ДИГИТАЛНА ТРАНСФОРМАЦИЯ НА ЗДРАВНОТО ЗАСТРАХОВАНЕ В КОНТЕКСТА НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

*Редовен докторант Тонина Янева
Икономически университет – Варна*

DIGITAL TRANSFORMATION OF HEALTH INSURANCE IN THE CONTEXT OF PERSONAL DATA PROTECTION

*Tonina Yaneva
University of economics – Varna*

Резюме: Дигиталната трансформация е една от най-важните детерминанти за устойчиво развитие. В отговор на повишените индивидуални изисквания на потребителите, застрахователите се изправят пред предизвикателството да адаптират дигиталните иновации в дейността си в съответствие с изискванията на законодателството за защита на личните данни на настоящи и потенциални клиенти и същевременно поддържат добър имидж и високо доверие сред тях.

Ключови думи: *GDPR, здравно застраховане, лични данни, кибератаки*

Abstract: The digital transformation is one of the most important determinants of sustainable development. In response to the increased consumers' requirements, the insurers face the challenge to adapt digital innovations in their activity in accordance with the requirements of current and potential customers' personal data protection legislation and at the same time to maintain a good image and high trust among them.

Key words: *GDPR, health insurance, personal data, cyber attacks*

DOI: <https://doi.org/10.36997/PPDD2021.180>

Въведение

Застрахователните дружества, в качеството си на администратори на лични данни, са длъжни да осъществяват своята дейност при стриктно спазване на изискванията на Закона за защита на личните

данни и Регламент (ЕС) 2016/679 на Европейския парламент и на съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни („Регламента“) с оглед осигуряване на поверителност и законосъобразно обработване на личните данни съгласно принципите, посочени в чл. 5 на Регламента. За изпълнение на целите за директен маркетинг на застрахователни продукти на настоящи и потенциални клиенти, управление на взаимоотношенията с клиенти, предлагане на персонализирани продукти и услуги чрез създаване на клиентски профил застрахователните компании, трябва да спазват задължението си да информират физическите лица за обработването на данни и да обезпечат упражняването на техните права. Обект на анализ в настоящия доклад е дигитализацията на здравните застрахователни продукти в контекста на Регламента, които се открояват като важна линия за бизнеса и завоюват все по-значим дял от премийния приход в животозастрахователния сектор в България. Глобалната пандемия COVID-19 провокира интереса на голяма част от населението към търсенето на медицински застраховки, осигуряващи бърз достъп до качествен медицински продукт и ускори процесите по дигитализация на целия търговски процес на тези застраховки. Целта на настоящата разработка е да се посочат предизвикателствата при имплементирането на основните принципи при обработване на лични данни при технологизирана пласментна верига на здравни застраховки и да се посочат проблемите, които може да възникнат при нарушение на сигурността на личните данни, както и да се изведат възможни мерки и алгоритъм за справяне с тях. Основни задачи, за да се постигне изпълнението на основната цел в настоящия доклад са:

- Да се специфицират личните данни, които застрахователите обработват при онлайн сключване на здравни застрахователни договори и условията за обработване на специални категории данни, изразяващи се като общи изключения от забраната за обработване.
- Да се проучи адаптирането на основните принципи при обработване на лични данни към продажбения процес на медицински застраховки в онлайн среда.
- Да се проучат най-честите нарушения на сигурността на личните данни и да се предложи алгоритъм за справяне и предотвратяване на кибератаки и други онлайн престъпления при обработката

и съхранението на данни за дигитална продажба и след продажбено обслужване на медицински застраховки.

Изложение

Клиентските данни винаги са били от фундаментално значение за застраховането, тъй като целият бизнес разчита на определена информация, с чиято помощ да се оцени рискът и да се взимат оптимални решения. Законодателството за защита на лични данни регламентира всяко обработване на лични данни на физически лица, което включва събиране, записване, организиране, структуриране, съхранение, изменение, достъпност, консултация, използване, разкриване, разпространение, изтриване или унищожаване, както и всеки друг начин, по който данните стават достъпни.

Основен приоритет на застрахователните компании е осигуряване на много добро клиентско изживяване в дигитална среда, предоставяйки персонализирани застрахователни продукти, с лесен достъп и бързина на получаване на оферта и покупка, както и поддържане и гарантиране на високо ниво на обслужване на клиентите. Ползвателите на застрахователни услуги са едни от основните действащи лица по GDPR като субекти на лични данни. Застрахователите, които разполагат с уеб сайт или мобилно приложение, през които клиентите могат да получат оферта и сключат застрахователна полица дистанционно, се отличават със значително конкурентно предимство пред своите конкуренти. Получаването на оферта през онлайн порталите изисква регистрация на потребителите и предоставяне на лични данни. Личните данни, които могат да се предоставят на застрахователите за обработка в различните етапи на дистанционен продажбен процес са описани във фигура 1.

Здравните данни са всички данни, които разкриват физическото или здравословно състояние на дадено лице и се квалифицират по GDPR като специални (чувствителни) данни. По Регламента са установени общи изключения от забраната за обработване, които намират израз в условия за обработване на специални категории данни.

Фигура 1. Категории данни, обработвани при различните етапи от дигиталния продажбен процес на медицински застраховки.

Източник: съставено от автора.

Обработването на данни за здравословното състояние на ползвателите на застрахователни услуги е необходимо за сключването и изпълнението, при определени съгласно разпоредбите на Кодекса за застраховането застрахователни договори (чл. 454 на КЗ) и респективно не се ползва съгласие като нормативно основание по GDPR. Преди сключване на застрахователен договор, както и по време на действието на договора, застрахователят има право да получи подробна и точна информация относно здравословното състояние на лицето, чийто живот, здраве или телесна цялост са предмет на застраховане. При настъпване на застрахователно събитие застрахователят има право на достъп до цялата медицинска документация във връзка със здравословното състояние на лицето, чийто живот, здраве и телесна цялост са застраховани, като може да я изисква от всички лица (лични лекари, лечебни заведения или институции), съхраняващи такава информация, включително съгласно Закона за лечебните заведения, Закона за здравното осигуряване и Закона за здравето и др. Законосъобразното обработване на лични данни включва пропорционалното използване на лични данни за целите, за които са събрани на законово основание и за периода време, необходим за по-

стигане на одобрените цели в съответствие с определените срокове за съхранение.

Таблица 1

Цели според основанията за законосъобразно обработване на лични данни

Цели за обработване на лични данни на основание законни задължения	<ul style="list-style-type: none"> • Комплексна проверка (идентификация, верификация и приемане) на ползватели на застрахователни услуги • Изготвяне на отчети до регулаторни органи • Докладване до регулаторни органи съгласно разпоредбите на Данъчно-осигурителния процесуален кодекс • Осъществяване на контрол и предотвратяване на застрахователни измами и конфликт на интереси • Защита на данните и информационните системи • Предоставяне на лични данни на държавни и контролни органи по техни правомощия • Анализ на потребностите и категоризиране на клиенти с цел изпълнения на изискванията на Кодекса за застраховането за предоставяне на продукт, отговарящ на изискванията и потребностите на клиента
Цели за обработване на лични данни на основание изпълнение на договор	<ul style="list-style-type: none"> • Оценка на застрахователния риск и изчисляване на застрахователната премия • Изготвяне на индивидуално предложение за сключване на застраховка • Изготвяне на застрахователен договор и изпълнение на законните задължения по сключването му • Анализ на нуждите на ползвателите на застрахователни услуги • Обработка на застрахователни претенции във връзка с настъпили застрахователни събития • Използване на продукти и услуги във връзка със сключен застрахователен договор
Цели за обработване на лични данни на основание законни интереси на администратора	<ul style="list-style-type: none"> • Тестване на нови и промени в съществуващите софтуерни приложения, демонстрационни платформи и вътрешни портали с оглед актуализация, валидация, разрешаване на инциденти, осигуряване на защита на данните, обучение на служители • Проучване и развитие на продукти и анализ на пазарни тенденции • Директен маркетинг на застрахователни продукти • Управление на взаимоотношенията с клиенти с цел предлагане на застрахователни продукти • Създаване на аналитични бизнес модели с цел развитие на нови продукти и услуги • Предотвратяване и разкриване на измами • Управление на връзките с клиенти с цел предоставяне на по-добро обслужване от дигитални дистрибуционни канали
Цели за обработване на лични данни на основание съгласие	<ul style="list-style-type: none"> • Предлагане на персонални продукти за настоящи клиенти чрез създаване на клиентски профил • Директен маркетинг на застрахователни продукти на потенциални клиенти

Източник: адаптирано от автора по *Защита на личните данни (2021)*, (<https://www.dzi.bg/privacy>, 13.09.2021).

С цел директен маркетинг и предлагане на персонални продукти и услуги, посредством изготвяне на точен клиентски профил, е необходимо потенциалните и настоящите клиенти да дадат свободно изрично писмено съгласие на застрахователя да обработва личните данни при строга конфиденциалност и в съответствие с приложимите нормативни изисквания към маркетинговото таргетиране на потребителите. Съгласието няма да е валидно, ако неговото непредоставяне би имало неблагоприятни последици за субекта, като например по-висока цена на услуга или сключването на договор да зависи от предоставянето на съгласие. Изграждането на доверие между застра-

хователя (администратор на лични данни) и потребителя на здравни застраховки (субект на лични данни) е възможност за справяне с предизвикателствата при обработване на данни в дигитална среда (Зисов, „Боянов и Ко.“, Николова 2015) . Съгласието по смисъла на GDPR се дава чрез *ясно утвърдителен акт*, изявяващ недвусмислената индикация от страна на субекта на данни, че той разрешава данните му да бъдат обработвани за съответните цели (Вълова 2020). Съгласието трябва да изпълнява следните условия: да бъде волеизявление на физическо лице, да бъде свободно изразено, конкретно, недвусмислено, информирано. Липсата дори и на един от компонентите може да доведе до невалидност на съгласието. Съгласието за директен маркетинг е валидно, ако е дадено преди изпращане на рекламно съобщение. В тази връзка е препоръчително застрахователите да поддържат регистър с получените изявления за съгласие. Основно право на субекта на данни по отношение на неговите данни, което правната рамка постановява, е оттегляне на съгласие. За да намалят риска от санкции, заради неправилен директен маркетинг, е целесъобразно да бъде поддържан *специален списък с лица*, които са оттеглили своето съгласие или са възразили срещу получаването на маркетингови материали. За да отговори на законовите изисквания, да не пропуска ползи и да не подлежи на санкции и глоби, застрахователният бизнес много бързо създава организация по събирането на декларации за съгласие от своите настоящи и бъдещи клиенти. Застрахователите трябваше да въведат определен механизъм при регистрация в уеб сайт или при инсталиране на приложение, по които клиентите информирани да отбелязват съгласие за обработка на лични данни чрез специфичен, уведомителен знак (примерно с отметка). Застрахователите трябва да инвестират в технически обезпечени системи за идентификация на физическите лица, посредством които клиентите да заявяват съгласие в онлайн среда и да се постигне еднообразно прилагане на съгласие с оглед защита на лични данни, независимо дали обработката става онлайн или офлайн.

Използването на големи бази данни в здравното застраховане не е систематично и повсеместно, но има голям потенциал да се увеличи и да се превърне в стандартна практика. Доклад от IMS Institute for Healthcare Informatics показва, че мобилните здравни приложения, които се предлагат на пазара, са се удвоили през последните две години и са повече от 165 000 приложения (The Precious 2019). Голям

процент от тези приложения са фокусирани върху здравословния начин на живот, като статистиката сочи, че едва 2% от застрахователите използват данни от мобилните приложения. Според световния застрахователен доклад за 2019 г. 37% от потребителите на застрахователни продукти, интервюирани в световен мащаб, са заявили своята готовност да споделят допълнителни данни за контрол на риска и услуги, свързани с превенция (World Insurance Report 2019) . Посредством данните, предоставяни от мобилни устройства, застрахователите идентифицират рисковите фактори, създават диференцирани потребителски сегменти, анализират здравословното състояние на потребителите и предлагат конкретни програми за профилактика, подобряване на здравето и предпазване от заболявания на застрахованите лица.

Нарушение на сигурността (вж. фиг. 2) на данни възниква, когато данните, за които застрахователят отговаря, са засегнати от инцидент със сигурността, в резултат на който се нарушава поверителността, наличието или целостта на данните. Ако това се случи и има вероятност нарушението да представлява риск за правата на дадено лице, дружеството трябва да уведоми надзорния орган (Комисия за защита на личните данни – КЗЛД) без ненужно забавяне и най-късно до 72 часа, след като е установено нарушението.

Фигура 2. Основни групи нарушения на сигурността при дигитална продажба на здравни застраховки.

Източник: съставено от автора.

Като нарушение на сигурността на лични данни в медицинско застраховане се определя събитие, водещо до случайно или неправо-

мерно унищожаване,¹ загуба,² промяна, неразрешено разкриване или достъп до лични данни, които се предават, разкриват, съхраняват или обработват.

В следствие на глобалната пандемия от COVID-19 настъпи съществена промяна, при която 91% от работната сила в застрахователния сектор работи дистанционно или от дома (home office) (2020 CIO Survey Insurance industry insights 2020). В резултат на това четири от десет организации съобщават за увеличаване на инциденти в киберсигурността с фишинг (89%) и атаките на зловреден софтуер (67%), като при застрахователите процентът е малко над средния в сравнение с останалите сектори (вж. фиг. 3). В по-широк и дългосрочен план устойчивостта и стабилното управление на риска са ключови за застрахователните компании. В контекста на пандемията приоритет в бъдеще за застрахователите се явява повишеният фокус върху вътрешните заплахы, произтичащи от стремежа за увеличаване на цифровизацията на застрахователните услуги, новите пакети дигитални приложения и тенденцията за отдалечена работа на служителите.

Фиг. 3. Видове кибер атаки в застрахователния и другите сектори.

Източник: 2020 Harvey Nash/KPMG CIO Survey, KPMG International.

За да реагират адекватно на кибератаките и да предотвратяват своевременно нарушението на сигурността на данните, застраховате-

¹ Унищожаване на данни е налице, когато данните вече не съществуват/ не съществуват във формата, в която могат да се ползват от администратора.

² Загуба на данни е налице, когато личните данни съществуват, но администратора е загубил контрол (достъп) на фактическата власт върху тях.

лите трябва да взаимодействат с експерти в областта на GDPR и информационните технологии, като в бъдеще инвестират в обучението и квалификацията на хибридни специалисти, съчетаващи знания и професионални умения в трите области – застраховане, законодателство и ИТ. Застрахователните компании трябва да имплементират в дейността си надеждни и ефективни процеси по управление на инциденти, с ясни етапи на изпълнение (вж. фиг. 4) и да обезпечат надеждност при обработка, информационна сигурност и предотвратяване на изтичането на данни, спазвайки един от основните принципи на цялостност и поверителност.

Фиг. 4. Етапи за действие при нарушение на сигурността на данните.

Източник: съставено от автора.

Заклучение

Дигиталната трансформация на бизнеса акцентира все по-устойчиво върху стратегията на българските застрахователни компании за завоюване на по-голям пазарен дял, като достъпът и законосъобразното обработване и съхранение на данни се превръщат в значително конкурентно предимство. Дигитализацията на процесите в здравното застраховане и своевременната им адаптация към строгите регулаторни изисквания за защита на личните данни създават възможност за повишаване на социалното благополучие и по-нататъшно подобрене на жизнения стандарт на живот на ползвателите на застрахователни услуги в национален мащаб.

Използвана литература

Вълова, Й. (2020). Директният маркетинг в контекста на GDPR. Правни акценти. Делойт Лигъл.

Valova, Y. (2020). Direktniyat marketing v konteksta na GDPR. Pravni aktsenti. Deloitte Legal.

Защита на личните данни (2021), (<https://www.dzi.bg/privacy>, 13.09.2021).

Zashtita na lichnite danni (2021). Retrieved Septamvri 13, 2021, from DZI: (<https://www.dzi.bg/privacy>, 13.09.2021).

Зисов, Н., „Боянов и Ко.“, Н. Николова (2015). Правни аспекти на съгласието за обработка на личните данни в дигитална среда. // Конференция „Доверие, неприкосновеност и сигурност на личните данни в цифровия свят“. София. Комисия за защита на личните данни: (<https://cpdp.bg>, 13.09.2021).

Zisov, N., „Boyannov i Ko.“, N. Nikolva (2015). Pravni aspekti na saglasieto za obrabotka na lichnite danni v digitalna sreda. Konferenciya „Doverie, neprikosnovenost i sigurnost na lichnite danni v cifroviya svyat“. Sofiya. Komisiya za zashtita na lichnite danni. (<https://cpdp.bg>, 13.09.2021).

2020 CIO Survey Insurance industry insights (2020). // KPMG (<https://home.kpmg/xx/en/home/insights/2021/02/cio-survey-2020-insurance-industry-insights.html>, 13.09. 2021).

Harvey Nash // KPMG CIO Survey 2020: Everything changed. Or did it? (2020), (<https://home.kpmg/xx/en/home/insights/2020/09/harvey-nash-kpmg-cio-survey-2020-everything-changed-or-did-it.html>, 13.09.2021).

The Precious (2019), (<http://www.thepreciousproject.eu/?p=922>, 10. 05.2021).

World Insurance Report (2019), (<https://worldinsurancereport.com/resources/world-insurance-report-2019>, 15.05.2021).

За контакти: Редовен докторант Тонина Янева
Икономически университет – Варна
e-mail: tonina.yaneva@ue-varna.bg