Академично издателство „За буквите – О писменехь“, 2020, 268 стр., ISBN: ISBN 978-619-185-432-5]

4. **Tselkov**, V. I G. Sredkov, Zashtita na li`nite danni i syotvetstvie s Reglament (ES) 2016/679, Nauchni trudiwe na UniBIT, Tom 18, 2020 g. [Целков, В. и Г. Средков, Защита на личните данни и съответствие с изискванията на Регламент (ЕС) 2016/679, Научни трудове на Университета по библиотекознание и информационни технологии, Том 18, 2020]

5. **Biolcheva**, P i G. Sredkov, Otsenka na vyzdejstvieto pri obrabotka na lichni danni v syotvetstvie s Reglament (ES)2016/679, UNSS, Yubilejna nauchno-prilozhna konferentsiya, 12-14 oktomvri 2018 g. [Биолчева, П., Средков, Г., Оценка на въздействието при обработване на лични данни в съответствие с Регламент (ЕС) 2016/679 (GDPR), УНСС, Юбилейна научно-приложна конференция, 12-14 октомври 2018]