ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ И ДИГИТАЛИЗАЦИЯТА – ПРЕДИЗВИКАТЕЛСТВА И ПЕРСПЕКТИВИ

Сборник с доклади

ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ И ДИГИТАЛИЗАЦИЯТА – ПРЕДИЗВИКАТЕЛСТВА И ПЕРСПЕКТИВИ

Сборник с доклади

PROTECTION OF THE PERSONAL DATA AND THE DIGITALIZATION – CHALLENGES AND PERSPECTIVES

Conference proceedings

2021

Издателство „Наука и икономика“
Икономически университет – Варна

Сборникът се издава като резултат от кръглата маса „Защитата на личните данни и дигитализацията – предизвикателства и перспективи“, проведена на 1 октомври 2021 г. в Икономически университет – Варна. Научният форум е проведен от катедра „Правни науки“ и Научноизследователския институт при Икономически университет – Варна.

Всички публикувани материали са рецензирани от утвърдени и водещи в съответната научна област специалисти, включени в Редакционния съвет.

The book is published as a result of a round table “Protection of the personal data and the digitalization – challenges and perspecives”, which took place at 1st October 2021 in the University of Economics – Varna. The scientific forum was organized by the Legal sciences Department and The Research Institute of the University of Economics – Varna

All published reports are refereed by acknowledged and leading specialists in the respective scientific area, members of the Editorial board.

DOI: https://doi.org/10.36997/PPDD2021

ISBN 978-954-21-1002-3

ОРГАНИЗАЦИОНЕН КОМИТЕТ

Председател:

доц. д-р Андрияна Андреева – ръководител катедра „Правни науки“

Членове:

доц. д-р Галина Йолова

гл. ас. д-р Живка Матеева

гл. ас. д-р Диана Димитрова

РЕДАКЦИОНЕН СЪВЕТ

доц. д-р Андрияна Андреева –
ръководител катедра „Правни науки“, ИУ – Варна

доц. д-р Галина Йолова –
ИУ – Варна, катедра „Правни науки“

КОНТАКТИ:

9002, гр. Варна, бул. „Княз Борис I“ №77
Икономически университет – Варна Катедра „Правни науки“
E-mail: katedra_pn@ue-varna.bg

ORGANIZING COMMITEE

Chairman:

Assoc. Prof. Andriyana Andreeva, PhD –
"Legal sciences" Department, UE – Varna

Members:

Assoc. Prof. Galina Yolova, PhD

Chief Assist. Prof. Zhivka Mateeva, PhD

Chief Assist. Prof. Diana Dimitrova, PhD

EDITORIAL BOARD

Assoc. Prof. Andriyana Andreeva, PhD
Head of "Legal sciences" Department, UE – Varna

Assoc. Prof. Galina Yolova, PhD
"Legal sciences" Department, UE – Varna

CONTACTS:

9002, Varna, 77, Knyaz Boris I Blvd.
University of Economics – Varna
„Legal sciences" Department
E-mail: katedra_pn@ue-varna.bg

СЪДЪРЖАНИЕ

ЗАЩИТА НА ДАННИТЕ ПО ПОДРАЗБИРАНЕ И НА ЕТАПА НА ПРОЕКТИРАНЕ В ЕПОХАТА НА ДИГИТАЛИЗАЦИЯТА

Венцислав Караджов
председател на Комисията за защита на личните данни
и заместник-председател на Европейския комитет
по защита на данните

DATA PROTECTION BY DEFAULT AND BY DESIGN IN THE AGE OF DIGITALISATION

Ventsislav Karadjov
Chairman Commission for Personal Data Protection
and Deputy Chair of the European Data Protection Board

Резюме: Концепцията на защита на данните по подразбиране и на етапа на проектиране е основополагаща за разбирането на съвременните процеси по защита на личните данни. Принципът *защита на данните на етапа на проектирането* е въведен да защити правата на физическите лица при автоматизирано обработване на лични данни. Той следва да намери отражение във всички съвременни проявления на дигитализацията, включително изкуствения интелект. Естествено негово продължение е защитата на данните по подразбиране.

Ключови думи: *лични данни, защита на данните, защита по подразбиране, защита на етапа на проектиране, дигитализация*

Abstract: The concept of data protection by default and by design is fundamental step for understanding contemporary personal data protection processes. The principle of "data protection by design" has been introduced to protect the rights of individuals in the automated processing of personal data. It should be reflected in all contemporary epitome of digitalisation, including artificial intelligence. Its continuation is the data protection by default.

Key words: *personal data, data protection, data protection by default, data protection by design, digitisation*

DOI: https://doi.org/10.36997/PPDD2021.9

Въведение

В последните три десетилетия, и най-вече през последните няколко години, личните данни на физическите лица все по-ясно и отчетливо се дефинират и налагат като защитимо право. На международно ниво Насоките на Организацията за икономическо сътрудничество и развитие (ОИСР) за защита на личните данни и задграничния им трансфер от 1980 г. (актуализирани през 2013 г.) и приетата малко след тях Конвенция на Съвета на Европа за защитата на физически лица по отношение на автоматизираното обработване лични данни (1981 г.) задават първоначалните стандарти за защита на личните данни при обработването им с автоматизирани средства.

Самото понятие за защита на данните на етапа на проектирането е разработено за приложение в дигиталния контекст на обработване на данни. Това е подход към разработване на информационни системи, изначално развит от г-жа Анн Кавукиан и формализиран през 1995 г. от съвместен доклад относно технологии за подобряване на поверителността на съвместен експертен екип на Комисаря по Информация и неприкосновеност на Онтарио, Нидерландския орган по защита на данните и Нидерландската организация за приложни научни изследвания. Правната рамка по защита на данните на етапа на проектирането е публикувана през 2009 г., а през следващата 2010 г. е приета и от Глобалната асамблея за защита на данните.

Защитата на данните на етапа на проектирането вменява задължението за включване на елемента за поверителност на данните през целия инженерен процес по разработване на дигитален продукт, т.е. защитата на данните следва да е концептуално заложен елемент в момента на разработване, а не нещо добавяно като допълнителна стойност при вече разработен и/или приключил дизайн на продукт. Този подход се възприема като *дизайн ориентиран към ценностите*, тъй като взема предвид общочовешките ценности по един ясно дефиниран начин през целия процес на разработване.

За описания времеви период се разви и процесът на дигитализация, който е една степен отвъд простото обработване на лични данни с технически средства. Дигитализацията по дефиниция е трансформация на всякакъв вид материална форма в поредица от знаци, предназначени за електронна обработка и предаване. В този контекст се

наложи и задълбочаване и детайлизиране на правните разпоредби за защита на данните, за да се отговори на настъпващата глобална дигитализация.

С въвеждането на изцяло новата правна рамка за защита на данните на ниво Европейски съюз, беше приет Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД), който се прилага пряко от 25 май 2018 г. Това е нормативният акт, определящ правилата, свързани със защитата на физическите лица при обработването на личните им данни и относно свободното движение на тези данни. Общият регламент надгражда предишния режим за защита на данните, въведен от Директива 95/46/ЕО, транспонирана в българския Закон за защита на личните данни от 2002 г., като в същото време отчита динамиката на развитието на новите технологии и на дейностите по обработка на лични данни. Този акт има директно и пряко приложение по отношение на всички държави – членки на ЕС, като правата и задълженията, произтичащи от него, са приложими на недискриминационен принцип както по отношение на частноправни субекти, така и на публични организации. Тази правна реформа в рамката на ЕС включва и приемането на Директива (ЕС) 2016/680 на Европейския парламент и Съвета относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета.

И двата европейски законодателни акта въвеждат изискването за защита на личните данни на етапа на проектирането и по подразбиране – съответно съображения 78 и 108 и чл. 25 от Регламент (ЕС) 2016/679 и съображения 53 и 55 и чл. 20 от Директива 2016/680. По този начин се обезпечава еднаквото и правилно прилагане на принципите за защита на неприкосновеността на личните данни на физическите лица както в чисто граждански и търговски аспект, така и в рамките на обработването на данни от правоприлагащи и правоохранителни органи. Този подход налага задължение на всеки администратор, обработващ лични данни, без значение от конкретната цел, за която той обработва данните, така да разработи и поддържа системите си, че да гарантира еднакъв, завишен и постоянен стандарт на защита.

Изложение

I. Защита на данните на етапа на проектиране

В рамките на Регламент (ЕС) 2016/679 защитата на данните на етапа на проектирането е базиран на седем *фундаментални принципа*:

- Проактивен, а не реактивен подход (превенция, а не последващо саниране).
- Настройката за поверителност да е зададена като default.
- Вграждане на поверителността в самия дизайн.
- Пълна функционалност – positive-sum, not zero-sum.
- Сигурност от край до край – пълен цикъл на защита.
- Видимост и прозрачност.
- Фокус към потребителя с уважение към поверителността му.

Технологиите за подобряване на поверителността дават възможност на ползвателите да защитят личната информация, която ги идентифицира, когато я предоставят или я управляват чрез услуги и приложения. Налице са много аспекти на защитата на данните на етапа на проектирането, включително при софтуерното разработване и инженерното разгръщане на системи, които включват административни елементи (например правна документация, политика за поверителност, процедури за преглед и при нарушение на сигурността), но предполагат и контрол в рамките на организацията, която използва технологията, както и адаптиране в контекста на конкретния бизнес процес. По този начин се налага да се вложат усилия за реализиране на принципа за справедлива информация, който да се внедри в дизайна и функционалността на информационните и комуникационните технологии. По този начин – при наличието на гаранции за поверителността на продукта от самото му разработване, администраторът на лични данни ще е в състояние (при спазване на принципа за защита на данните по подразбиране) да докаже, че обработва лични данни законосъобразно, в необходимия обем и без да ги съхранява за неприложим период от време.

Следва да бъдат установени отговорностите и задълженията на администратора за всяко обработване на лични данни, извършено от администратора или от негово име. По-специално, администраторът следва да е длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съот-

ветствие с Регламент (ЕС) 2016/679, включително ефективността на мерките. Тези мерки следва да отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица.

Когато се обсъжда минимумът от отговорности и задължения на администратора на лични данни, те се обуславят от общите принципи за защита на данните (чл. 5 от Регламент (ЕС) 2016/679, а именно: законосъобразност, ограничаване на целите за обработване, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност и поверителност, отчетност.

В този смисъл бизнес ориентираният подход на етапа на разработването на дигитален продукт би бил да се направи преглед, който да търси и да даде отговор на следните условия:

- Трябва ли наистина да събирам тези данни?
- Могат ли данните да бъдат анонимизирани или псевдонимизирани и да продължат да ми вършат работа?
- Какви други допълнителни данни могат да бъдат събрани и трябва ли да искам тези данни?
- Коя е заплахата?
- Какви категории или класове данни могат да бъдат засегнати?

Точно такъв подход ще гарантира и ориентирано към риска разработване, което да позволи и последващо актуализиране на технологията по начин, който ще създаде възможност за надграждане на защитата по обработване на данните по подразбиране (разглеждана по-долу). Понятието за риск за правата и свободите на физическите лица може да произтича от обработването на лични данни, което да доведе до физически, материални или нематериални вреди, да породи 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. В подобни случаи субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни, особено когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, както и обработването на генетични данни, данни за здравословното

състояние или данни за сексуалния живот или за присъди и нарушения, или за свързаните с тях мерки за сигурност.

Не на последно място е налице риск, 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. Специално внимание Регламент (ЕС) 2016/679 отделя на обработването на данни на уязвими лица, по-специално на деца, и в националното законодателство е въведено ограничение за обработване на такива данни на лица под 14- годишна възраст (чл. 25в от Закона за защита на личните данни). Когато обработването включва голям обем лични данни и засяга голям брой субекти на данни по дефиниция се приема, че е налице завишен риск за правата на физическите лица, което и налага подробен и ориентиран към защитата на поверителността дизайн.

Вероятността и тежестта на риска за правата и свободите на субекта на данни следва да се определят с оглед на естеството, обхвата, контекста и целта на обработването. Рискът следва да се оценява въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до *риск* или до *висок риск*. От тази оценка произтича и необходимостта от предварителна консултация с компетентен надзорен орган по реда на чл. 36 от Регламент (ЕС) 2016/679.

Инструмент, който е изключително полезен за администраторите на лични данни при спазването на изискванията на защита на данните на етапа на проектирането са Насоки № 4/2019 относно чл. 25 – Защита на данните на етапа на проектирането и по подразбиране на Европейския комитет по защита на данните, приети на 20 октомври 2020 г. В тях ясно е посочено, че задължение на администратора е да прилага подходящи технически и организационни мерки и необходимите гаранции в процеса на обработване.

В тези насоки ЕКЗД конкретно сочи, че дадена техническа или организационна мярка и гаранция може да включва всичко — от използване на усъвършенствани технически решения до основно обучение на персонала. Примерите, които могат да са подходящи в зависимост от характера на дейността, и рисковете, свързани със съ-

ответната операция по обработване, включват псевдонимизация на лични данни, съхранение на наличните лични данни в структуриран, широко използван и пригоден за машинно четене формат, предоставяне на възможност на субектите на данни да се намесват в дейността по обработване, предоставяне на информация за съхранението на лични данни, експлоатация на системи за откриване на зловреден софтуер, организиране на обучение на служителите по базова *кибер-хигиена*, въвеждане на системи за управление на неприкосновеността на личния живот и сигурността на информацията, въвеждане на договорни задължения за обработващите лични данни да прилагат определени практики за свеждане на данните до минимум и т.н.

Изрично се подчертава, че ефективността не изисква осъществяването на специфични технически или организационни мерки, т.е. прилагането на конкретен набор от мерки, а напротив, ефективността изисква да се докаже, че избраните мерки и гаранции са подходящи с оглед на прилагането на принципите на защита на данните в рамките на разглежданата дейност по обработване. Във връзка с това мерките и гаранциите следва да бъдат разработени така, че да са надеждни, а администраторът трябва да има капацитет да реализира допълнителни мерки, за да противодейства на възможно нарастване на нивото на риска. Следователно ефективността на мерките зависи от характера на конкретната дейност по обработване и от оценката на определени елементи, които трябва да се вземат предвид, когато се определят средствата за обработване.

Друг съществен елемент застъпен от ЕКЗД е практическото прилагане на критерия „достижения на техническия прогрес“, който се отнася не само до технологичните, но и до организационните мерки. Липсата на подходящи организационни мерки може да намали или дори изцяло да подкопае ефективността на избраната технология. Примерите за организационни мерки включват приемане на вътрешни политики, обучение, насочено към придобиване на актуални знания за дадена технология, сигурност и защита на данните, политики за управление на сигурността и административно управление на информационните технологии.

Пример: Използване на псевдонимизация (замяна на лично идентифицируем материал с изкуствени идентификатори) и криптиране (кодиране на съобщения така, че да могат да ги прочетат само оторизираните лица).

Важен елемент също така е определянето на *средствата за обработване*, които варират от общите до конкретните елементи при проектирането на обработването, включително архитектурата, процедурите, протоколите, оформлението и външния вид. Същевременно *моментът на определяне на средствата за обработване* се отнася до периода от време, когато администраторът взема решение относно начина на осъществяване на обработването и механизмите, посредством които ще се осъществи то.

Именно в контекста на горното се определя и, впоследствие, защитата на данните по подразбиране. Това обработване по подразбиране, което ще допълва и поддържа обработването на данни на етапа на проектиране, ще гарантира, че при едно добро планиране на защитата на данните на етапа на проектирането, последващото актуализиране ще гарантира все така завишено ниво на защита на неприкосновеността.

II. Защита на данните по подразбиране

Защитата на данните по подразбиране представлява принцип, според който администратор на лични данни обработва само данни, които са изрично необходими за всяка отделна цел, за която се обработват, без намесата на ползвателя на съответната технология. Съгласно тълкуването на ЕКЗД, понятието „по подразбиране“ при обработването на лични данни се отнася до определянето на стойности за конфигуриране или функции за обработване, които са зададени или предварително определени в рамките на система за обработване, като например софтуерно приложение, услуга или устройство, или процедура за ръчно обработване, които оказват въздействие върху обема на събраните лични данни, обхвата на тяхното обработване, периода на тяхното съхранение и тяхната достъпност. Администраторът следва да отговаря за въвеждането на такива настройки и опции „по подразбиране“, които да позволяват само обработване, което е строго необходимо за постигане на определената законосъобразна цел.

В контекста на дигитализацията има няколко практични стъпки, които ще гарантират, минимум, че обработването отговаря на изискването „по подразбиране“:

- Необходими ли са ми данните, които обработвам?
- Колко дълго се обработват личните данни?
- Кой има достъп до тези данни?

Администраторите следва да вземат предвид както обема на личните данни, така и видовете, категориите и нивото на детайлност на личните данни, необходими за целите на обработването. Когато събират големи обеми от лични данни, на етапа на проектирането те трябва да отчетат увеличения риск за принципите на цялостност и поверителност, да сведат данните до минимум и да ограничат съхранението, както и да го сравнят с намаления риск при събиране на намалени обеми и/или не толкова подробна информация за субектите на данни.

За описаните по-горе цели е неизбежно администраторът на лични данни да прави периодичен преглед и актуализация на настройките на изпитваната програма, приложение и т.н., както и да актуализира политиките си за поверителност, успоредно с напредъка на технологиите, които използва. Като примери в тази насока могат да се използват актуализирането на настройките „по подразбиране“ относно периодите за съхранение на данните в зависимост от варирашите изисквания за допустимите срокове за съхранение.

Особено съществен елемент при защитата по подразбиране е достъпността на данните и, в частност, контролът на достъпа до тези данни през цялото време на обработване. Дигитализацията като цяло предполага свързването на множество софтуерни продукти и предаването на данни чрез тях, в този смисъл, както и ЕКЗД подчертава, че без изрична човешка намеса/контрол, личните данни не трябва да бъдат достъпни за неограничен брой физически лица. По подразбиране администраторът трябва да ограничи достъпа и да предостави на субекта на данните възможност да се намеси, преди да публикува или по друг начин да предостави лични данни за субекта на данни на неограничен брой физически лица.

Предоставянето на достъп до лични данни на неограничен брой физически лица може да доведе до още по-широко разпространение на данните от предвиденото. Това е от особено значение при използването на интернет търсачките. Следователно, по подразбиране, администраторите следва да предоставят на субектите на данни възможност да се намесят, преди техните лични данни да бъдат предоставени за свободен достъп в интернет. Това е от особена важност, когато става дума за деца и лица от уязвими групи, както беше посочено и по повод рисковете на етапа на проектирането, които са приложими в цялост и при разработване на системата за поверителност

по подразбиране.

Пример: Социална медийна платформа трябва да се насърчи да зададе такива настройки на потребителските профили, които са най-благоприятни за неприкосновеността на личния живот, като например ограничи от самото начало достъпността до потребителските профили, за да не бъдат достъпни по подразбиране за неопределен брой лица.

Заключение

От особено значение и за двете системи за гарантиране на високо ниво на защита на личните данни е предоставянето на информация на крайния потребител. Част от принципите на *дизайн, ориентиран към ценностите* е зачитането на информираността на субектите на данни. От администраторите се дължи открита, ясна и точна информация какви данни ще бъдат обработвани, как ще се събират и обработват и ще бъдат ли предавани на трети лица. За тази цел ЕКЗД извежда в цитираното становище няколко основни принципа:

- яснота: информацията трябва да е представена на ясен и достъпен език, да бъде кратка и разбираема;
- смисъл: съобщенията следва да имат ясно значение за конкретната аудитория;
- достъпност: информацията трябва да е лесно достъпна за субекта на данните;
- контекст: информацията следва да е предоставена в правилния момент и в подходяща форма;
- уместност: информацията следва да е съотносима и приложима към конкретния субект на данни;
- универсална форма: информацията трябва да бъде достъпна за всички субекти на данни, да включва използване на подлежащи на машинно четене езици, за да се улесни и автоматизира четимостта и яснотата;
- разбираема: субектите на данни трябва да разбират достатъчно добре какво могат да очакват във връзка с обработването на личните им данни, особено когато става дума за деца или членове на други уязвими групи;
- различни комуникационни канали: информацията трябва да се предоставя чрез различни канали и медии, не само чрез писмен текст,

за да повиши вероятността за реално достигне на информацията до субекта на данните;

• структурирана в различни нива: информацията следва да бъде структурирана в различни нива по такъв начин, по който да бъде преодоляно противоречието между изисквания за пълнота и разбираемост, като същевременно се вземат предвид разумните очаквания на субектите на данни.

Използвана литература

Европейска комисия. (н.д.). Какво означава защитата на данните „на етапа на проектирането“ и „по подразбиране“? (https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_bg, 27.09.2021).

Evropeyska komisia. (n.d.). Kakvo oznachava zashtitata na dannite „na etapa na proektiraneto“ i „po podrazbirane“? (https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_bg, 7.09.2021).

Европейски комитет по защита на данните (2019). Насоки № 4/2019 относно член 25 Защита на данните на етапа на проектирането и по подразбиране. Брюксел: Европейски комитет по защита на данните.

Evropeyski komitet po zashtita na dannite (2019). Nasoki № 4/2019 otnosno chlen 25 Zashtita na dannite na etapa na proektiraneto i po podrazbirane. Bryuksel: Evropeyski komitet po zashtita na dannite.

Проект № 2007CB16IPO007-2011-2-06 Дигитална култура за регионално сближаване, съфинансиран от ЕС чрез Програма за ТГС по ИПП № 2007CB16IPO007.

Proekt № 2007CB16IPO007-2011-2-06 Digitalna kultura za regionalno sblizhavane, safinansiran ot ES chrez Programa za TGS po IPP № 2007CB16IPO007.

A Guide to Privacy by Design (2019). Madrid: Agencia Espanola Proteccion Datos.

Giannakakis, I. (2019). Privacy by Design and By Default. A Practical Guide for the Digital Era.

Mauritius: LAP Lambert Academic Publishing.

Jason Cronk, R. C. C. (2018). Strategic Privacy by Design. Oberlin, Ohio: IAPP, p. 278.

Stallings, W. (2020). Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices. Pearson Education Inc.

Resolution on Privacy by Design (2010). // 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem: Global Privacy Assembly.

За контакти: Венцислав Караджов
Комисията за защита на личните данни
e-mail: kzld@cpdp.bg

НЯКОИ АСПЕКТИ НА ЗАЩИТАТА НА ДАННИ ПРИ ПРОВЕЖДАНЕ НА НАУЧНИ ИЗСЛЕДВАНИЯ

доц. д-р Петя Данкова
Икономически университет – Варна

ON SOME ASPECTS OF DATA PROTECTION IN SCIENTIFIC RESEARCH

Assoc. Professor Dr. Petya Dankova
University of Economics – Varna

Резюме: Настоящият доклад разглежда някои проблеми, свързани със събирането, обработката, съхранението и защитата на лични данни при провеждане на научни изследвания. Представени са основни моменти от Общия регламент относно защитата на данните и Европейския етичен кодекс за почтеност на научните изследвания, касаещи нормативните и етични аспекти при провеждане на научни изследвания.

Ключови думи: *изследователска етика, защита на данните, Общ регламент относно защитата на данните, Европейски етичен кодекс за почтеност на научните изследвания.*

Abstract: This paper discusses issues related to gathering, processing and protection of personal data in scientific research. Highlights of the General Regulation on Data Protection and the European Code of Conduct for Research Intregrity concerning the regulatory and ethical aspects of research are presented.

Key words: *research ethics, data protection, General Data Protection Regulation (GDPR), European Code of Conduct for Research Intregrity.*

DOI: https://doi.org/10.36997/PPDD2021.21

Въведение

Развитието на информационните технологии в последните години създава все повече възможности за натрупване и обработване на данни за целите на научноизследователската дейност. Заедно с това

обаче на преден план се открояват и въпроси, свързани със законовите и етични аспекти при събирането, обработването и съхраняването на тези данни. В тази връзка изследователите следва да познават и прилагат в своята практика редица европейски документи, в това число Общия регламент относно защитата на данните, Хартата на основните права на Европейския съюз, Европейския етичен кодекс за почтеност на научните изследвания и други.

Изложение

Европейският етичен кодекс за почтеност на научните изследвания дефинира научните изследвания като процес на „търсене на знание чрез систематично проучване и размисъл, наблюдение и експериментиране. Макар че различните дисциплини може да използват различни подходи (в хода на това търсене), всички те са обединени от стремежа да подобрят разбирането ни за нас самите и за света, в който живеем“ (Европейски етичен кодекс за почтеност на научните изследвания 2017: 2). Дори за начинаещия изследовател е ясно, че извършването на научни изследвания е немислимо без натрупването на емпирични данни в съответната научна област, обработването им посредством подходящи научни методи и споделянето на изводите и резултатите от тях с представителите на научната общност, а често и с широката общественост. Заедно с това, събирането на данни и тяхното обработване следва да бъдат подчинени на съответните законови и етични норми.

Лаубер-Рьонсберг обръща внимание върху възможния конфликт между нуждата от набиране на емпирични данни за целите на научните изследвания, от една страна, и необходимостта от стриктна защита на данните, от друга страна. Хартата на основните права на Европейския съюз постулира редица свободи на гражданите на съюза, в това число свобода на зачитане на личния и семейния живот (чл. 7), свобода на защита на личните данни (чл. 8), както и свобода на изкуството и науките (чл. 13). „На практика обаче между тези свободи би могъл да възникне конфликт, изискващ намирането на баланс между свободата на науката, от една страна, и защитата на данните във всеки отделен случай.“ (Lauber-Rönsberg 2018: 30).

Европейският етичен кодекс за почтеност на научните изследвания формулира следните принципи, от които следва да се ръководят

изследователите:

• Надеждност на научните изследвания, което намира отражение в техния дизайн, методология, анализ и използване на ресурсите.

• Честност при разработването, провеждането, рецензирането, отчитането и разпространяването на резултатите от проведените научни изследвания по прозрачен, справедлив, изчерпателен и безпристрастен начин.

• Уважение към колегите, участниците в научните изследвания, обществото, екосистемите, културното наследство и околната среда.

• Отговорност за научните изследвания – от зараждането на идеята до публикуването, по отношение на тяхното управление и организация, обучение, надзор и наставничество, както и на цялостното им въздействие. (The European Code of Conduct for Research Intregrity 2017: 4).

През 2018 г. Европейската комисия публикува документ под заглавие „Етика и защита на данни“, в който засяга проблематиката на управлението и защитата на данни в контекста на научноизследователската дейност. В документа се подчертава: „Защитата на данните е не само въпрос с ключово значение за изследователската етика в Европа, но и основно човешко право. Тя е тясно свързана с независимостта на личността, с човешкото достойнство и с принципа, че всеки трябва да бъде ценен и уважаван. За да може този принцип да ръководи развитието на днешното информационно общество, изследователската общност следва стриктно да прилага защита на личните данни“ (Ethics and data protection 2018: 3).

Когато в хода на извършване на дадено научно изследване се събират и обработват лични данни, изследователят следва да се придържа както към съответните законови регламенти, така и към нормите на научната етика. Всеки научен проект, включващ обработка на лични данни, следва задължително да съдържа информация относно предвижданите мерки за защита на тези лични данни. В таблица 1 са обобщени категории данни, които се асоциират с по-висока степен на етичен риск, когато бъдат използвани за целите на извършване на научни изследвания. Следва да се подчертае, че етични съображения могат да възникнат както във връзка със съдържанието на събраните данни, така и с произхода на данните, с начина на тяхното получаване и обработката им. Заедно с това, дискусионни са въпросите относно предоставянето на свободен достъп до данните, използва-

ни за целите на научните изследвания, което е изискване на някои научни издания или организации, финансиращи научни изследвания (Kämper 2016: 4; Schaar 2016: 2).

Таблица 1

Данни с висок етичен риск при провеждане на научни изследвания

Съдържание на личните данни	• Лични данни, свързани с: • расов или етнически произход • политическа и религиозна принадлежност • генетични, биометрични и касаещи здравословното състояние • сексуален живот или сексуална ориентация • членство в профсъюз
Субекти на личните данни	• деца • уязвими лица • лица, които не са дали изричното си съгласие да участват в проекта
Техники за събиране на данните	• методи или технологии, нарушаващи неприкосновеността на личния живот (например камери за скрито наблюдение, вкл. записи от тях) • извличане на данни (data mining), вкл. данни от социални мрежи • профилиране на индивиди и групи (особено поведенческо или психологическо профилиране) • използване на изкуствен интелект за анализ на лични данни • използване на автоматизирано вземане на решения със съществено влияние върху субектите на данни

Източник: *European Commission. Ethics and data protection, 2018, p. 6.*

Следва да се подчертае, че всички европейски проекти, включващи обработка на лични данни на идентифицирани лица или лица,

които могат да бъдат идентифицирани[1], са предмет на Общия регламент относно защитата на данните. От друга страна, извън ограниченията на Общия регламент остава обработването на анонимна информация за изследователски цели. „Принципите на защита на данните не следва да се прилагат по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данните да не може или вече не може да бъде идентифициран“ (Общ регламент относно защитата на данните: 26). Данните, които не се отнасят до идентифицируеми лица, в т.ч. обобщени и статистически данни, данни, които по друг начин са били анонимизирани, не са лични данни и следователно са извън обхвата на Общия регламент.

Следователно, с оглед премахване на етичния риск в сферата на научните изследвания, произтичащ от използването на лични данни, е необходимо тяхното анонимизиране, така че те да не могат да бъдат свързвани с идентифицируеми лица. Важно е да се има предвид, че процесът на анонимизация може да бъде поставен под въпрос поради опасността от ре-идентификация на субектите на лични данни (Ethics and data protection 2018: 8).

Във връзка с горното следва да се обърне внимание върху разликата между процесите по анонимизация и псевдонимизация на данни, използвани за целите на научни изследвания. Съгласно Общия регламент, „псевдонимизация означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано“ (Общ регламент

[1] Съгласно дефиницията на Общия регламент, чл. 4. – „*лични данни* означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано (*субект на данни*); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице“.

относно защитата на данните, чл. 4, т. 5). Псевдонимизацията включва заместване на лична информация (като например име на индивид) с уникален идентификатор, като се използват техники като кодиране или хеширане. Ако обаче е възможно обратно идентифициране на субектите на данни, задължително следва да се спазват разпоредбите на Общия регламент.

В унисон с Общия регламент е и принципът на минимизация на данните, съгласно който изследователят следва да събира и обработва само и единствено данни, които са необходими за постигане целите на даденото научно изследване. Следователно, не бива да се събират лични данни, които нямат отношение към целите на проучването. В съзвучие с принципа на минимизация на данните, личните данни следва своевременно да бъдат унищожавани от изследователя.

Общият регламент налага строги изисквания относно прозрачността при събирането на данни за целите на научни изследвания. Субектът на данни следва да бъде информиран в „кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език, особено що се отнася до всяка информация, конкретно насочена към деца“ (Общ регламент относно защитата на данните, чл. 12, т. 1). Това включва информация относно целите, за които ще се използват събраните данни, обработката на данните, както и всеки планиран трансфер на личните данни към трети страни. Участниците следва също така да бъдат информирани за техните права, включително право на достъп,[2] право на изтриване[3] и др.

Задължителен елемент при събирането и обработката на данни за целите на научни изследвания е изследователят да получи информирано съгласие от страна на всеки отделен субект на данни. „Съгласие следва да се дава чрез ясно утвърдителен акт, с който да се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни за обработване на свързани с него лични данни, например чрез писмена декларация, включително по електронен път, или устна декларация“ (Общ регламент относно защитата на данните: 32). Съгласието трябва да бъде

---

[2] Касаещо правото на субекта да получи потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до тях. Вж. ОРЗД, чл. 15.

[3] Касаещо правото на субекта да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне. Вж. ОРЗД, чл. 17.

дадено свободно и може да бъде оттеглено по всяко време (Schaar 2016: 5).

За да се счита, че субектът на данни е дал своето информирано съгласие, трябва да му бъде предварително предоставена подробна информация, най-малко относно:

• администратора на лични данни и, ако е приложимо, да се предоставят контактите на длъжностното лице за защита на данните;

• целите, за които ще бъдат използвани и обработвани личните данни;

• правата на субекта на лични данни, в т.ч. правото му да оттегли съгласието си;

• дали събраните данни ще бъдат споделяни с трети страни и за какви цели и

• периода на съхраняване на данните преди те да бъдат унищожени (Ethics and data protection 2018: 11).

Заключение

Бурното развитие на информационните технологии изпреварва регулациите за тяхното използване и често повдига редица въпроси и проблеми, някои от които са предвидими, а други – неясни, трудни за идентифициране, дефиниране и разрешаване. То разкрива и широки нови възможности за достъп до емпирични данни и провеждане на мащабни научни изследвания. Заедно с това нараства отговорността на научната общност като цяло, както и на всеки отделен изследовател, за придържане към строги етични норми при извършване на научноизследователска дейност и разпространение на резултатите от нея.

Използвана литература

Регламент (ЕС) 2016/679 на Европейския парламент и на 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 относно защитата на данните).

Харта на основните права на Европейския съюз (2016/C 202/02).

Ethics and data protection. (2018). European Commission.

Lauber-Rönsberg, A. (2018). Data Protection Laws, Research Ethics and Social Sciences. // Research Ethics in the Digital Age. Ethics for the Social Sciences and Humanities in Times of Mediatization and Digitization. Springer VS: Wiesbaden, pp. 29 – 44.

Kämper, E. (2016). Risiken sozialwissenschaftlicher Forschung? Forschungsethik, Datenschutz und Schutz von Persönlichkeitsrechten in den Sozial - und Verhaltenswissenschaften. // RatSWD.Working Paper, № 255, (http://www.ratswd.de/dl/RatSWD_WP_255.pdf, 02.10.2021).

The European Code of Conduct for Research Intregrity. (2017). Revised Edition. ALLEA – All European Academies, Berlin.

Schaar, K. (2016). What is important for Data Protection in science in the future? General and specific changes in data protection for scientific use resulting from the EU General Data Protection Regulation. // RatSWD Working Paper №258, (hhttps://www.konsortswd.de/wp-content/uploads/RatSWD_WP_258.pdf , 02.10.2021).

За контакти: доц. д-р Петя Данкова
Икономически университет – Варна
e-mail: dankova@ue-varna.bg

НАРУШЕНИЯ НА СИГУРНОСТТА НА ДАННИТЕ И ДИГИТАЛИЗАЦИЯТА

Христо Аламинов
началник отдел „Международно сътрудничество и управление на проекти“
Комисия за защита на личните данни

DATA BREACHES AND DIGITALISATION

Hristo Alaminov
Head of International Cooperation and Project Management Department
Commission for Personal Data Protection

Резюме: Докладът представя общ преглед на значението и ползите от изследване на нарушенията на сигурността на личните данни в контекста на глобална тенденция, каквато е дигитализацията. Независимо от крайно отрицателните последици, които нарушенията на сигурността имат както за физическите лица, чиито данни са засегнати, така и за администраторите/ обработващите лични данни, те са ценен източник на информация.

Ключови думи: *Нарушение на сигурността на данните, защита на личните данни, дигитализация.*

Abstract: The report provides an overview of the importance and benefits of examining personal data breaches in the context of a global trend such as digitalisation. Regardless of the extremely negative consequences that security breaches have, both for the individuals whose data are affected and for the data controllers / processors, data breaches are valuable sources of information.

Key words: *Data breaches, protection of personal data, digitalisation*

DOI: https://doi.org/10.36997/PPDD2021.29

Изложение

Легална дефиниция за понятието „нарушение на сигурността на личните данни“ е предоставена в член 4 на Регламент (ЕС) 2016/679, а именно, това е „всяко нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин“. Нарушение на сигурността на данни възниква, когато данните, за които дружество/организация (администратор или обработващ лични данни) отговаря, са засегнати от инцидент със сигурността, в резултат на който се нарушава поверителността, наличието или целостта.

Съгласно Приложение № 1 към Инструкция за практическото осъществяване на надзорната дейност на Комисия за защита на личните данни. Методика за определяне нивото на риска при нарушения на сигурността на личните данни на Комисията за защита на личните данни, „нарушение на сигурността на данните е всяка една комбинация или самостоятелно проявление на някой от следните три типа нарушения – *нарушение на поверителността*, *нарушение на целостта* и/или *нарушение на наличността*“.

Нарушението на поверителността представлява неправомерно преднамерено или случайно разкриване или достъп до лични данни. Това включва разкриване на лични данни пред (или достъп до тях на) получатели, които не са оправомощени да ги получат (или да имат достъп до тях), или всеки друг вид обработване, което се явява нарушение на ОРЗД.

Нарушение на целостта е преднамерено или случайно повреждане на лични данни. *Повреждане* е налице, когато личните данни са променени, подправени или са станали вече непълни.

Нарушение на наличността е преднамерена или случайна загуба на данни, унищожаване на данни или неналичена услуга. *Загуба* на лични данни е състояние, при което данните може да са все още налични, но администраторът на лични данни е загубил контрол или достъп до тях или вече не ги притежава. *Унищожаване* на лични данни е налице, когато данните са във вид, в който не може да бъдат използвани или вече не са налични.

Важно е да се отбележи, че нарушаването на сигурността на лични данни може, ако не бъде овладяно по подходящ и навременен на-

чин, да доведе до физически, материални или нематериални вреди за физическите лица. Сред тези вреди са загубата на контрол върху личните им данни или ограничаването на правата им, дискриминацията, кражбата на самоличност или измамата с фалшива самоличност, финансовите загуби, неразрешеното премахване на псевдонимизация, накърняването на репутацията, нарушаването на поверителността на лични данни, защитени от професионална тайна, както и всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица.

Във връзка със започване прилагането на ОРЗД, Европейската комисия публикува на институционалната си интернет страница два примера за нарушение на сигурността на данните:

1. Данните на служителите на текстилно дружество са разкрити. Данните включват личните адреси, членове на семейството, месечната заплата и медицински бележки на всеки служител. В този случай текстилното дружество трябва да информира надзорния орган за нарушението. Тъй като личните данни включват чувствителни данни като например данни за здравословното състояние, дружеството трябва да уведоми и служителите.

2. Болничен служител решава да копира данните на пациентите на компактдиск и да ги публикува онлайн. Болницата разбира за това няколко дни по-късно. Веднага след като болницата разбере, тя има 72 часа, за да информира надзорния орган, и тъй като личните данни съдържат чувствителна информация като например дали даден пациент е болен от рак, дадена пациентка е бременна и т.н., тя трябва да информира и пациентите. В този случай би било под въпрос дали болницата е въвела подходящи технически и организационни мерки за защита. Ако тя действително е въвела подходящи мерки за защита (например криптиране на данните), би било малко вероятно рискът да се осъществи и тя би могла да бъде освободена от изискването за уведомяване на пациентите.

Сред общите елементи на двата примера, освен нарушението на сигурността на данните, е и задължението на администраторът/ обработващият лични данни да информира националния надзорен орган по защита на данните за нарушението. Макар да не е нова концепция в защитата на лични данни, уведомлението за нарушение на сигурността на данните намира значително място в общата парадигма на Регламент (ЕС) 2016/679. По-наблюдателните вероятно са открили същест-

ването му в Регламент (ЕС) № 611/2013 на Комисията от 24 юни 2013 г. относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронни комуникации, където към онзи момент се съдържат правилата относно съобщаването на нарушения на сигурността на личните данни от доставчиците на обществено достъпни електронни съобщителни услуги, в случай че личните данни на клиентите са изгубени, откраднати или компрометирани по друг начин.

Наличието на подобна правна разпоредба във връзка с електронните комуникации демонстрира, че европейският законодател е преценил, още в края на първото десетилетие на XXI в., технологиите и, в частност, електронните съобщения и свързаната с тях дигитализация като област, в която биха възникнали нарушения на сигурността на данните. Ето защо задължение на организациите, обработващи лични данни, е, веднага след като се установи нарушение на сигурността на личните данни, да уведомят надзорния орган за нарушението на сигурността на личните данни. Действието следва да се осъществи без ненужно забавяне и когато това е възможно – не по-късно от 72 часа, след като той е разбрал за него.

Както всяко правило, и настоящото задължение има изключение, ако администраторът е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Във всички случаи процесът следва да бъде документиран с оглед последващо доказване на адекватността на мерките. От съществено значение е да се сподели, че когато такова уведомление не може да бъде подадено в срок от 72 часа, то следва да посочва причините за забавянето и че информацията може да се подаде поетапно без ненужно допълнително забавяне.

Сред основните причини, които предопределят важността на уведомлението, е, че чрез него може да установи дали са били приложени всички подходящи мерки за технологична защита и организационни мерки (задължение на администратора/ обработващия лични данни съгласно чл. 24 от Общия регламент относно защитата на данните). Съдържанието на уведомлението е определено в чл. 33, пар. 3 от Регламент (ЕС) 2016/679. Всяко уведомление следва да съдържа най-малко:

а) описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

б) името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително и мерки за намаляване на евентуалните неблагоприятни последици.

При установяване на подробни правила за формàта и процедурите, приложими за уведомяването за нарушения на сигурността на личните данни, следва да се отдаде необходимото внимание на обстоятелствата, свързани с нарушението, включително дали личните данни са били защитени чрез подходящи технически мерки за защита, ефективно ограничаващи вероятността за измама с фалшива самоличност или други форми на злоупотреба. Заслужава внимание и хипотезата, в която при такива правила и процедури следва да се отчитат законните интереси на правоприлагащите органи, когато ранното разкриване може ненужно да попречи при разследването на обстоятелствата, свързани с нарушението на сигурността на личните данни.

Предвид широкото определение на понятието „лични данни“ съвсем логично и процесът по преобразуване (конвертиране) на аналогови данни под всякаква форма – текст, снимки, глас, в цифрова информация, с възможност да бъде репродуцирана неограничено във времето без промяна на качеството ѝ чрез общодостъпни комуникационни канали, може да попадне в обхвата на Общия регламент относно защитата на данните. След нейното цифровизиране същата може да бъде събрана, записана, организирана, структурирана, съхранявана, адаптирана, променяна чрез извличане, консултиране, употребяване, разкриване чрез предаване, разпространяване или друг начин, по който информацията става достъпна, подредена или комбинирана, ограничавана, изтривана или унищожавана – операции по обработване, които съвпадат с дефиницията на „обработване“ съгласно Регламент (ЕС) 2016/679.

При прилагане на второто значение на термина „дигитализирам“ – интегрирането на дигиталните технологии в ежедневието на хората също попада в обсега на регламента и дори в по-голяма степен представлява интерес от гледна точка защитата на личните данни. Тук следва да се представи възможността за профилиране на субектите на данните. По определение „профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно – за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.

Независимо кой от 6-те елемента на дигитализацията (съдържателен модел, концепция за дигитална конверсия, технологични решения, бюджетиране и финансиране, човешки ресурси и партньорства) се изследва, със сигурност може да се открият условия за нарушения на сигурността на данните. Тези предпоставки трябва да се анализират и да се въведат подходящи технически и организационни мерки.

Както вече беше посочено, уведомлението за нарушение на сигурността на данните съдържа необходимите данни, които да позволят на националния надзорен орган по защита на данните да изпълнява задачите и и да упражнява правомощия, вменени с ОРЗД. Те обхващат обработването в контекста на дейностите на мястото на установяване на администратора или обработващия лични данни на територията на неговата държава членка, обработването на лични данни, извършвано от публични органи или частни структури, действащи в обществен интерес, обработване, което засяга субекти на данни на неговата територия, или обработване, извършвано от администратор или обработващ лични данни, който не е установен в Европейския съюз, когато субектите на данни, към които това обработване е насочено, са с местопребиваване на територията на Съюза.

Въпреки настоящите предизвикателства, светът се глобализира. По силата на европейското законодателство държавите членки прилагат общи правила за защита на личните данни. Като част от единния пазар на Европейския съюз икономическите субекти често развиват своята дейност в държава – членка на ЕС, която е различна от държавата по регистрация.

За да се гарантира последователното прилагане на територията на Европейския съюз за Регламент (ЕС) 2016/679, се създаде механизъм за съгласуваност за осъществяване на сътрудничество между надзорните органи. Този механизъм се прилага, когато даден надзорен орган възнамерява да приеме мярка, целяща да породи правни последици по отношение на операции по обработване на данни, които засягат съществено значителен брой субекти на данни в няколко държави членки. Това се прилага също, когато засегнатият надзорен орган или Европейската комисия поиска този въпрос да бъде разгледан чрез механизма за съгласуваност.

Прилагането на подобен механизъм е условие за законосъобразността на мярка, целяща да породи правни последици, издадена от надзорния орган в случаите, когато прилагането му е задължително. В други случаи с трансгранично значение следва да се прилага механизмът за сътрудничество между водещия надзорен орган и засегнатите надзорни органи и могат да се осъществяват взаимопомощ и съвместни операции между засегнатите надзорни органи на двустранна или многостранна основа, без да се задейства механизмът за съгласуваност.

При прилагането на механизма за съгласуваност Европейският комитет по защита на данните (ЕКЗД, Комитета) излиза със становище в срок, при условие че бъде взето решение с мнозинство от неговите членове след искане от засегнат надзорен орган или от Европейската комисия. В допълнение, Комитетът приема решения със задължителен характер в случай на спорове между надзорни органи. При противоречиви становища от страна на националните надзорни органи ЕКЗД приема решение със задължителен характер. Това важи особено за условията на механизма за сътрудничество, между водещия надзорен орган и засегнатите надзорни органи по съществото на спора относно възможното нарушение на Регламент (ЕС) 2016/679.

С времето тези данни започват да се обобщават, а Комитетът, подпомаган от експерти от националните надзорни органи, издава насоки, препоръки и най-добри практики по отношение на обстоятелствата, при които нарушението на сигурността на личните данни има вероятност да доведе до висок риск за правата и свободите на физическите лица. Този процес демонстрира значението, което нарушенията на сигурността на данните имат, като спомага за предотвратяване на бъдещи нарушения на разпоредбите на Общия регламент,

благодарение на използването на нарушенията на сигурността на данните като източник на информация. Практически пример в тази посока са Насоки 01/2021 на ЕКЗД относно примери, свързани с уведомлението за нарушение на сигурността на данните.

Използвана литература

Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации).

Закон за защита на личните данни на Република България. // ДВ, №1, 2002; посл. изм. ДВ, №7, 2018.

Приложение № 1 към Инструкция за практическото осъществяване на надзорната дейност на Комисия за защита на личните данни. Методика за определяне нивото на риска при нарушения на сигурността на личните данни.

Проект № 2007CB16IPO007-2011-2-06 Дигитална култура за регионално сближаване, съфинансиран от ЕС чрез Програма за ТГС по ИПП № 2007CB16IPO007.

Регламент (ЕС) № 611/2013 на Комисията от 24 юни 2013 г. относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронни комуникации.

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).

Guidelines 01/2021 of the European Data Protection Board on Examples regarding Data Breach Notification.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_bg

За контакти: Христо Аламинов
Комисия за защита на личните данни
e-mail: halaminov@cpdp.bg

ПРАВНА ЗАЩИТА ПРИ НЕРЕГЛАМЕНТИРАНО РАЗПРОСТРАНЯВАНЕ НА СНИМКИ В ИНТЕРНЕТ

доц. д.н. Драгомир Кръстев
Висше училище по телекомуникации и пощи

LEGAL PROTECTION IN CASE OF UNREGULATED DISTRIBUTION OF PHOTOS ON THE INTERNET

Assoc. Prof. DSc. Dragomir Krastev
University of telecommunications and posts

Резюме: В доклада са разгледани формите на правна защита при нерегламентираното използване и разпространяване на фотографски снимки в интернет пространството. Анализирани са основните нормативни актове от българското и европейското законодателство в тази сфера. Отделено е внимание и на защитата на авторското право и личните данни при използване на снимков материал във виртуалното пространство.

Ключови думи*: авторско право, правна защита, интернет, снимки, лични данни.*

Abstract: The report examines the forms of legal protection in the unregulated use and distribution of photographic photos on the Internet. The main normative acts of the Bulgarian and European legislation in this field are analyzed. Attention is also paid to the protection of copyright and personal data when using photographic material in cyberspace.

Key words: *copyright, legal protection, internet, photos, personal data*

DOI: https://doi.org/10.36997/PPDD2021.37

Въведение

С непрекъснатото разширяване на функционалностите на глобалната информационна мрежа интернет, наред с проблемите пред технологиите, възникват и предизвикателства пред правната наука. Едно от най-честите нарушения в този контекст е нерегламентирано-

то използване на фотографски снимки в интернет. Господства схващането, че щом нещо е качено в интернет, то може да се употребява свободно. От правна гледна точка противоправните действия на нарушителите могат да се класифицират в две основни групи – нарушения на авторското право и такива спрямо защитата на личните данни на лицата, регламентирани в националните и международните юридически актове.

Изложение

Според ЗЗЛД и Общия регламент за защита на данните (GDPR) „лични данни“ е понятието по чл. 4, т. 1 от Регламент (ЕС) 2016/679, а именно: „...всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице“.[1]

Дадено лице обаче може да бъде идентифицирано и чрез някакви специфични негови признаци (вкл. белези и татуировки).

Именно възможността заснетото лице да бъде идентифицирано чрез използването на горните признаци прави снимките част от обхвата на понятието „лични данни“, а оттам и разпространението им без неговото съгласие представлява законово нарушение.

За да е налице нарушение при разпространение на снимки, е необходимо на тях да се вижда лицето на заснетия или други негови особени признаци. Ако тези условия не са налице, заснетият не може да бъде идентифициран. Съответно снимката не попада в обхвата на понятието „лични данни“. Ако обаче се разкрива например част от лице, въпросът дали заснетият може да бъде идентифициран подле-

[1] 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).

жи на преценка.[2]

Идентично е положението и в случаите на разпространение на компрометиращи интимни фотографии. Ако на снимката не се вижда лицето на заснетия, белези, татуировки или други подобни признаци, по които да бъде идентифициран, нарушение няма да има. По наказателноправен ред обаче би могло да се търси отговорност на лицето, което ги разпространява, в случай че то твърди, че на снимката е заснет точно определен конкретен човек.

Дискусионен е въпросът ще бъде ли неправомерно разпространението на снимка, качена от заснетото лице в социалните мрежи с ограничение в секция „само приятели“. Според преобладаващото мнение на експерти в тази материя, отговорът на този въпрос следва да бъде положителен. Това е така, защото поставяйки ограничението „само приятели“, заснетият изразява мълчаливо съгласие снимките му да бъдат видяни единствено от определен кръг от хора. Съответно, разпространение без негово изрично съгласие извън този кръг следва да се квалифицира като нарушение. Така например, ако дадена медия е получила снимки на определено лице чрез негов „приятел“ в социалните мрежи. Снимката е част от ограничените за широката публика публикации и е в секцията „само приятели“. Разпространението, от страна на медията, на такава снимка би следвало да се приеме като нарушение.

Административноправна защита

Този вид защита срещу неправомерно разпространение на снимки се осъществява чрез подаване на жалба до Комисията за защита на личните данни. Срокът за подаване на жалба е шестмесечен и тече от деня на узнаване на нарушението и не по-късно от две години от извършването му. Комисията се произнася в тримесечен срок от получаването ѝ, като в случай че констатира неправомерно разпространение на снимки, тя я уважава.

Съществуват някои изключения от общия режим. Така съгласно чл. 25з, ЗЗД (нов – ДВ, № 17, 2019) (1) „Обработването на лични

[2] Петкова, С. Разпространение на снимки без наше съгласие. (https://petkovalegal.com/%D1%80%D0%B0%D0%B7%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BD%D0%B0-%D1%81%D0%BD%D0%B8%D0%BC%D0%BA%D0%B8-%D0%B1%D0%B5%D0%B7-%D0%BD%D0%B0%D1%88%D0%B5-%D1%81%D1%8A/, 08.10.2021).

данни за журналистически цели, както и за академичното, художественото или литературното изразяване, е законосъобразно, когато се извършва за осъществяване на свободата на изразяване и правото на информация, при зачитане на неприкосновеността на личния живот“, а също така и чл. 25з, ЗЗД (5): „При обработването на лични данни за целите на създаване на фотографско или аудиовизуално произведение чрез заснемане на лице в хода на обществената му дейност или на обществено място не се прилагат чл. 6, чл. 12 – 21, чл. 30 и 34 от Регламент (ЕС) 2016/679“.[3]

Доскоро тези изключително общи формулировки бяха конкретизирани от десет субективни критерия, въз основа на които да се прави преценка дали обработването на лични данни за горните цели се прави при наличието баланс между свободата на изразяване и правото на информация и правото на защита на личните данни. Те обаче са обявени за противоконституционни, поради което вече не могат да намерят приложение. Ето защо, за момента, преценката за наличието на такъв баланс се прави за всеки конкретен случай.

Наказателноправна защита

Този вид защита при разпространение на снимки без съгласието на заснетото лице се използва най-често в случаите на разпространение на интимни (голи) снимки. В зависимост от техния характер те могат да попаднат в обхвата на определението за порнографски материал.

Според Наказателния кодекс на Репубика България, чл. 93, т. 28 (нова – ДВ, №38, 2007): „Порнографски материал“ е неприличен, неприемлив или несъвместим с обществения морал материал, който изобразява открито сексуално поведение. За такова се приема поведение, което изразява реални или симулирани полови сношения между лица от същия или различен пол, содомия, мастурбация, сексуален садизъм или мазохизъм, или похотливо показване на половите органи на лице“[4]. Така може да се окаже, че в определени хипотези разпространението на такъв тип снимки представлява престъпление. В този случай наказанието е лишаване от свобода до една година и глоба от хиляда до три хиляди лева. Ако заснетото лице е непълнолетно или изглежда като такова, наказанието е лишаване от свобода до шест

[3] Закон за защита на личните данни. // ДВ, №.1, 2002 ; посл. изм. ДВ, №7, 2018.
[4] Наказателен кодекс. // ДВ, №26, 1968, доп. ДВ, №54, 2017.

години и глоба до осем хиляди лева.

Кога дадена снимка представлява порнографски материал, подлежи на преценка за всеки конкретен случай?

Гражданскоправна защита

Гражданскоправната защита е тази, посредством която се обезщетява пострадалото от нарушението лице. Тя се активира тогава, когато нарушението е констатирано официално от съответния държавен орган. Искането за обезщетение се предявява пред съответния съд по местоживеене/местонахождение на нарушителя. То обхваща претърпените имуществени и неимуществени вреди от нарушението. В повечето случаи най-сериозни са нанесените морални щети, размерът на чието обезщетяване се определя от съда по справедливост. Те включват претърпените притеснения, унижения, страх, засягане на честта и доброто име, уронване на авторитет и престиж, издаване на интимна тайна и т.н.

Именно при реализирането на гражданскоправната защита се проявява и второто измерение на проблема с неправомерното използване на снимков материал в интернет. Освен нарушения свързани със защитата на личните данни сме свидетели и на накърняване на авторското право в определени хипотези. Това е всеки един случай, когато някой свали и на следващ етап качи чужда снимка на своя сайт или платформа.

Нарушаването на авторските права представлява деликт. За да бъде осъществен такъв, трябва да налице фактически състав от следните елементи: деяние, противоправност, вина и настъпили вреди.

В случая противоправното деяние се състои от два елемента:

- използване на чужда снимка без предварителното съгласие на автора (чл. 35, ЗАПСП) и
- и неплащане на съответното възнаграждение (чл.19, ЗАПСП).

Вината при генералния деликт, според българското законодателство, се презюмира във всички хипотези (чл. 45, ал.2, ЗЗД). Това означава, че ще е налице нарушение, независимо от това дали субектът, който използва чужди снимки, е бил наясно, че те са обект на авторски права. При нарушаване на авторското право почти винаги директно произтичат и вреди. Те се състоят най-малкото в пропуснатите ползи от нереализираното лицензионно възнаграждение за използване на снимките. Възможни са и загуби, свързани с усилията

за преустановяване на правонарушението, както и неимуществени вреди от липсата на посочване на автора. Ако при публикуването на снимките авторът не е отбелязан, се нарушава и неимущественото му право да иска признаване на авторството му върху произведението (чл. 15, ал. 1, т. 2 и 4 ЗАПСП)[5].

Закономерно възниква въпросът дали всички снимки, които са качени във виртуалното пространство са обект на авторски права? Отговор на този въпрос дава и българското и европейското законодателство.

Според чл. 3, ал. 1 ЗАПСП, всяка снимка, която е израз на индивидуалните творчески решения на нейния автор е валиден обект на авторското право. Съгласно решение на Съда на Европейския съюз C-145/10 изборът на определен ъгъл, композиция, осветление, филтър и т.н. при подготовката на заснемането изразяват творческия процес на фотографа и са основание за защита на авторското право на произведението му. Без значение е въпросът какъв обект е заснет на съответната снимка.[6]

Заключение

Въпросът за неправомерното разпространение на снимки в интернет пространството е сравнително нов за българското правоприлагане. С напредването на информационните технологии такива случаи стават все по-често срещани и разнообразни. От гледна точка на превенцията от съществено значение е навременното подаване на сигнали до компетентните органи, което би довело до пресичане на тези непозволени практики още в зародиш.

Използвана литература

Кога се нарушават авторски права върху снимки онлайн? (https://gglaw.bg/ip-photography-internet/, 08.10.2021).

Петкова, С. Разпространение на снимки без наше съгласие (https://petkovalegal.com/%D1%80%D0%B0%D0%B7%D0%BF%D1%80%-

[5] Кога се нарушават авторски права върху снимки онлайн? (https://gglaw.bg/ip-photography-internet/, 08.10.2021).

[6] Case C-145/10, Eva-Maria Painer v Standard VerlagsGmbH and Others (Reference for a preliminary ruling from the Handelsgericht Wien).

D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BD%D0%B0-%D1%81%D0%BD%D0%B8%D0%BC%D0%BA%D0%B8-%D0%B1%D0%B5%D0%B7-%D0%BD%D0%B0%D1%88%D0%B5-%D1%81%D1%8A/, 08.10.2021).

Закон за защита на личните данни. // ДВ, №.1, 2002 ; посл. изм. ДВ, №7, 2018.

Наказателен кодекс. // ДВ, №26, 1968; доп. ДВ, №54, 2017.

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).

Case C-145/10, Eva-Maria Painer v Standard VerlagsGmbH and Others (Reference for a preliminary ruling from the Handelsgericht Wien).

За контакти: доц. д.н. Драгомир Кръстев
Висше училище по телекомуникации и пощи
e-mail: drago.krastev@gmail.com

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ – ИЗИСКВАНИЯ, СТАТУС И ФУНКЦИИ

доц. д-р Андрей Александров
Институт за държавата и правото
при Българската академия на науките
Югозападен университет „Неофит Рилски“

DATA PROTECTION OFFICER – REQUIREMENTS, STATUS AND FUNCTIONS

Assoc. Prof. Andrey Aleksandrov, PhD
Institute for the State and the Law –
Bulgarian Academy of Sciences
South-West University „Neofit Rilski“

Резюме: Изследването е посветено на една от най-значимите от практическа гледна точка теми, свързани с прилагането на Общия регламент за защита на данните – този за определянето, статуса и функциите на длъжностното лице по защита на данните. Представени са актуалните тенденции по тези въпроси в европейската и българската практика. Потърсени са отговори на често възникващи в практиката проблеми.

Ключови думи: *длъжностно лице по защита на данните (ДЛЗД), Общ регламент за защита на данните (ОРЗД), изисквания, роля, права и задължения*

Abstract: The study is devoted to one of the most important from a practical point of view topics related to the implementation of the General Data Protection Regulation - that of the definition, status, and functions of a data protection officer. The current trends on these issues in European and Bulgarian practice are presented. Answers to frequently encountered problems in practice are sought.

Key words: *Data Protection Officer (DPO), General Data Protection Regulation (GDPR), requirements, roll, rights and obligations*

DOI: https://doi.org/10.36997/PPDD2021.44

Въведение

Вече над три години се прилага Общият регламент за защита на данните (ОРЗД),[1] който бележи началото на мащабна реформа в законодателството по защита на личните данни, а и в развитието на Европейския съюз (Тошкова – Николова, Фети 2019). Като че ли в последно време темата мина донякъде на заден план, изместена от безпрецедентната заплаха на пандемията от COVID-19 и *антикризисните* промени в законодателството, възприети във връзка с извънредното положение и извънредната епидемична обстановка. Тя обаче не е загубила голямата си обществена значимост и не бива да се забравя за нея. Причините са не само и не толкова в големите размери на санкциите при установени нарушения, а в нещо много по-важно: защитата на данните не е самоцел, а средство за предпазване на личната неприкосновеност на лицата, а оттук – и гаранция за основните им права (Кръстева, Александров 2018). Оттук произтича и голямата практическа важност на въпроса кой ще бъде определен за длъжностно лице по защита на данните (ДЛЗД). Удачният избор на такова лице може да се окаже решаващ за сигурността на обработваните данни.

Изложение

I. Хипотези на определяне на ДЛЗД

ДЛЗД е *отговорник* по всички въпроси, свързани със защитата на личните данни в организацията на администратора или на обработващия лични данни. Това е служител на администратора/обработващия или външно за организацията лице, натоварено с консултативни функции в областта на защитата на личните данни, надзор по спазването на регламента в организацията и повишаването на осведомеността и обучението на персонала (Матеева 2019).

Съгласно ОРЗД могат да се обособят две групи случаи на определяне на ДЛЗД: (а) при първата от тях то представлява правно задължение и евентуалното му неизпълнение може да доведе до налагане на санкции на задължените лица; (б) във втората група случаи

[1] 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. Той започва да се прилага от 25 май 2018 г.

определянето на ДЛЗД става по избор на съответната организация с цел да се оптимизира защитата на обработваните лични данни (Захариев 2018а, 2018б). Независимо дали определянето на ДЛЗД е било задължително или е предприето от организацията доброволно, неговите статут и функции са еднакви.

По въпросите, свързани с определянето на ДЛЗД, са издадени нарочни указания (насоки) от Работната група по чл. 29 от Директива 95/46/ЕО (след 25.05.2018 г. – Европейски комитет по защита на данните. В тях е дадена препоръка към администраторите и обработващите лични данни, освен ако е очевидно, че дадена организация не е задължена да определя ДЛЗД, да документират направения вътрешен анализ с оглед на вземането на решение дали да бъде назначено ДЛЗД или не, за да бъдат в състояние да докажат, че съответните фактори са взети предвид по надлежен начин. Този анализ представлява част от документацията според принципа на отчетност. Той може да бъде изискан от надзорния орган и следва да се актуализира при нужда, например ако администраторите или обработващите лични данни започнат осъществяването на нови дейности или предоставянето на нови услуги, които е възможно да попадат в случаите на задължително определяне на ДЛЗД (Александров 2018).

Хипотезите на задължително определяне на ДЛЗД според регламента са следните: (а) когато обработването се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции; (б) когато основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни; (в) когато основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

Така описаните хипотези налагат няколко уточнения, например кога обработването на данни представлява основна дейност на администратора или на обработващия. За *основни дейности* се считат ключовите операции, които са необходими за постигането на целите на администратора или обработващия лични данни. Обработването на данни е основна дейност и в случаите, когато то е неразделна част от останалите дейности на организацията. Казаното може да се она-

гледи със следните примери:

► Основната дейност на една болница е предоставянето на здравно обслужване. Болницата обаче не може да предоставя здравно обслужване безопасно и ефективно, без да обработва данни за здравословното състояние като например здравни досиета на пациенти. Следователно обработването на тези данни е нужно да се счита за една от основните дейности на всяка болница и съответно болниците трябва да определят ДЛЗД.

► Частно охранително дружество осъществява наблюдение върху няколко частни търговски обекта и обществени места. Основната дейност на дружеството е наблюдение, което от своя страна е неразривно свързано с обработването на лични данни. Следователно това дружество също трябва да определи ДЛЗД.

► КЗЛД е имала повод да изрази специално становище по отношение на училищата: „Съгласно разпоредбата на чл. 37, пар. 1, б. „а" от Регламент (ЕС) 2016/679 във вр. с пар. 1, т. 17 от ДР на Закона за защита на личните данни, институциите в системата на предучилищното и училищното образование (училища, детски градини и др.), в качеството си на администратори на лични данни, са задължени да определят ДЛЗД."[2]

Обратно, следните дейности по обработване на данни не трябва да се считат за основна дейност на администратора/обработващия: (а) обработка на данни на работници и служители с цел изплащане на възнагражденията им; (б) стандартна IT поддръжка на фирмени системи; (в) наблюдение на интернет и имейл трафик с цел спазване на изискванията за киберсигурността и др. п. Това са примери за спомагателни функции, които са необходими за основната дейност или основното направление на стопанската дейност на организацията. Въпреки че тези дейности несъмнено са необходими, те обикновено са считани за спомагателни функции, а не за основна дейност.

Що се отнася до хипотезите на *мащабно обработване* на данни, липсва точен количествен критерий кога е налице такова обработване. При преценката следва да се вземат под внимание фактори като броят на субектите на данни, обемът или видът данни, които се обработват, продължителността на обработването, географският обхват на обработването. При това е нужно тези критерии да се съобразят

[2] https://www.cpdp.bg/index.php?p=news_view&aid=1576

кумулативно (едновременно), а не самостоятелно. Обработването, например, може да се осъществява паралелно в няколко държави членки и да е налице широк географски обхват, но да засяга малко на брой лица и незначителен обем данни. В този случай то няма да се характеризира като мащабно.

Понятието за редовно и систематично наблюдение на субектите на данните също не е изрично дефинирано в регламента. Според тълкуването на Работната група по чл. 29 *редовно* означава: текущо или възникващо на определени интервали за определен период; многократно или повтарящо се на определени интервали; случващо се постоянно или периодично наблюдение. Наблюдението е систематично, когато се осъществява чрез система, организирано е или е част от целенасочен план или стратегия за събиране на данни.

Редовно и систематично наблюдение може да е налице при профилиране и оценяване на субектите за целите на оценка на риска (например за целите на определяне на кредитоспособността, изчисляване на застрахователни премии, предотвратяване на измами, откриване на случаи на изпиране на пари) и др.п.

II. Изисквания към ДЛЗД

В чл. 37, пар. 5 от регламента е предвидено, че „длъжностното лице по защита на данните се определя въз основа на неговите професионални качества и, по-специално, въз основа на експертните му познания в областта на законодателството“. Необходимото ниво на експертни познания следва да се определи в съответствие с извършваните операции по обработване на данни и защитата, която е необходима за тях. Въпреки че регламентът не поставя конкретни изисквания относно необходимата професионална квалификация и опит на ДЛЗД, то следва да познава добре сектора и организацията на администратора, както и да разбира операциите по обработка, информационните системи, сигурността на данните и необходимостта от тяхната защита. При дейността на публичните органи е препоръчително и добро познаване на административните правила и процедури, които се прилагат от администратора. При частните организации се предполага познаването на специалните закони и процедури, регулиращи тяхната дейност (напр. Закона за кредитните институции и съответните подзаконови актове – по отношение на дейността на банките и т.н.)

Фразата *съответен опит* не следва да се чете и разбира изрично като опит, придобит като длъжностно лице по защита на данните – това би могъл да е опит в изготвянето и прилагането на политики в съответната организация (или подобна организация) или в съответните област като IT, разработване на продукти и т.н. Достатъчно е да се спомене, че позицията не следва да бъде възлагана на сравнително млад, неопитен човек или на лице, което не е запознато с конкретния (тип) организация, за която става въпрос. (Наръчник за длъжностните лица по защита на данните, публикуван на интернет страницата на КЗЛД).[3]

Длъжностното лице по защита на данните играе ключова роля в насърчаването на културата по защита на данните в рамките на организацията. Затова, наред с професионалните качества, регламентът поставя като изискване и „способността му да изпълнява задачите, посочени в чл. 39“. Според Работната група по чл. 29 тази способност трябва да се тълкува като отнасяща се до личните качества и знания на лицето, като се изисква почтеност и висока професионална етика. „То е в деликатна позиция: трябва да е готово да каже „не” на своите началници в редки случаи, но по-често да бъде в състояние да помага за намирането на решение на въпроси, което трябва както да бъде приемливо за организацията, така и изцяло да бъде в съответствие със закона (и, ако не друго, да следи и защитава неприкосновеността).“ (цитирания по-горе наръчник).

III. Статус на ДЛЗД

Според регламента ДЛЗД може да бъде както служител на предприятието, така и да изпълнява задълженията си по договор за услуги. Няма пречка служителят, определен от администратора за лице по защита на данните, да изпълнява и други функции в рамките на организацията (т.е. вече назначен на друга длъжност служител да поеме и функциите на длъжностно лице по защита на данните по вътрешно съвместителство).

Възможно е и съвместно определяне на ДЛЗД в група предприятия. Условието е всяко предприятие да има *лесен достъп* до длъжностното лице по защита на данните. Достъпността се отнася до задачите на длъжностното лице като точка за контакт на субектите на

[3] https://www.cpdp.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG(1).pdf

данни и надзорния орган, но също и в рамките на организацията, като се има предвид, че една от задачите му е да информира и съветва администратора или обработващия и служителите, които извършват обработване, за техните задължения. В многонационалните групи предприятия улесняването на достъпа до ДЛЗД би включвало и възможността с него да се комуникира на език, какъвто владеят служителите и в останалите държави, в които компанията има структури.

Предвид възможността длъжностното лице по защита на данните да изпълнява и други задачи, регламентът въвежда изискването те да не водят до конфликт на интереси. Работната група по чл. 29 приема, че ДЛЗД не може да заема позиция в организацията, която е свързана с определяне на целите и средствата за обработка на личните данни. Поради специфичната организационна структура във всяка организация, конфликтът на интереси трябва да се преценява конкретно за случая.

Работната група дава примерни насоки, като посочва, че висшите ръководни позиции (например главен изпълнителен директор, главен оперативен директор, главен финансов директор, ръководителите на звената за човешките ресурси и информационните технологии) могат да създадат такъв конфликт, т.е. такива лица не следва да се определят за ДЛЗД. Противното би означавало тези лица да съчетават в едно качествата на контролиращ и контролиран, т.е. да осъществяват контрол над собствените си действия, което е логически неиздържано, а оттук – и юридически недопустимо.

Пряко свързан с правилото за предотвратяване на всеки възможен конфликт на интереси е и принципът на независимост на ДЛЗД. Администраторът/обработващият трябва да гарантират, че това лице не получава никакви указания във връзка с изпълнение на своите задачи. Това означава не само те да се въздържат от указания как да се реши конкретен въпрос или жалба, но да важи и за всички други техни служители. Работната група по чл. 29 препоръчва да се даде възможност на ДЛЗД да изразява несъгласие с решения на администратора или обработващия, които са несъвместими с неговите препоръки.

ДЛЗД се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни. Това е проявление на неговата независимост от други ръководни нива в структурата.

Според чл. 38, пар. 3 от регламента ДЛЗД не може да бъде осво-

бождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Дадените от Работната група по чл. 29 насоки в тази връзка изясняват, че санкциите са забранени, само ако са наложени във връзка с изпълнението на задълженията като ДЛЗД. Например няма да е допустимо налагане на наказание от страна на администратора, ако той не е съгласен с дадената от ДЛЗД оценка на въздействие за дадена операция по обработване на лични данни. ДЛЗД не може да бъде уволнено за даване на този съвет.

ДЛЗД е обвързано със задължение да спазва конфиденциалност при изпълнение на неговите задачи. Това е важна гаранция за субектите на данни, които могат да се обръщат към него по всички въпроси, свързани с обработването на лични данни и с упражняването на техните права съгласно регламента. Задължението за поверителност е установено по отношение на конкретните обстоятелства, станали известни на длъжностното лице при или по повод изпълнение на неговите задачи.

ДЛЗД не са лично отговорни в случай на неспазване на правилата на регламента. Администраторът или обработващият лични данни е този, който е длъжен да гарантира и да е в състояние на докаже, че обработването се извършва в съответствие с предвидените в него разпоредби (чл. 24, пар. 1). Спазването на разпоредбите за защита на данните е отговорност на администратора на данни или на обработващия лични данни.

IV. Основни задачи на ДЛЗД

На длъжностното лице по защита на данните могат да се възлагат редица задължения, по-важните от които са: (а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на нормативните актове за защита на личните данни; (б) да наблюдава спазването на правилата за защита на личните данни и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити; (в) да си сътрудничи с надзорния орган и да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването

на данните; (г) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката. Работната група по чл. 29 препоръчва администраторът да потърси съвет от длъжностното лице по защита на данните най-малко по следните въпроси: (аа) да извърши, или не, оценка на въздействието върху защитата на данните; (бб) по каква методология да се извършва оценката на въздействието върху защитата на данните; (вв) дали оценката на въздействието върху защитата на данните да се извърши в организацията, или да се възложи на външен изпълнител; (гг) какви гаранции (включително технически и организационни мерки) да се прилагат, за да се намалят рисковете за правата и интересите на субектите на данни; (дд) дали оценката на въздействие върху защитата на данните е извършена коректно и дали нейните заключения са в съответствие с регламента.

Ако администраторът не е съгласен с препоръките на длъжностното лице по защита на данните, е препоръчително да обоснове конкретно и в писмена форма причините, поради които не ги взема предвид.

Задължение на администратора и на обработващия лични данни е да гарантират участието на ДЛЗД по всички въпроси, свързани със защитата на личните данни. Това трябва да става по *подходящ начин* и *своевременно*, т.е. като се отчитат конкретните обстоятелства при организиране на защитата и операциите по обработване на лични данни, извършвани в структурата на администратора или обработващия, и се осигури запознаване с тях на ДЛЗД. Удачно е участието му в решаването на всички въпроси, свързани със защитата на личните данни, да става на възможно най-ранен етап, включително да се изисква и негово предварително становище.

В чл. 38, пар. 2 от регламента са посочени някои задължения на администратора и обработващия личните данни за подпомагане на ДЛЗД при изпълнение на неговите задачи. Те са свързани с осигуряването на необходимите ресурси, достъпа до личните данни и операциите по обработване и поддържане на експертните познания на длъжностното лице по защита на данните. Тук се включват активната подкрепа на функцията на ДЛЗД от висшето ръководство, осигуряването на достатъчно време за изпълнение на задълженията му и осигуряването на финансови ресурси, инфраструктура и персонал към длъжностното лице по защита на данните, ако е необходимо и т.н.

Администраторът или обработващият лични данни са длъжни да публикуват данните за контакт с длъжностното лице по защита на данните и да ги съобщят на надзорния орган. Това е гаранция, че субектите на данни и надзорните органи могат да се свържат с длъжностното лице пряко, без *посредничеството* на администратора или обработващия данните. Такива данни за контакт могат да бъдат адрес, телефонен номер, електронен адрес, специален формуляр за контакт на интернет страницата на организацията, адресиран до длъжностното лице по защита на данните и др. На интернет страницата на КЗЛД е публикуван образец на Уведомление за определено длъжностно лице по защита на данните. Указания относно попълването се съдържат в самото уведомление. Администраторът или обработващият имат задължението да информират за всяка настъпила промяна на обстоятелствата/данните от уведомлението. Указаните са и начините, по които може да се подаде уведомлението – на място в деловодството на Комисията, чрез автоматизирана информационна система на КЗЛД и т.н. КЗЛД публикува данните в Регистъра на администраторите/обработващите лични данни, определили ДЛЗД.

Заключение

Ако накратко трябва да се обобщи всичко казано по-горе, несъмнено се налага изводът за съществената роля, която играе ДЛЗД в процесите на обработване на данните във всяка организация. Затова към определянето на такова лице не следва да се пристъпва лекомислено, прибързано или с мотив, че трудно се намират желаещи да се нагърбят с подобна отговорност и затова тя ще бъде вменена на този, който не е в позиция да откаже. Подобен подход обрича администратора или обработващия на едно формално присъстващо в организацията ДЛЗД, което не проявява никаква инициативност и само маркира изпълнението на възложените му функции. Едва ли е необходимо специално да се обоснова какви рискове крие подобна ситуация за сигурността на данните и, разбира се, за защитата на правата на субектите на тези данни.

Използвана литература

Александров, А. (2018). Статус и функции на длъжностните лица по защита на данните. // Труд и право, № 9, с. 49 – 57.

Aleksandrov, A. (2018). Status i funktsii na dlazhnostnite litsa po zashtita na dannite. // Trud i pravo, № 9, s. 49 – 57.

Захариев, М. (2018а). Задължение за назначаване на ДЛЗД и уведомление за него в КЗЛД. // Данъци ТИТА, №104, 2018 (https://www.tita.bg/free/commercial-law/553, 27.09.2021).

Zahariev, M. (2018a). Zadalzhenie za naznachavane na DLZD i uvedomlenie za nego v KZLD. // Danatsi TITA, №104, 2018 (https://www.tita.bg/free/commercial-law/553, 27.09.2021).

Захариев, М. (2018б). Автоматизираното профилиране и защитата на личните данни. Анализ на GDPR. София: За буквите (О писменехь), с. 206 – 210.

Zahariev, M. (2018b). Avtomatiziranoto profilirane i zashtitata na lichnite danni. Analiz na GDPR. Sofia: Za bukvite (O pismenehy), s. 206 – 210.

Кръстева, Д., А. Александров (2018). Защита на личните данни. Мисия възможна. София: Резон България ЕООД.

Krasteva, D., A. Aleksandrov (2018). Zashtita na lichnite danni. Misia vazmozhna. Sofia: Rezon Bulgaria EOOD.

Mateeva, Z. (2019). Specific Nature of the New Profession „Data Protection Officer" in the Context of Digitalization. // Международни клъстерни политики: Българо-китайски форум. Сборник с доклади от международна конференция. Варна: Наука и икономика, с. 112 – 122.

Mateeva, Z. (2019). Specific Nature of the New Profession „Data Protection Officer" in the Context of Digitalization. // Mezhdunarodni klasterni politiki: Balgaro-kitayski forum. Sbornik s dokladi ot mezhdunarodna konferentsia. Varna: Nauka i ikonomika, c. 112 – 122.

Тошкова-Николова, Д., Н. Фети (2019). Защита на личните данни. София: Труд и право.

Toshkova-Nikolova, D., N. Feti (2019). Zashtita na lichnite danni. Sofia: Trud i pravo.

Наръчник за длъжностните лица по защита на данните (https://www.cpdp.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG(1).pdf, 27.09.2021).

Narachnik za dlazhnostnite litsa po zashtita na dannite. (https://www.cpdp.bg/userfiles/file/Documents_2019/T4DATA-MANUAL-2019-BG(1).pdf, 27.09.2021).

Определяне на длъжностно лице по защита на данните в сферата на предучилищното и училищното образование (разяснение на КЗЛД). (https://www.cpdp.bg/index.php?p=news_view&aid=1576,27.09.2021).

Opredelyane na dlazhnostno litse po zashtita na dannite v sferata na preduchilishtnoto i uchilishtnoto obrazovanie (razyasnenie na KZLD). (https://www.cpdp.bg/index.php?p=news_view&aid=1576, 27.09.2021).

За контакти: доц. д-р Андрей Александров
ИДП при БАН, ЮЗУ „Н. Рилски“
e-mail: a.alexandrov@kambourov.biz

НАДГРАЖДАНЕ НА БАНКОВИЯ СОФТУЕР – ГЕНЕРИРАНЕ НА ДЕКЛАРАЦИИ ПО GDPR

проф. д-р Юлиан Василев
Икономически университет – Варна

BANKING SOFTWARE UPGRADE – GENERATING THE GDPR DECLARATION

Prof. PhD Julian Vasilev
University of Economics Varna

Резюме: Цел на доклада е представяне на подход за генериране на декларация по GDPR от банков софтуер. Използвани са съвременни информационни технологии. В доклада се представя подход за надграждането на банков софтуер, така че бързо и лесно да се отпечатва декларация по GDPR, да се коригира бланката на декларацията от банковите специалисти, да се следи кои клиенти са подписали декларацията. Направеното предложение може да се адаптира от всеки разработчик на банков софтуер.

Ключови думи: *банков софтуер, SQL*

Abstract: The purpose of the paper is to present an approach for generating a GDPR declaration from banking software. Modern information technologies are used. The paper presents an approach to upgrading banking software so that the GDPR declaration can be printed quickly and easily, the GDPR declaration form of the banking specialists can be corrected, and it can be monitored which clients have signed the declaration. The proposal can be adapted by any banking software developer.

Key words: *banking software, SQL*

DOI: https://doi.org/10.36997/PPDD2021.56

Въведение

Надграждането на софтуерните продукти е сложна задача, изискваща високо квалифицирани и опитни IT специалисти (Kuyumdzhiev

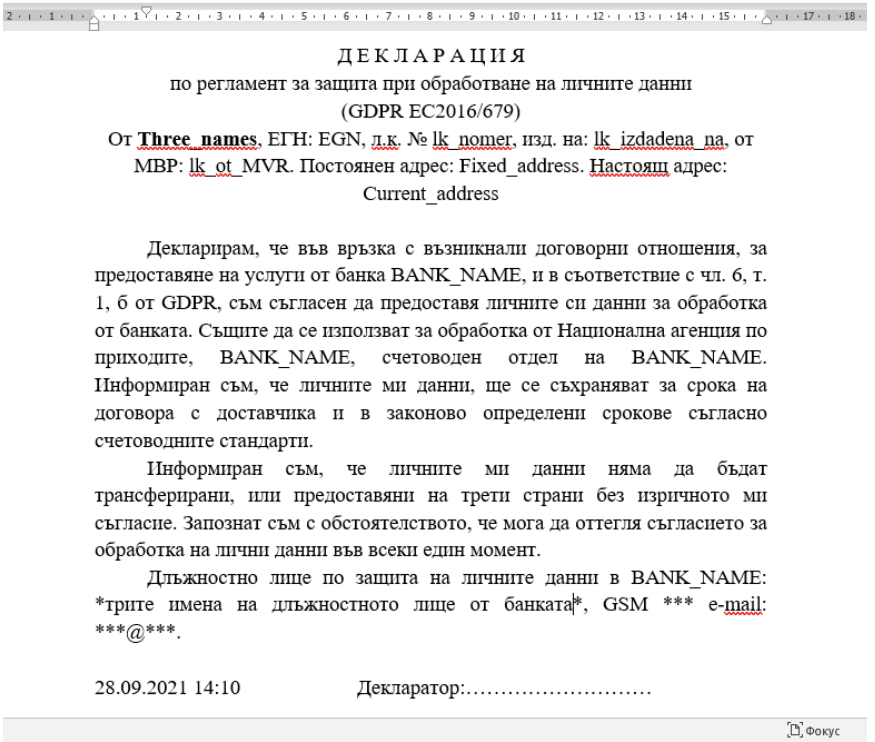
2016; Nacheva, Sulova 2020; Petrov et al. 2021; Pólkowski, Prasad, Mishra 2021; Todoranova, Penchev 2020). Законодателните промени в повечето случаи налагат промени в използваните софтуерни системи (Kuyumdzhiev 2020; Petrov et al. 2020; Raychev 2020), включително и тези за GDPR декларациите (Czaplewski, Modzelewska-Stalmach, Popiołek 2018). Намирането на добри практики по надграждане на софтуерни системи за всяка конкретна законодателна промяна е трудна задача (Bankov, 2020; Ramona, Pompiliu, Stoyanova 2020; Petrov et al. 2020; Stoyanova 2020). Тестването на производителността на направените доработки е отделна задача, която изисква време и средства (Aleksandrova, Parusheva 2019; Cristescu 2019; Nacheva, Sulova 2021; Todoranova et al. 2020). Понякога при софтуерните доработки се налага адаптирането на математически модели (Miryanov, Petkov 2017; Miryanov, Yordanova 2017; Nikolaev, Milkova, Miryanov, 2018a, 2018b). Технологиите, използвани от банките, са специфични (Parusheva, Pencheva 2022; Petrov et al. 2018). Тестването на софтуера в специализирана среда изисква специфични знания, умения и компетентности (Czaplewski 2018a, 2018c, 2018b). Използването на шаблони при доработването на софтуер е обичайна практика (Armyanova 2019, 2020).

Изложение

Подход за надграждане на банковия софтуер за генериране на декларация по GDPR

Подписването на декларация по GDPR от клиенти на банки е обичайна практика. След влизането в сила на разпоредбите по GDPR банките и кредитните институции трябва да доработят използвания от тях софтуер, така че да може: (1) бързо и лесно да се отпечата декларация по GDPR и (2) да се следи кои клиенти са подписали подобна декларация и кои не са я подписали.

В настоящия доклад се предлага подход, при който декларацията по GDPR се съхранява извън банковия софтуер – като DOCX файл (фиг. 1).



ДЕКЛАРАЦИЯ
по регламент за защита при обработване на личните данни
(GDPR EC2016/679)

От **Three_names**, ЕГН: EGN, л.к. № lk_nomer, изд. на: lk_izdadena_na, от МВР: lk_ot_MVR. Постоянен адрес: Fixed_address. Настоящ адрес: Current_address

Декларирам, че във връзка с възникнали договорни отношения, за предоставяне на услуги от банка BANK_NAME, и в съответствие с чл. 6, т. 1, б от GDPR, съм съгласен да предоставя личните си данни за обработка от банката. Същите да се използват за обработка от Национална агенция по приходите, BANK_NAME, счетоводен отдел на BANK_NAME. Информиран съм, че личните ми данни, ще се съхраняват за срока на договора с доставчика и в законово определени срокове съгласно счетоводните стандарти.

Информиран съм, че личните ми данни няма да бъдат трансферирани, или предоставяни на трети страни без изричното ми съгласие. Запознат съм с обстоятелството, че мога да оттегля съгласието за обработка на лични данни във всеки един момент.

Длъжностно лице по защита на личните данни в BANK_NAME: *трите имена на длъжностното лице от банката*, GSM *** e-mail: ***@***.

28.09.2021 14:10 Декларатор:.....

Фокус

Фигура 1. Декларация по GDPR.
Източник: собствена разработка.

Правният отдел на банката има възможност да редактира и дописва бланката (фиг. 1), без да е нужно да се доработва самият банков софтуер.

За да може декларацията да се отпечатва от банковия софтуер, следва да се направят доработки.

В базата от данни, в таблица „Клиенти“, следва да се добави колона от булев тип *dekl_GDPR*, която да служи за ориентир – на кои клиенти е отпечатана декларация и на кои клиенти не е отпечатана декларация. Понеже тази колона не съществува при клиентите, следва да се изпълни следният скрипт.

```
SQL := ‚ALTER table Customers ADD column dekl_GDPR BIT‘;
```

Фигура 2. Скрипт за добавяне на нова колона в таблица „Клиенти“.
Източник: собствена разработка.

След отпечатването на декларация по GDPR от банковия софтуер се налага да се смени флагът на конкретен клиент – че вече му е отпечатана декларация по GDPR.

```
sql := 'Update Customers set dekl_GDPR = 1 where egn = %s';
sql := format( sql, [ Customer.Text ] );
```

Фигура 3. Скрипт за отбелязване в таблица „Клиенти“, че е отпечатана декларация по GDPR.

Източник: собствена разработка.

Следващите стъпки в средата на банковия софтуер са следните:

1. Проверка дали съществува бланката (файл: *Deklaracia_po_GDPR.docx*).
2. Проверка дали е инсталиран Word.
3. Създаване на OLE обект в банковия софтуер за достъп до Word файла.
4. Създаване на копие на файла с бланката (файл: *Deklaracia_po_GDPR_4_print.docx*).
5. Извличане от базата от данни на данни за конкретен клиент.

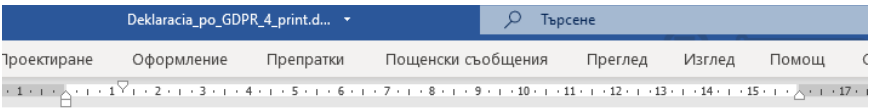
```
SQL :=
      ,SELECT , +
      ,  Three_names, , +
      ,  Town, , +
      ,  Address, , +
      ,  lk_nomer, , +
      ,  lk_izdadena_na, , +
      ,  lk_ot_MVR, , +
      ,  Current_address , +
      ,FROM Customers , +
      ,WHERE ( EGN = %f )';

SQL := Format( SQL, [ aEGN ] );
```

Фигура 4. Скрипт за извличане на данни за конкретен клиент.

Източник: собствена разработка.

6. Попълване на служебните полета от DOCX файла за печат с данните за конкретен клиент.

7. Отпечатване на декларацията с попълнени данни на клиент (файл: *Deklaracia_po_GDPR_4_print.docx*).



ДЕКЛАРАЦИЯ

по регламент за защита при обработване на личните данни

(GDPR EC2016/679)

От **Стефан Николов**, ЕГН: 333333333333, л.к. № 11, изд. на: 22, от МВР: 33. Постоянен адрес: Балчик, Ив. Чернев 11. Настоящ адрес: Балчик, Ив. Чернев 11

Във връзка с възникнали договорни отношения, за предоставяне на услуги от банка ААА, и в съответствие с чл. 6, т. 1, б от GDPR, съм съгласен да предоставя личните си данни за обработка от банката. Същите да се използват за обработка от Национална агенция по приходите, банка ААА, счетоводен отдел на ААА. Информиран съм, че личните ми данни, ще се съхраняват за срока на договора с доставчика и в законово определени срокове съгласно счетоводните стандарти.

Фигура 5. Отпечатване на попълнена декларация за конкретен клиент.
Източник: собствена разработка.

В доклада не се дава конкретен програмен код за останалите стъпки, защото този програмен код зависи от средата на разработка, на която е написан банковият софтуер.

Заключение

Законовите промени, включително тези, свързани с подписване на декларации по GDPR, налагат доработване на използваните софтуерни продукти. От особена важност е банковият софтуер. В доклада се представя подход за надграждането му, така че бързо и лесно да се отпечатва декларация по GDPR, да се коригира бланката на декларацията от банковите специалисти, да се следи кои клиенти са подписали декларацията.

Използвана литература

Aleksandrova, Y., S. Parusheva. Social media usage patterns in higher education institutions - An empirical study. // International Journal of Emerging Technologies in Learning, 2019, Vol. 14 №5, pp. 108 – 121, (https://doi.org/10.3991/ijet.v14i05.9720).

Ana-Maria Ramona, S., C. Marian Pompiliu, M. Stoyanova (2020). Data Mining Algorithms for Knowledge Extraction. // Challenges and Opportunities to Develop Organizations Through Creativity, Technology and Ethics, pp. 349–357, (https://doi.org/10.1007/978-3-030-43449-6_20).

Armyanova, M. Design patterns for smart home systems development. // Известия на Съюза на учените – Варна, 2019, том 8, №2, с. 56 – 67.

Armyanova, M. Applying patterns to e-government. // Известия на Съюза на учените –Варна, 2020, том 9, №1, с.156 – 167.

Bankov, B. (2020). Game design principles in enterprise web applications. // 20th International Multidisciplinary Scientific GeoConference Proceedings SGEM 2020. Informatics, Geoinformatics and Remote Sensing, 20. pp. 161–168, (https://doi.org/10.5593/sgem2020/2.1/s07.021).

Cristescu, M. P. Specific aspects of the optimization of the reengineering processes of the distributed information applications. International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM, 2019, Vol.19, №2.1, pp. 627 – 636, (https://doi.org/10.5593/sgem2019/2.1/s07.082).

Czaplewski, M. Managing Frequencies As An Important Area For Regulation Of The Eu Telecommunications Market. // Ekonomiczne Problemy Usług, 2018a, №131, (https://doi.org/10.18276/epu.2018.131/1-09).

Czaplewski, M. (2018b). Organization of goods delivery in e-commerce. // European Journal of Service Management, 2018b, №27, (https://doi.org/10.18276/ejsm.2018.27/1-05).

Czaplewski, M. Selected issues of trust between transaction partners in e-commerce. // European Journal of Service Management, 2018c, №25, (https://doi.org/10.18276/ejsm.2018.25-06).

Czaplewski, M., A. Modzelewska-Stalmach, M. Popiołek. General Data Protection Regulation – results of a pilot study. // European Journal of Service Management, 2018, №28, (https://doi.org/10.18276/

ejsm.2018.28/2-12).

Kuyumdzhiev, I. The dimbi project innovative approaches for teaching business informatics. // Economics and Computer Science 2, 2016, Vol. 2, №5, pp. 26 – 36, (http://eknigibg.net/Volume2/Issue5/spisanie-br5-2016_pp.26-36.pdf).

Kuyumdzhiev, I. A model for timely delivery of it solutions for Bulgarian universities. // 20th International Multidisciplinary Scientific GeoConference Proceedings SGEM 2020. Informatics, Geoinformatics and Remote Sensing, 20. pp. 3–10, (https://doi.org/10.5593/sgem2020/2.1/s07.001).

Miryanov, R., J. Petkov. An application of the relation between arithmetic mean and geometric mean for rational proving some inequalities. // Mathematics and Informatics, 2017, Vol. 60, №4, pp. 363 – 369.

Miryanov, R., V. Yordanova (2017). Optimizing the positioning of serving units in the tourism business. // Mathematics and Informatics, 2017, Vol. 60, №5, pp. 515 – 520.

Nacheva, R., S. Sulova (2020). Internationalization in Context of Education 4.0: AHP Ranking of Bulgarian Universities. // ACM International Conference Proceeding Series, pp. 278 – 284, (https://doi.org/10.1145/3407982.3408006).

Nacheva, R., S. Sulova (2021). Research on the Overall Attitude Towards Mobile Learning in Social Media: Emotions Mining Approach. // Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data, pp. 429–440, (https://doi.org/10.1007/978-3-030-65722-2_27).

Nikolaev, R., T. Milkova, R. Miryanov. A new meaning of the notion “expansion of a number.” // Mathematics and Informatics, 2018a, Vol. 61, №6, pp. 596 – 602.

Nikolaev, R., T. Milkova, R. Miryanov. Some types of problems with symmetric numbers. // Mathematics and Informatics, 2018b, Vol. 61, №2, pp. 200 – 205.

Parusheva, S., D. Pencheva (2022). Modeling a Business Intelligent System for Managing Orders to Supplier in the Retail Chain with Unified Model Language. // Digital Transformation Technology. Singapore: Springer, pp. 375 – 393.

Petrov, P. et al. Using the universal two factor authentication method in web applications by software emulated device. // International Multidisciplinary Scientific GeoConference Surveying Geology and

Mining Ecology Management, SGEM, 2020, №2.1, pp. 403 – 410, (https://doi.org/10.5593/sgem2020/2.1/s07.052).

Petrov, P. et al. Opportunities to use virtual tools in start-up fintech companies. // 20th International Multidisciplinary Scientific GeoConference Proceedings SGEM 2020. Informatics, Geoinformatics and Remote Sensing, 2020, №20, pp. 247 – 254, (https://doi.org/10.5593/sgem2020/2.1/s07.032).

Petrov, P. et al. (2018). Web technologies used in the commercial banks in Finland. // ACM International Conference Proceeding Series, (https://doi.org/10.1145/3274005.3274018).

Petrov, P. et al. A Systematic Design Approach in Building Digitalization Services Supporting Infrastructure. // TEM Journal, 2021, Vol. 10, №1, pp. 31 – 37.

Pólkowski, Z., S.S. Prasad, S. K. Mishra (2021). Retrieval Mechanisms of Data Linked to Virtual Servers Using Metaheuristic Technique. // Data Analytics and Management. Singapore: Springer, pp. 901–909, (https://doi.org/10.1007/978-981-15-8335-3_68).

Raychev, T. Assessment of structural changes of concessions in the water and sewerage sector. // Economics and Computer Science, 2020, Vol. 6, №1, pp. 92–123.

Stoyanova, M. (2020). Good practices and recommendations for success in construction digitalization. // TEM Journal, 2020, Vol. 9, №1, pp. 42 – 47, (https://doi.org/10.18421/TEM91-07).

Todoranova, L. et al. (2020). A model for mobile learning integration in higher education based on students' expectations. // International Journal of Interactive Mobile Technologies, 2020, Vol. 14, №11, pp. 171 – 182, (https://doi.org/10.3991/ijim.v14i11.13711).

Todoranova, L., B. Penchev (2020). A Conceptual Framework for Mobile Learning Development in Higher Education. // ACM International Conference Proceeding Series, pp. 251 – 257, (https://doi.org/10.1145/3407982.3407996).

За контакти: проф. д-р Юлиан Василев
Икономически университет – Варна
E-mail: vasilev@ue-varna.bg

ПО НЯКОИ ВЪПРОСИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ТРУДОВАТА КНИЖКА

доц. д-р Андрияна Андреева
Икономически университет – Варна
д-р Марияна Ширванян
Административен съд – Варна

ON SOME QUESTIONS FOR PROTECTION OF THE PERSONAL DATA IN THE WORK BOOK

Assoc. Prof. Andriyana Andreeva PhD
University of Economics – Varna
Mariyana Shirvaniyan PhD
Administrative Court – Varna

Резюме: В доклада е направен анализ на действащото законодателство, уреждащо института на *Трудовата книжка* в аспекта на защитата на личните данни на физическите лица. Акцентирано е върху правната същност на трудовата книжка и е изследвано качеството на субектите работодател и работник в контекста на изискванията на Закона за защита на личните данни (ЗЗЛД) и 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). На база на анализа са направени обобщения, изводи и препоръки.

Ключови думи*: работник, работодател, трудова книжка, лични данни*

Abstract: The report analyzes the current legislation regulating the institute of "work book" in the aspect of personal data protection of natural persons. The accent is put on the legal nature of the work book and examines the quality of the subjects employer and employee in the context of the requirements according to the Personal Data Protection Act (PDPA) and REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Based on the analysis summaries, conclusions and recommendations are made.

Key words*: employee, employer, work book, personal data*

DOI: https://doi.org/10.36997/PPDD2021.64

Въведение

Трудовата книжка е документ, отразяващ трудовата активност на работниците и служителите. Тя е обект както на нормативна уредба, така и на научен интерес в различните аспекти на проблематиката, свързана с този правен институт и с данните, които инкорпорира (Мръчков 2018: 320 – 325) (Василев 1997: 530 – 534) (Средкова1993) (Мръчков, Средкова, Василев 2009: 1035 – 1044). С оглед на създаване на стабилност в трудовите и впоследствие осигурителни правоотношения законодателят е въвел трудовата книжка. Този официален документ е безспорно с изключителна значимост, от една страна, за субектите на трудовоправната връзка, а от друга страна – за редица държавни институции, натоварени с функции, касаещи обстоятелства, свързани с трудовата дейност – Инспекцията по труда (Димитрова 2019: 71 – 82), Национален осигурителен институт (НОИ), Национална агенция по приходите (НАП) и др. (Андреева 2019: 292 – 299).

Съгласно КТ „Трудовата книжка е официален удостоверителен документ за вписаните в нея обстоятелства, свързани с трудовата дейност на работника или служителя“. Регламентирано е задължение на работодателя в трудовата книжка да вписва точно и своевременно конкретно посочени в правната норма данни за работника или служителя, както и настъпилите по отношение на тях изменения (Банов 2019: 99 –112). На вписване в трудовата книжка подлежат:1. име, дата и място на раждането; 2. адрес; 3. номер на личната карта или друг документ за самоличност и единен граждански номер; 4. образование, професия, специалност; 5. заемана длъжност и организационно звено, в което работи (отдел, цех, служба); 6. уговореното трудово възнаграждение; 7. дата на постъпване на работа; 8. дата и основание за прекратяване на трудовото правоотношение (член, алинея, точка и буква от този кодекс); 9. продължителност на времето, което се при-

знава за трудов стаж, както и на времето, което не се признава за трудов стаж; 10. изплатени обезщетения при прекратяване на трудовото правоотношение; 11. запорни съобщения, предвидени в чл. 512, ал. 5 от Гражданския процесуален кодекс.

Част от данните, регламентирани от КТ като задължителни за вписване в трудовата книжка, са лични и попадат в предметния обхват на защита, предоставен с Общия регламент относно защитата на данните. Лични данни според регламента са тези, които позволяват идентификацията на физическото лице. На този етап тези данни се вписват в трудовата книжка от работодателя, като последната се съхранява от работника и се предоставя на работодателя при настъпването на промяна във вписаните данни или на нови, подлежащи на вписване.

В обществото ни непрекъснато се поставя изискването за законодателното уреждане на електронна трудова книжка (включително и в 46-тото Народно събрание е внесен законопроект на 27.07.2021г. с предложения за регламентация на трудовата книжка). Това поставя няколко въпроса:

1. За необходимостта от съществуването на трудовата книжка и съответно за необходимостта от трансформирането на трудовата книжка от създавана на хартиен носител в електронна, т.е. създавана и съхранявана в електронен формат.

2. За качествата, които придобиват лицата – страни по трудовото отношение предвид изискването за създаване, попълване и съхранение на трудовата книжка.

В доклада се търсят отговорите на поставените въпроси чрез изследване на съществуващите регулации в КТ, ЗЗЛД, Регламент (ЕС) 2016/679 и в Наредбата за трудовата книжка и трудовия стаж (приета с ПМС № 227 от 23.11.1993 г. последно изменение ДВ, №.2 от 3-ти януари 2018 г.).

Разработката има за цел да направи анализ на действащото законодателство, уреждащо института на *Трудовата книжка* в аспекта на защитата на личните данни на физическите лица. Акцентирано е върху правната същност на трудовата книжка и е изследвано качеството на субектите работодател и работник в контекста на изискванията на Закона за защита на личните данни (ЗЗЛД) и 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). На база на анализа са направени обобщения, изводи и препоръки.

За постигане на заложената цел и свързаните с нея изследователски задачи авторите използват традиционните за правните изследвания научни методи и по-конкретно – индукция и дедукция, нормативен и сравнителноправен анализ. Материалът е със заложени предметни ограничения, които са свързани с неговия обем, поради което авторите не претендират за изчерпателност на въпроса.

Докладът е съобразен с регламентацията на разглежданите отношения в законодателството на Р България и Европейския съюз (ЕС) към 30.09.2021 г.

Изложение

В Конституцията на Р България е предвидено правото на неприкосновеност на личния живот, жилището и кореспонденцията на всеки индивид. В чл.32, ал.1 от Конституцията е предвидена съответната гаранция за прокламираните права, чрез регламентирането на правото на защита срещу незаконна намеса и срещу посегателство върху честта, достойнството и доброто име на човека (Петров 1997). След присъединяването на Р България към Европейския съюз (ЕС) регламентите, приемани от законодателните органи на ЕС, имат пряко приложение на територията й, като част от това вторично право на съюза въвежда разпоредби, имащи значение за регламентираните в Конституцията субективни права.

Регламент (ЕС) 2016/679 урежда защитата на физическите лица във връзка с обработването на личните им данни. Тази защита се предоставя по силата на чл. 8, пар. 1 от Хартата на основните права на Европейския съюз (*Хартата*) и чл. 16, пар. 1 от Договора за функционирането на Европейския съюз (ДФЕС), които предвиждат, че всеки има право на защита на личните му данни. Тези разпоредби определят правото на защита на личните данни на човека като негово субективно основно право.

По смисъла на легалното определение на *лични данни*, дадено в регламента, това е всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифи-

цирано (*субект на данни*). Физическо лице, което може да бъде идентифицирано, е лицето, което може да бъде идентифицирано, пряко или непряко, по-конкретно чрез идентификатори като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице. В регламента също е посочено, че *обработване* е всяка операция, съвкупност от операции, извършвани с лични данни или набор от данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване, а *администратор* е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни, когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.

Предвидено е трудовата книжка да бъде издавана на хартиен носител по утвърден образец и в нея от работодателя да бъдат вписвани конкретни данни, които, както вече беше посочено, са включени в обхвата на Регламент **(**ЕС) 2016/679. Съхранението на трудовата книжка, обаче, е възложено на работника. Само при определени изключения съхранението на трудовата книжка е възложено на работодателя и на териториалните звена на Националния осигурителен институт (Андреева, Йолова 2020: 193 –194, 213 – 214) и на Инспекцията по труда. От тези изключения ни интересува само предвиденото по отношение на работодателя и то е, когато работникът не е получил трудовата си книжка. Начинът, по който са регламентирани задълженията на страните по трудовото правоотношение – работник и работодател относно вписването на данните в трудовата книжка и съхранението ѝ, налага извода, че по отношение на последната работодателят не се явява *администратор на лични данни*. Работодателят има задължението само да въведе необходимата по обем информация в трудовата книжка и тази информация не подлежи в нейната цялост

на по-нататъшна обработка от него. Тази информация се извлича от оригинални документи или от документи, които са заверени за вярност, представени от работника или от трети лица (например в случаите на налагането на запор върху част от трудовото възнаграждение) или подписани между работника и работодателя (например договор за изменение на трудовото правоотношение или за прекратяването му).

При прекратяването на трудовото правоотношение с един работодател работникът сам представя съхраняваната от него трудова книжка пред следващия работодател. Работникът се явява лицето, което, съхранявайки трудовата си книжка, съхранява и личните данни, които са вписани в нея.

С други думи при съществуващата регламентация, въпреки че в трудовата книжка се съдържат лични данни, попадащи в обхвата на регламента, по отношение на тези данни (конкретно само вписаните в трудовата книжка) работодателят не се явява администратор на лични данни, поради което и не носи административнонаказателна отговорност (Димитрова 2020: 254 – 262; Димитрова 2019: 56 –70) за неправилната им обработка. Това не се променя от практиката, наложена от някои работодатели, да съхраняват трудовите книжки в трудовите досиета на работниците. В този случай работодателят поема и изпълнява чуждо задължение възникнало *ex lege* и именно от начина на възникване на задължението и липсата на регламентирана от закона възможност за прехвърлянето му на друго лице се извлича изводът, че при приемането на трудовата книжка за съхранение, работодателят не се превръща в администратор на лични данни по отношение на информацията в последната, въпреки че се явява администратор на лични данни по отношение на информацията предоставена, обработвана и съхранявана в трудовото досие на работника.

При регламентирането на електронната трудова книжка следва да се съобрази, че основното предназначение на трудовата книжка към момента на въвеждането на този правен институт е отчитането на трудовия стаж на работника. Трудовият стаж обаче може да се установи, освен с трудова, също и с осигурителна и занаятчийско-ученическа книжка и с удостоверение, издадено въз основа на изплащателни ведомости или партидни книги или други документи, удостоверяващи време, което се признава за трудов стаж по чл. 354 от Кодекса на труда. Докато при предходната регламентация (същест-

вувала преди 1991 г.) трудовият стаж е имал основно значение за реализирането на правата на работника да получи редица социални плащания по дългосрочното и краткосрочното обществено осигуряване, сега тези права се реализират при доказването на осигурителен стаж. Трудовият стаж намалява своето значение за работниците да получат и други права по трудовото правоотношение – като правото на процент върху трудовото възнаграждение за прослужено при работодателя време. Това право би следвало да се трансформира в задължение на работодателя да увеличава с определен процент трудовото възнаграждение на работника всяка календарна година. При намаляването на правното значение на трудовия стаж за работника следва на първо място да се направи анализ на необходимостта да се въвеждат задължения (на работника и работодателя) за създаването и съхранението на трудова книжка, в която се дублира частично информацията с вписваната в осигурителната книжка и не е ли целесъобразно отпадането на регламентацията на първата и едва след това да се прецени следва ли, чрез законодателни промени, трудовата книжка от създавана и съхранявана на хартиен носител да се трансформира в електронен формат.

Необходимо е да се отчете, че регламентирането на трудовата книжка в електронен формат ще постави изисквания както към работодателя, така и към работника – за закупуване и поддържане на определени технически устройства и софтуер; за съвместимостта на софтуерите на различните работодатели; за съхранението в електронна среда на личните данни (това налага ясно посочване кой, как и къде ще ги съхранява – работникът или работодателят и кой ще носи отговорност за защитата им); как ще се подходи при несъвместимост на програмите, използвани от различните работодатели или при загубване на данни поради технически проблеми и т.н.. При решаване на поставените въпроси следва да бъдат разгледани и интересите на работодателите, които включват например да не бъдат прекомерно натоварени с администриране на доказателствата относно трудовия и осигурителния стаж (Йолова 2015: 113 – 117, Йолова 2015(2): 20 – 29) на работниците (и при сега действащата уредба имат значителни по обем задължения, между които – да водят трудово досие на работника; да вписват данни в трудовите и осигурителните книжки и да заверяват последните; да подават по електронен път данни за сключените и прекратени трудови договори пред НАП), както и с разходи

по създаването, обработването и съхранението на тези доказателства. Без да се подценява значението на използването на различни дигитални инструменти в администрирането на персонала, допринасящо за усъвършенстване на процесите по управление на хора (Иванова 2020), при преценката за необходимост от въвеждане на електронна трудова книжка в българското законодателство следва да бъде спазено съображение 13 от преамбюла на регламента,[1] като бъдат отчетени спецификите в дейността на микропредприятията и малките и средните предприятия при прилагането на законодателството в областта на събирането, обработването, съхранението и защитата на личните данни. А това, както вече беше подчертано, налага процесите по дигитализацията на дейността на предприятията да не бъдат прекомерно оскъпени (особено за работодатели, които имат малък брой работници и малък обем производство и печалба), а и следва да се мисли в посока на отпадане на задължения на работодателя като например изискването за подаване на данни в НАП за сключените трудови договори, като се постави на преценка и необходимостта от свързването на базите данни на работодателите относно трудовите книжки с базите данни на НАП за сключените трудови договори.

Заключение

Правото на законосъобразно обработване на личните данни на физическите лица като аспект на правото на неприкосновеност на личния живот е измежду личните права, осигуряващи духовния и физическия интегритет на личността (Петров 1997). За реализирананието на това право от изключително значение е нормативната уредба на предоставянето, събирането, обработването и съхраняването на

[1] Съгласно което: „За доброто функциониране на вътрешния пазар е необходимо свободното движение на лични данни в рамките на Съюза да не се ограничава, нито забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни. За да се отчете особеното положение на микропредприятията и малките и средните предприятия, в настоящия регламент е включена дерогация за организации с по-малко от 250 служители по отношение на воденето на регистър. Освен това, институциите и органите на Съюза, както и държавите членки и техните надзорни органи, се приканват да вземат предвид специфичните нужди на микропредприятията и малките и средните предприятия при прилагането на настоящия регламент. Разбирането на понятието за микропредприятия и малки и средни предприятия следва да се основава на чл. 2 от приложението към Препоръка 2003/361/ЕО на Комисията“.

информацията за физическите лица, включително и чрез уредбата на изискванията към носителите на тези данни (хартиен, електронен, друг) и на начина на съхранението им.

След проведения анализ се налага извод, без да се изключва приложението на чл. 25 и чл. 25к от ЗЗЛД, че регламентацията на съдържанието и начина на съхранението на трудовата книжка по българското законодателство не определят работодателя като администратор на личните данни на работника в нея, поради което и при нарушения във връзка с обработването им съгласно ЗЗЛД, но при спазването на изискването на КТ за вписването на данните и връщането на трудовата книжка на работника, работодателят не следва да носи административната отговорност, предвидена за администратор на личните данни, доколкото съхранението на трудовата книжка е задължение на работника.

Използвана литература

Александров, А. Нови опити за „дигитализиране“ на трудовата книжка. // Труд и право, 2020, № 11, с. 16 –24.

Aleksandrov, A. Novi opiti za „digitalizirane“ na trudovata knizhka. // Trud i pravo, 2020, № 11, s. 16 – 24.

Александров, А. (2020). За неслучилото се дигитализиране на трудовоправната документация и правораздаването по трудови спорове и вредите, които понася обществото от това. // Правото и бизнесът в съвременното общество. Сборник с доклади от 3-та Национална научна конференция. Варна: Наука и икономика, с. 338 – 348.

Aleksandrov, A. (2020). Za nesluchiloto se digitalizirane na trudovopravnata dokumentatsiya i pravorazdavaneto po trudovi sporove i vredite, koito ponasya obshtestvoto ot tova. V: Pravoto i biznesat v savremennoto obshtestvo. Sbornik s dokladi ot 3-ta Natsionalna nauchna konferentsiya, 13 noemvri. Varna: Nauka i ikonomika, s. 338–348.

Андреева, А. (2019). За значимостта на трудовата книжка и потребността от нови нормативни решения в уредбата. // Правото и бизнесът в съвременното общество. Сборник с доклади от 2-ра Национална научна конференция. Варна : Наука и икономика, с. 292 – 299.

Andreeva, A. (2019). Za znachimostta na trudovata knizhka i potrebnostta ot novi normativni resheniya v uredbata. Pravoto i biznesat v savremennoto obshtestvo : Sbornik s dokladi ot 2-ra Natsionalna nauchna

konferentsiya. Varna : Nauka i ikonomika, s. 292 – 299.

Андреева, А., Г. Йолова (2020). Трудово и осигурително право. Варна: Наука и икономика, с.193 – 194, 213 – 214.

Andreeva, A., G. Yolova (2020). Trudovo i osiguritelno pravo Varna: Nauka i Ikonomika, s. 193 –194, 213 – 214.

Банов, Х. Задължението на работодателя за предаване на трудовата книжка и отговорността за неизпълнението му. // Бизнес и право, 2019, № 3, с. 99–112.

Banov, H. Zadalzhenieto na rabotodatelya za predavane na trudovata knizhka i otgovornostta za neizpalnenieto mu. // Biznes i pravo, 2019, № 3, s. 99–112.

Василев, А. (1997). Трудово право. Бургас: БСУ.

Vasilev, A. (1997). Trudovo pravo. Burgas: BSU.

Димитрова, Д. (2020). По някои въпроси на административноправната защита на правото на труд. Правото и бизнесът в съвременното общество. // Сборник с доклади от 3-та Национална научна конференция. Варна: Наука и икономика, с. 254 – 262.

Dimitrova, D. (2020). Po nyakoi vaprosi na administrativnopravnata zashtita na pravoto na trud. Pravoto i biznesat v savremennoto obshtestvo. // Sbornik s dokladi ot 3-ta Natsionalna nauchna konferentsiya. Varna: Nauka i ikonomika, s. 254 – 262.

Димитрова, Д. (2019). Съвременна роля на изпълнителна агенция „Главна инспекция по труда“ за защита правата на страните по трудовите правоотношения. Правото и бизнесът в съвременното общество // Сборник с доклади от 2-ра Национална научна конференция. Варна : Наука и икономика, с. 71 – 82.

Dimitrova, D. (2019). Savremenna rolya na izpalnitelna agentsiya „Glavna inspektsiya po truda“ za zashtita pravata na stranite po trudovite pravootnosheniya. Pravoto i biznesat v savremennoto obshtestvo. // Sbornik s dokladi ot 2-ra Natsionalna nauchna konferentsiya. Varna : Nauka i ikonomika, s. 71 – 82.

Димитрова, Д. (2019). Съвременни тенденции в административното законодателство на България. Правото и бизнесът в съвременното общество. // Сборник с доклади от 2-ра Национална научна конференция. Варна : Наука и икономика, с. 56 – 70.

Dimitrova, D. (2019). Savremenni tendentsii v administrativnoto zakonodatelstvo na Balgariya. Pravoto i biznesat v savremennoto obshtestvo : Sbornik s dokladi ot 2-ra Natsionalna nauchna konferentsiya.

Varna : Nauka i ikonomika, s. 56 – 70.

Иванова, П. Новите тенденции в трудовите отношения. // Известия, 2020, том 64, №4, с.401 –418.

Ivanova, P. Novite tendentsii v trudovite otnosheniya. // Izvestiya , 2020, tom 64, №4, s. 401 – 418.

Йолова, Г. (2015,1). За някои хипотези на признаване на осигурителен стаж. Върховенството на закона – предпоставка за развитие на бизнеса и за икономически растеж, София: УНСС, с. 113 – 117.

Yolova, G. (2015,1). Za nyakoi hipotezi na priznavane na osiguritelen stazh. Varhovenstvoto na zakona - predpostavka za razvitie na biznesa i za ikonomicheski rastezh, Sofiya: UNSS, s. 113 – 117.

Йолова, Г. Осигурителен стаж и сродни институти при признаване на някои видове обезпечения. Известия, 2015, №3, с. 20 – 29.

Yolova, G. Osiguritelen stazh i srodni instituti pri priznavane na nyakoi vidove obezpecheniya. Izvestiya, 2015, № 3, s. 20 – 29.

Мръчков, В. (2018). Трудово право. София: Сиби.

Mrachkov, V. (2018). Trudovo pravo. Sofiya: Sibi.

Мръчков, В., К. Средкова, А. Василев (2009). Коментар на Кодекса на труда. София: Сиби.

Mrachkov, V., K. Sredkova, A.Vasilev (2009). Komentar na Kodeksa na truda. Sofiya: Sibi.

Петров, Т. Система на основните права на гражданите в демократичната държава. Въведение в политологията, книга втора. Варна: Министерство на отбраната, Висше военноморско училище „Н.Й.Вапцаров”; с. 87 – 88.

Petrov, T. (1997). Sistema na osnovnite prava na grazhdanite v demokratichnata darzhava, Vavedenie v politologiyata, kniga vtora. Ministerstvo na otbranata, Visshe voennomorsko uchilishte „N.Y.Vaptsarov”, s. 87 – 88.

Петров, Т. Класификация на системата на основните права на гражданите. //Теория, методика и управление на учебно-възпитателния процес политология, връзки с обществеността и право. Юбилейна научна сесия 97 с международно участие, 1997, № 56, с. 380 – 387.

Petrov, T. Klasifikatsiya na sistemata na osnovnite prava na grazhdanite. // Teoriya, metodika i upravlenie na uchebno-vazpitatelniya protses politologiya, vrazki s obshtestvenostta i pravo. Yubileyna nauchna sesiya 97 s mezhdunarodno uchastie, 1997, № 56, s. 380 – 387.

Средкова, К. (1993). Трудова книжка. Практическо право (2). София: Сиби.

Sredkova, K. (1993). Trudova knizhka. Prakticheskо pravo (2). Sofia: Sibi.

За контакти: доц. д-р Андрияна Андреева
Икономически университет - Варна
e-mail: a.andreeva@ue-varna.bg
д-р Марияна Ширванян
Административен съд-Варна
e-mail: irgo@abv.bg

ЗА ЕЛЕКТРОННИТЕ ЗДРАВНИ ЗАПИСИ В КОНТЕКСТА НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

доц. д-р Галина Йолова
Икономически университет – Варна

FOR ELECTRONIC HEALTH RECORDS IN CONTEXT FOR PROTECTION ON PERSONAL DATA

Assoc. Prof. Galina Yolova, PhD
University of Economics - Varna, Bulgaria

Резюме: Разработката анализира същността и принципите при използване на електронните здравни записи в контекста на изискванията за защита на личните данни, установени в 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 предвид нуждата от адекватни механизми за тяхната поверителност с оглед охрана интересите и правата на пациентите и осигурените лица. Извежда се същността на електроните здравни записи като цифрови инструменти за съхраняване и споделяне на данни, изясняват се принципите за създаване, ползване, съхранение и споделяне на записите в контекста на принципите на защита на личните данни, както и се систематизират обобщения за нуждата от гарантиране на поверителност, адекватна и ефективна правна защита.

Ключови думи: *електронен здравен запис, защита на личните данни, принципи за защита на личните данни*

Abstract: The development analyzes the nature and principles of the use of electronic health records in the context of the data protection requirements set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data. personal data and on the free movement of such data, and given the need for adequate mechanisms for their confidentiality in order to protect the interests and rights of patients and insured persons.The essence of electronic health

records as digital tools for data storage and sharing is presented, the principles for creation, use, storage and sharing of records in the context of the principles of personal data protection are clarified, as well as summaries of the need to ensure confidentiality, adequate and effective legal protection.

Key words*: electronic health record, personal data protection, principles of personal data protection*

DOI: https://doi.org/10.36997/PPDD2021.76

Въведение

Като важна част от инструментите на електронното здравеопазване електронните здравни записи са компонент от цялостната система на цифровизация на здравните услуги, предвидена като поетапно изграждане в Националната здравна стратегия 2014 – 2020, Програмата за развитие на електронното здравеопазване (2014), Пътната карта към програмата за развитие на електронното здравеопазване (2014), Националната здравна стратегия 2020 (Политика 2.6 „Развитие на електронно здравеопазване“). Базисни в тази система са понятията „електронно здравно досие“, „пациентски здравен запис“ (Electronic Patient Records – EPR), eGenomics, PACS (архивна система за образната диагностика), e-Health Portal, „е- рецепта“, „е – доставка“, „е-аптека“, „телемедицина“, „мобилно здравеопазване“ и др. (Йолова 2020).

От друга страна, те са свързани пряко и с процесите по надграждане и доразвитие на Националната здравноинформационна система, в аспектите на възможността за централизиран достъп до здравните услуги чрез Националния електронен здравен портал като част от e-Health инициативите на ЕС за болничната помощ и общопрактикуващите лекари.

В тези насоки **цел на разработката** е анализиране същността и принципите при използване на електронните здравни записи в контекста на изискванията на защита на личните данни, установени в 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 предвид нуждата от адекватни механизми за тяхната

поверителност с оглед охрана на интересите и правата на пациентите и осигурените лица. В изпълнение на целта са и следните изследователски задачи:

1. Анализиране същността на електронните здравни записи като цифрови инструменти за съхраняване и споделяне на данни.

2. Принципи за създаване, ползване, съхранение и споделяне на записите в контекста на принципите на защита на личните данни.

3. Извеждане на обобщения за гарантиране на поверителност и адекватна и ефективна правна защита.

За постигане на заложената цел и свързаните с нея изследователски задачи се използват индуктивен и дедуктивен подход, формално-юридически, нормативен и сравнителноправен анализ.

Докладът е съобразен с регламентацията на разглежданите отношения в законодателството на Р България и Европейския съюз (ЕС) към 30.09.2021 г.

Изложение

1. Същност и съдържание на електронните здравни записи като елемент на електронното здравеопазване

Инфраструктурата на здравните данни като общоевропейска политика е част от Европейската стратегия за данните (19 февруари 2020 г.), чрез която следва да се доразвият цифровите услуги и политики в европейските референтни мрежи и в частност – проектът „Геномика“. В тази връзка общото европейско пространство на здравни данни е приоритетна политика за периода 2019 г. – 2025 г., която е предвидено да се базира на стълбовете – стабилна система за управление на данните и правила за обмена на данни, качество на данните, стабилна инфраструктура и оперативна съвместимост, както и на принципите на прозрачност и защита в ползването и преносимостта на данните съгласно чл. 20 от Общия регламент относно защитата на данните. В тази връзка се очаква то да осигури качествен обмен и достъп до здравни данни и използването им с цел ефективно и качествено здравно обслужаване, както и за целите на здравните изследвания, разработването на здравни политики и подкрепяне на иновациите в прилагането на общите здравни стратегии.

Електронният здравен запис (ЕЗЗ) като интернет базиран интерактивен запис е механизъм, чрез който съгласно чл. 28г., ал.3 от За-

кона за здравето (ЗЗ) Националната здравноинформационна система събира, обработва и съхранява информация за здравното състояние на населението. В този смисъл като способ за улесняване обменът на медицинските документи и интегрирането им в множество доставчици, терминът „електронен здравен запис“ се прилага за интегриране на процесите на съхраняване на данни и едновременно с това – за осигуряване на достъп до електронния медицински регистър на пациента. Изграждането му е част от процесите по създаване на връзка между разработени към момента системи в различни организации в сферата на здравеопазването, в това число НЗОК, доброволни дружества, национални центрове и изпълнителни агенции и лечебни заведения. Целта на тази интеграция е обединяване на процесите в здравеопазването в единна система с възможност за обмен и контрол на информацията в реално време, включваща, освен електронен пациентски запис, още и електронна автентификация, регистри на основните участници в системата на здравеопазването и обвързаност между тях.

Съгласно дефиницията, дадена от Европейския съюз, ЕЗЗ е „изчерпателен медицински запис или проста документация на минало и настоящо физическо и умствено здравно състояние на индивида, в електронна форма, предоставящ лесен достъп до тази информация за медицинско лечение и други, свързани с това цели“. Като обединяващ система от първични медицински, здравни, персонални и административни данни за пациента е предвидено той да съдържа базисна и минимална систематика от данни в следните насоки:

- Данни на пациента – лични данни, данни за контакт, данни за здравно осигуряване (задължително и доброволно), антропометрични данни (ръст тегло, и др.).
- Лични и професионални данни за общопрактикуващите лекари, при които лицето е било или е записано – лични и професионални данни: имена, адреси, УИН, специалности, лечебни заведения, в които работят.
- Контакти при спешност (име, роднинска връзка, адрес, телефон).
- Кръвна група, резус фактор.
- HLA типизиране.
- Кръвопреливане и кръводаряване – на коя дата е имало кръвопреливане, с какъв кръвен продукт.

- Рискови фактори и рискови групи с описание на риска,
- Съгласие/несъгласие за донорство.
- Поставени до момента диагнози.
- Алергии.
- Имунизации, в това число дати на направени имунизации, търговско наименование на ваксината, количество и партидния номер на използваната ваксина.
- История на предписаните и отпуснати лекарствени продукти, медицински изделия и храни за специални медицински цели.
- Прегледи с информация за направени амбулаторни прегледи, която съдържа данните от амбулаторните листове.
- Назначени и изпълнени медико-диагностични дейности.
- Диспансеризация и хоспитализации.
- Фамилна обремененост и наследствени заболявания.
- Остри заразни заболявания, временна или трайна неработоспособност.

Очевидно е, че се касае за една сравнително широка систематика от записи в реално време, целяща всеобхватност на клиничния статут и медицинската история на лицето, създадена с цел незабавно доставяне на информация до оторизираните потребители. Като свързан с възможно най-точна и актуална информация за здравето и статуса на пациентите чрез него се цели осигуряване на бърз достъп в условията на координирано здравно обслужване, както и облекчаване на административната тежест при оказване на първична и вторична медицинска помощ, профилактика и превенция на заболяванията. Както се отбелязва в Националната здравна стретегия, по този начин се „дава възможност да се извършват онлайн повече административни и здравни услуги в сектора, осигурява се достъп до информация на пациента за собственото му здраве, подобряват се взаимовръзките между отделните нива на системата, подобрява се качеството на медицинските услуги и ефективността на разходването на публичните средства за здравеопазване“.

От друга страна обаче, повече от безспорно е, че правилното обработване и съхраняване на данните следва да е свързано с високи нива на сигурност на споделянето на медицинска информация, както и непрекъснато подобряване на сигурността и поверителността на данните за пациента.

2. Принципи при обработка и достъп на електронни здравни записи в контекста на защита на личните данни

Както вече се спомена, предвидено е европейското пространство на здравни данни да се базира на принципите за прозрачност и защита в ползването и преносимостта на данните, както и на основните стълбове – стабилна система за управление на данните и правила за обмена на данните, качество на данните, стабилна инфраструктура и оперативна съвместимост.

Съгласно Регламент (ЕС) 2016/679 личните данни за здравословното състояние на лицата следва да обхващат всички данни, свързани със здравословното състояние на субекта на данните, които разкриват информация за физическото или психическото му здравословно състояние в миналото, настоящето или бъдещето. В този смисъл обемът на събираната информация в хода на регистрацията за здравни услуги или тяхното предоставяне следва да се отнасят до характеристики, определени за дадено физическо лице с цел уникалното му идентифициране за здравни цели, информация, касаеща генетични данни и биологични проби, заболяване, увреждане, риск от заболяване, медицинска история, клинично лечение или физиологично или биомедицинско състояние на субекта на данните, независимо от източника на информация, в частност – лекар или друг медицински специалист, болница, медицинско изделие или инвитро диагностично изследване.

Общите принципи, свързани с обработването на лични данни, заложени в регламента са законосъобразно, добросъвестно и по прозрачен по отношение на субекта на данните начин обработване и събиране за конкретни, изрично указани и легитимни цели – *свеждане на данните до минимум*, точност и актуалност, съхраняване във форма, позволяваща идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни, обработване по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки (*цялостност и поверителност*). (Александров 2016; Александров 2017; Александров 2018; Александров 2020; Andreeva, Mateeva 2018).

При това в чл. 9, по повод обработване на специални категории

лични данни, в което число следва да се отнасят и данните, свързани със здравния статус на лицата, е изрично предвидена забраната за обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическото лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

Забраната не се прилага при алтернативност на условията – обработването да е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на правото на Съюза, правото на държава членка или договор с медицинско лице. От друга страна, дерогиране на забраната е допустима, в случай че обработването е необходимо от съображения от обществен интерес в областта на общественото здраве, осигуряването на високи стандарти за качество и безопасност на здравните грижи, лекарствените продукти или медицинските изделия, но при едновременно и навременно прилагани подходящи мерки за гарантиране на правата и свободите на субекта на данните и, по-специално, опазването на професионална тайна.

В чл. 32 на регламента са и предвидените мерки за сигурност при обработването на данните, съгласно който, 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, администраторът и обработващият лични данни следва да прилагат подходящи мерки за осигуряване на съобразено с този риск ниво на сигурност, в частност – 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 това, при оценката на подходящото ниво на сигурност, се вземат предвид по-специално рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или

достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

На национално ниво стабилитетът и законосъобразността при ползване на данни от здравните записи се гарантират, от една страна, от общите рамки за функциониране на Националната здравнооинформационна система, която съгласно чл. 28г ЗЗ следва да се основава на принципите – гарантиране на актуалност и точност на предоставените и съхраняваните данни, осигуряване на подходяща среда за обмен на данни, гарантиране на регламентиран достъп, осигуряване на оперативна съвместимост и информационна сигурност.

От друга страна и в конкретика, защитата на данните по здравни записи следва да се гарантира и от правилата и механизмите за достъп. Така съгласно чл. 28д, ал.1 ЗЗ право на безвъзмезден достъп до Националната здравноинформационна система, в това число и до електронните здравни записи, имат гражданинът – до информацията в неговия електронен здравен запис, лечебните и здравните заведения и Националната здравноосигурителна каса при и по повод осъществяване на функциите си, застрахователните дружества, лицензирани по отделни видове медицински застраховки, както и държавни органи, за които в закона е предвиден достъп до регистри с национално значение.

Предоставянето на достъп до информацията в електронния здравен запис на гражданите и на лечебните и здравните заведения, на Националната здравноосигурителна каса, застрахователните дружества и държавните органи се извършва само след изрично писмено съгласие при условия и по ред, определени с наредба на министъра на здравеопазването. (Андреева, Йолова 2020).

В технологичен порядък е предвидено пациентите да могат получават достъп до порталния интерфейс след регистрация, като използват квалифициран електронен подпис за идентификация – КЕП или до националната система за електронна идентификация, но само относно записите за тях или за лицата, на които са родители, настойници или попечители. Медицинските специалисти от своя страна трябва да достъпват системата и здравната информация след предварителна регистрация, като се идентифицират с електронен подпис, като прегледът на здравната информация следва да се осъществява след изрично съгласие от пациента. Във всички случаи достъпът до здравната информация трябва да се управлява от пациента и, като ми-

нимум, да се дефинират конкретният медицински специалист, който да достъпва здравната информация, конкретната здравна информация в досието на пациента, за която се дава съгласие за достъп, както и периодът от време за достъп до данни. Всеки достъп до данните следва да се регистрира в контролната част на портала.

Заключение

Цифровизацията на здравните услуги и нейното качествено и в интерес на всички участници изграждане безспорно предполага такива механизми и средства, които взети в своята систематика, следва да допринесат за едно ново и качествено по-добро ниво на здравна грижа (Андреева, Йолова 2021). Същевременно обаче прилагането и развитието й в практиките на здравните системи следва да е функционално на адекватни нива на гарантиране правата, достойнството и личното пространство на индивида чрез висока степен – и законодателна, и технологична, на защита при обработването, съхраняването и запазване поверителността на личните данни.

Досега установените – и европейски, и на национално ниво разпоредби и законови механизми очертават една добра нормативна рамка, въпреки че електронните здравни записи съдържат в максималната възможна степен чувствителна лична информация, на чието обработване следва да отговаря значително по-висок праг за законосъобразност при съхраняването, ползването и обмена. От друга страна, предизвикателства пред нормативната рамка и адекватното й приложение са недобрата технологична готовност, слабото ниво на защита на програмните продукти, недобрата координираност в отделните сегменти на електронното здравеопазване, създаващи реални заплахи както за злоупотреба с данни или неправомерното им разпространяването, така и за кибератаки и здравен тероризъм.

Използвана литература

Andreeva,A, Z. Mateeva. Employers as Personal Data Administrators – Specifics and Requirements in the Context of the Information Society. // Globalization, the State and the Individual, 2018, Vol.2, №18, pp. 139 – 147.

Александров, А. (2016). Защита на личните данни на работници-

те и служителите. София: Труд и право.

Александров, А. (2017). Новият Общ регламент за защита на личните данни в ЕС и какво трябва да знаят работодателите за него. София: Труд и право, с. 1 – 28.

Александров, А. (2018). Общият регламент за защита на личните данни в ЕС: нови изисквания и предизвикателства за работодателите. // Сборник доклади от Юбилейна международна научна конференция на тема „Ролята и значението на международното и наднационалното право в съвременния свят. София: УНСС, с. 202 –217.

Александров, А. (2020). Защо вътрешното ни законодателство по защита на личните данни (отново) не покрива изискванията на правото на ЕС. Сборник доклади от научна конференция на тема „Традиция и развитие на законодателството в сферата на икономиката. София: ИК УНСС, с. 33 – 43).

Андреева, А., Г. Йолова. Изграждане на Националната здравноинформационна система – тенденции и правна рамка. // Медицински мениджмънт и здравна политика. 2020, том 51, №1, с. 27 – 51.

Андреева, А., Г. Йолова (2021). Цифровата трансформация в здравеопазването в контекста на правото на достъп до медицинска помощ. // Медицинско право и здравеопазване, 2021, №1, 20 – 37.

Йолова, Г. (2020). Еволюция на правната рамка за развитие на електронното здравеопазване. // Правото и бизнесът в съвременното общество. Сборник с доклади от 3-та Национална научна конференция. Варна: Наука и икономика, с. 324 – 329.

Национална здравна стратегия 2020, с. 90, (https://www.mh.government.bg/media/filer_public/2016/09/12/nzs_2020.pdf)

Health informatics — Electronic health record — Definition, scope, and context, ISO TC 215, ISO/TR 20514, ISO TC 215/WG 1, 2005-01-22.

Министерство на здравеопазването – Техническо задание по обособена позиция № 4 „избор на изпълнител на дейност 9 – Изграждане на единно национално електронно медицинско досие/ електронен здравен запис“ – приложение № 4, (https://www.mh.government.bg/media/filer_public/2018/08/28/tekhnichesko_zadanie_po_obosobena_pozitsiia__4-prilozhenie__4.pdf).

За контакти: доц. д-р Галина Йолова
Икономически университет – Варна
e-mail: ina_yolova@ue-varna.bg

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В СОЦИАЛНОТО ОСИГУРЯВАНЕ В УСЛОВИЯТА НА ЦИФРОВИЗАЦИЯ

доц. д-р Христина Благойчева
Икономически университет – Варна

PROTECTION OF PERSONAL DATA IN SOCIAL SECURITY IN THE SETTINGS OF DIGITALIZATION

Assoc. Prof. Hristina Blagoycheva, PhD
University of Economics - Varna, Bulgaria

Резюме: Цифровизацията увеличава потенциала на социалното осигуряване за по-висока ефективност при предоставянето на нови услуги и разгръщането на мащабни социални програми. Съществува обаче възможността тези технологии да станат предпоставка за нерегламентиран достъп до информация и лични данни, съхранявани в цифровата мрежа. Затова целта на доклада е да се изведат някои предизвикателства в тази насока и да се потърсят възможни решения.

Ключови думи: *социално осигуряване, цифровизация, поверителност, лични данни*

Abstract: Digitization increases the potential of social security for greater efficiency in the provision of new services and the deployment of large-scale social programs. However, there is a possibility that these technologies will become a prerequisite for unregulated access to information and personal data stored in the digital network. Therefore, the purpose of the report is to identify some challenges in this direction and to seek possible solutions.

Keywords: *social security, digitization, confidentiality, personal data*

DOI: https://doi.org/10.36997/PPDD2021.86

Въведение

Функционирането на социалното осигуряване се обуславя от необходимостта за задоволяване на широк спектър индивидуални потребности, свързани с издръжката на живота. То може да се разглежда

като вид защитна мрежа, предпазваща осигурените лица от бедност и други икономически последици при временна или постоянна загуба на трудови доходи. В тази връзка и осигурителната система се въвежда в законодателствата като гаранция за закрила на базисни човешки потребности, възникващи както при загубата на способности за полагане на труд, така и предвид подпомагане и солидарна съпричастност на маргинални житейски условия на индивида, лишаващи го от средства за достойно и социално приемливо съществуване (Йолова 2016: 181). Логично социалното осигуряване е една от най-значимите съвременни правителствени програми и в обхвата му попада огромна част от населението на съответната страна. То работи като икономически, социален и политически стабилизатор, редуцира доходните неравенства до приемливи нива и осигурява механизми за облекчаване и предотвратяване на бедността .

За да подобрят ефективността и качеството на услугите за бенефициентите си, социалноосигурителните институции все по-широко се отварят към използването на цифровите технологии. Цифровизацията позволява нови услуги, ориентирани към потребителите и разгръщането на мащабни социални програми, включващи дори организации на национално и до известна степен на международно ниво. Автоматизираната обработка на данните спомага програмите за социална защита да се прилагат на основата на информационно обосновани решения. А увеличеното използване на мобилни технологии дава по-добър достъп на гражданите до социалноосигурителни онлайн услуги.

Успоредно с многото ползи обаче съществува и възможността цифровите технологии да създадат предпоставки за нерегламентиран достъп до информация и лични данни, съхранявани в различни възли на социалноосигурителната мрежа. Затова въпросът за гарантиране на сигурността на данните и зачитане на правото на гражданите на поверителност е по-значителен отвсякога. Използването на цифровите технологии за подобряване на социалноосигурителните мероприятия не трябва да се осъществява в противоречие със защитата на личните данни.

Целта на настоящия доклад е както да се изведат основните предизвикателства, които цифровизацията поставя пред социалноосигурителните институции по защитата на информацията и личните данни, така и да се потърсят възможни решения. В тази връзка се

разглеждат предимствата за социалноосигурителната система от използването на цифровите технологии и възможните рискове за поверителността и сигурността на личните данни на обхванатите лица. Представят се и както предприетите мерки, така и някои допълнителни решения.

1. Използването на лични данни в цифрова среда

Институциите, провеждащи социалноосигурителните мероприятия, не могат да функционират без достъп до лични данни. Те съхраняват и ежедневно оперират с огромно количество лична информация. Тази информация може допълнително да се използва за генериране на услуги с добавена стойност, за подобряване на дизайна на програмата или дори за прогнозиране на бъдещи ползи.

Някои от ползите са систематизирани в табл. 1

Таблица 1

Предимства от интегрирането на данните в цифровите системи

За политиката и планирането в социалното осигуряване	За администраторите на програмите	За бенефициентите
Идентифициране на планираните популации, профилиране на нуждите и характеристиките	Споделени ресурси за прием и регистрация във „фронт офис“	Насърчаване на осведомеността и достъпа до множество предимства и услуги
Подобрена ефективност, точност и качество на данните => по-добро използване на публичните разходи	По-ниски административни разходи	Може да кандидатстват за много програми едновременно с по-прости процедури, спестявайки време – разходи – посещения
Мониторинг кой какви програми получава, идентифициране на пропуски в обхвата, дублиране, допълване	Подобрена точност, качество на данните, ефективност, прозрачност => по–малко дублиране и грешки	Достъп до техните данни, информация за получените обезщетения и статут на допустимост

Улесняване на координираното реагиране на социалните програми на кризи	Улесняване на посредничеството и сезиране, интегрирано управление на случаи	По-ефективни и координирани обществени услуги

Източник: адаптирано по Socialprotection.org. (2019).

Очевидно дигитализирането на информацията в социалното осигуряване има широк потенциал за подобряване на дейността му. Тя може да ограничи фрагментираните, изолирани интервенции за социална защита, подкрепяйки системния подход към универсализирането им и да свърже бенефициентите на системата с други услуги и възможности за подкрепа. Цифровите технологии могат да поддържат по-точни и ефективни услуги, чрез автоматизиране и подобрено управление на данните. Те редуцират натоварването на персонала в социалноосигурителните институции и позволяват по-информирани управленски решения. Т.е. могат да предоставят по-удобни, по-бързи и по-сигурни услуги на бенефициентите (Handayani et al. 2017).

Успоредно с ползите обаче могат да възникнат някои предизвикателства и рискове, сред които както увеличаване на разходите и сложността, така и рискове за поверителността и сигурността на личните данни. Това безспорно следва да е свързано с изключителни нива на защита при управлението и използването на данните (Андреева, Йолова 2018: 259). Barca (2017 : 43) подчертава, че „някои категории данни могат да бъдат по-спорни от други, що се отнася до съображения за поверителност и сигурност на данните“. Т.е. цифровизирането на информацията може да не отчете в достатъчна степен защитата на данните и правото на гражданите на поверителност. Съществува дори и мнението, че технологията сама по себе си не гарантира добро управление на информацията (Barca 2017: 55). В този контекст въпросът за поверителността на данните е крайно належащ за разглеждане.

При изпълнението си програмите за социална защита обработват значителни количества лични данни (име, възраст, пол, адрес, здравословно състояние, биометрични данни като пръстови отпечатъци и много други), събирани от лица, семейства и домакинства и сред които се среща и чувствителна информация, която би следвало да подлежи на специфични условия на обработване. В тази връзка

Европейската комисия дава отговор на въпроса кои лични данни се считат за „чувствителни“[1]:

• лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения;

• членство в професионална организация;

• генетични данни, биометрични данни, обработвани единствено с цел идентификацията Ви като човешко същество;

• данни за здравословното състояние;

• данни за сексуалния живот или сексуалната ориентация на дадено лице.

Липсата на достатъчни предпазни мерки понякога е предпоставка за злоупотреба с такива чувствителни данни (информация за самоличността, адреса, здравето, имущество и банковите сметки на бенефициента на социалните програми) чрез неправомерен достъп от трети страни.

В тази връзка като предпоставки за неправомерен достъп могат да се изведат:

– прекомерно разширяване на обема на събираната, обработваната и съхраняваната информация;

– широко използване на компютърни мрежи и тяхната интеграция в обработката и съхраняването на информацията с лични данни;

– широк брой на потребителите, получили достъп до системата и информационните ресурси;

– използване на база данни, в която са обединени различни информационни фондове.

При по-ниско ниво на сигурност на информационната система тя става уязвима за кибератаки, които целят достъп до лична информация. Такива атаки може да са насочени към отделен компютър, мрежова връзка или цяла мрежова инфраструктура, както и към (или чрез) телекомуникационните мрежи и оператори.

2. Мерки за защита на личните данни

Защитата на данните е важна за спазване на правото на гражданите на неприкосновеност на личния им живот. Правото на неприкосновеност е международно признато право на човека, заложено

[1] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_bg

още през 1948 г. във Всеобщата декларация на правата на човека на ООН, а впоследствие и в различни конвенции на регионално ниво и национални конституции и закони. Неприкосновеността на личния живот може да се представи като право на индивидите да разполагат с лично пространство, свободно от намеса на други хора и организации (Кларк 1999). От своя страна правото на защита на данните гарантира „основното право на неприкосновеност на личния живот чрез регулиране на обработването на лични данни: осигуряване на права на индивида върху техните данни и създаване на системи за отчетност и ясни задължения за тези, които контролират или предприемат обработката на данни “ (Privacy International 2018: 12).

Всяко лице има право на защита на своите лични данни (Oostveen, Irion: 2018). Следователно защитата на данните има важно значение за упражняването на правото на личен живот. Отчитайки това значение, през 2016 г., Международната асоциация за социално осигуряване (ISSA) разработи Насоки за информационни и комуникационни технологии (ISSA 2016), извеждайки на преден план управление при висока информационна сигурност и неприкосновеност на личния живот в институциите за социална сигурност. Насоките подчертават от една страна значението на създаването на адекватна рамка за защита на данните, съобразена с правната и регулаторна среда, а от друга – необходимостта от въвеждане на глобална система за защита на личните данни в съответствие с изискванията, свързани с международния обмен на данни.

В тази връзка може да се посочат и Директива 2002/58/CE за защита на личните данни в електронните комуникации, Директива 2006/24/CE относно запазването на данни за трафика при предоставянето на обществено достъпни електронни съобщителни услуги (2006) и Общият регламент за защита на данните от 2016 г., който влезе в сила на 28 май 2018 г. (Regulation (EU) 2016). Пак през 2018 г. ООН прие Принципи за защита на личните данни и поверителност (UN 2018).

Увеличените кибератаки в кризисното време на пандемията COVID 19 изведоха на преден план необходимостта от стабилна защита, съобразена с очакваното бъдеще на публичните институции в областта на здравеопазването, социалното осигуряване и др. системи. Затова в края на 2020 г. Европейската комисия и върховният представител на Съюза по въпросите на външните работи и политиката

на сигурност представиха нова стратегия на ЕС за киберсигурност. Фокусът на стратегията е върху изграждането на колективни способности за реакция при големи кибератаки и работа с партньори по целия свят, за гарантиране на международната сигурност и стабилност в киберпространството. (European Commission 2021a). А чрез Програмата за цифрова Европа за периода 2021 г. – 2027 г. се планира инвестиция от 1,9 милиарда евро в капацитета за киберсигурност и широкото разполагане на инфраструктури и инструменти за киберсигурност в целия ЕС за публични администрации, предприятия и физически лица (European Commission 2021b).

Според едно глобално проучване, към ноември 2019 г., 13 държави са приели закони за защита на данните/поверителността, други 30 държави и юрисдикции имат предстоящи инициативи за защита на личните данни, притежавани от частни и публични органи (Банисар 2021).

Очевидно, за да се запази доверието на осигурените лица към институцията, са необходими силни практики за защита на данните и ефективно законодателство, което да съдейства за свеждане до минимум на киберриска от страничното наблюдение и използването на данни. Например подобрения в сигурността на използваните данни може да се постигнат и с няколко допълнителни стъпки:

- информиране на обхванатите лица за естеството и целта на събиране на данните;
- създаване на механизъм за обратна връзка при забелязани нарушения;
- постоянни процедури по наблюдение и оценка на риска;
- въвеждане на правила и стандарти за всеки етап от процеса на събиране и използване на данните;
- при необходимост от споделяне на данни – сключване на споразумения с партньора за неразкриване на информация;
- защитено архивиране на данните и специално оторизиране на лице, което да отговаря за процедурите.

Набирането на лични данни изисква съгласие на собствениците им. А при обработката им е необходимо спазването на такива принципи като законност, справедливост и прозрачност. Самите институции също трябва да гарантират, че данните са адекватно защитени и да разработят убедително ценностно предложение, демонстриращо ползата за потребителя. За целта те трябва да са наясно към какви

рискове са уязвими и какво могат да направят, за да се смекчат заплахите и евентуалното въздействие.

Заключение

Дигиталните технологии променят начина на проектиране и прилагане на системите за социална защита. Въвеждат се нови системи за идентификация, информационни системи за управление, информационни системи за социална защита, цифрови плащания и др. Цифровите технологии могат да улеснят и ускорят процесите по предоставяне на социална защита, да намалят някои разходи, да подобрят прозрачността и приобщаването на субектите в системата и като цяло, да повишат нейните ефективност и ефикасност. Но те носят и специфични предизвикателства, сред които високи технологични разходи, сложност (необходимост от различни умения на персонала), възможни компромиси (например намаляване на общата ефективност) и сериозни рискове за поверителността и личните данни. Затова работата с лични данни трябва да се извършва при запазване на поверителността и строга защита.

Поради тази причина всички институции, които обработват лични данни, трябва да разработят и прилагат ясна и бърза политика за защита на данните като част от политиката за сигурност на информацията и политиката за сигурност на национално и международно ниво.

Използвана литература

Aloisi, A., E. Gramano (2019). Workers without workplaces and unions without unity: Non-standard forms of employment, platform work and collective bargaining. // Bulletin of Comparative Labour Relations. Employment Relations in the 21st Century: Challenges for Theory and Research in a Changing World of Work, Chapter: 4. Alphen aan den Rijn, Zuid-Holland: Kluwer Law International.

Banisar, D. (2021). National Comprehensive Data Protection/ Privacy Laws and Bills, (https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416 , 01.10.2021).

Barca, V. (2017). Integrating data and information management for social protection: Social registries and integrated beneficiary registries.

Canberra: Commonwealth of Australia, Department of Foreign Affairs and Trade, (https://socialprotection.org/discover/publications/integrating-data-and-information-management-social-protection-social, 07.09.2021).

CaLP. (2013). Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and E-transfer Programmes. Oxford: Cash Learning Partnership (CaLP) (https://reliefweb.int/sites/reliefweb.int/files/resources/calp-beneficiary-privacy-web.pdf, 27.09.2021).

Clarke, R. Internet privacy concerns confirm the case for intervention. // Communications of the ACM, 1999, Vol. 42, №2, pp. 60 – 67, (http://dx.doi.org/10.1145/293411.293475).

European Commission. (2021a). Cybersecurity Policies, (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies, 15.09.2021).

European Commission. (2021b). The Digital Europe Programme, (https://digital-strategy.ec.europa.eu/en/activities/digital-programme, 15.09.2021).

Handayani, S. et al. (2017). Improving the delivery of social protection through ICT – Case studies in Mongolia, Nepal, and VietNam. ADB Sustainable Development Working Paper 50. Manilla: Asian Development Bank, (https://www.adb.org/sites/default/files/publication/384386/sdwp-50.pdf, 07.09.2021).

ISSA. (2016). ISSA Guidelines on information and communication technology. Geneva: International Social Security Association, (https://ww1.issa.int/guidelines/ict/174551, 29.08.2021).

Oostveen, M, U. Irion (2018). The golden age of personal data: How to regulate an enabling fundamental right? // Personal Data in Competition, Consumer Protection and Intellectual Property Law. Singapore: Springer, pp. 7 – 26, (https://link.springer.com/chapter/10.1007/978-3-662-57646-5_2, 47.09. 2021).

Privacy International (2018). The Keys to Data Protection: A Guide for Policy Engagement on Data Protection, Privacy International, London, (https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf, 19.09.2021).

Regulation (EU) 2916/679 of the European Parliament and the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protect Regulation),

European Commission, 2016, (https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A32016R0679).

Socialprotection.org. (2019). Digital social protection – innovation for effectiveness. The fourth webinar of the USP2030 webinar series, organised by socialprotection.org and in collaboration with the International Policy Centre for Inclusive Growth, (https://socialprotection.org/digital-social-protection-%E2%80%93-innovation-effectiveness, 11.09.2021).

UN. (2018).UN Principles for the Protection of Personal Data and Privacy, (https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf, 22.09.2021).

Андреева, А., Г. Йолова (2018). Тенденции при антидискриминационните политики в сферата на здравното осигуряване в условията на дигиталното общество. Защита срещу дискриминацията: Правна уредба, проблеми и тенденции. // Сборник с доклади от национална научна конференция на ИУ – Варна. Варна : СТЕНО, с. 259.

Йолова, Г. (2016). За социалната роля на осигуряването. Правната наука и бизнесът – заедно за устойчиво развитие на икономиката. Варна: Наука и икономика, с.181.

За контакти: доц. д-р Христина Благойчева
Икономически университет – Варна
e-mail: hrblagoycheva@ue-varna.bg

СЪЩНОСТ НА ПРАВОТО НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

гл. ас. д-р Живка Матеева
Икономически университет – Варна

ESSENCE OF THE RIGHT TO PROTECTION OF PERSONAL DATA

Chief Assist. Prof. Zhivka Mateeva, PhD
University of Economics – Varna

Резюме: В ерата на информационното общество възможностите за възникване на проблеми за защита на личните данни, свързани с опасността и заплахата от неблагоприятни последици за личността, е изключително голяма. Нарушаването на правото на личността във връзка с разкриването на личните й данни е посегателство върху неприкосновеността на личността и личния живот. В настоящия материал се изследва същността на правото на защита на личните данни, което е неразделна част от правото на неприкосновеност. На базата на анализа на правото на защита на личните данни са изведени съществените негови белези, характерни за основните човешки права. На тази основа се очертава ролята на правото на защита на личните данни, намираща приложение в най-разнообразни сфери на съвременния живот.

Ключови думи: *лични данни, защита, неприкосновеност, субект на лични данни*

Abstract: In the age of the information society, the possibilities for problems of personal data protection related to the danger and threat of adverse consequences for the individual are extremely high. Violation of the right of the individual in connection with the disclosure of personal data is an encroachment on privacy. This paper examines the nature of the right to the protection of personal data, which is an integral part of the right to privacy. On the basis of the analysis of the right to protection of personal data, its essential features, characteristic for the basic human rights, are derived. On this basis, the role of the right to personal data protection is outlined, finding application in various spheres of modern life.

Key words: *personal data; protection, inviolability; personal data subject*

DOI: https://doi.org/10.36997/PPDD2021.96

Въведение

Бързото развитие на информационните технологии и дигитализацията на информацията поставят нови предизвикателства пред защитата на личните данни, тъй като предоставят все по-големи възможности за незабавен достъп и разпространение на информация. През последните години защитата на личните данни придобива огромно обществено значение и признание, защото почти няма сфера в съвременния обществен, социален и икономически живот, в която да не се налага да бъдат извършвани действия по обработване на лични данни. Всичко това разкрива съществени проблеми за защитата на данните, свързани с опасността и заплахата от неблагоприятни последици за личността. Много често личните данни на физическите лица са обект на обработване и поддържане в определени масиви от база данни, които могат да се използват във вреда на субектите на данни като се започне от измама, кражба на самоличност и се стигне до продажба на стоки и услуги при т. нар. директен маркетинг (Сулев 2012). По този начин информационните масиви от данни се превръщат във важен инструмент в ръцете на бизнеса по отношение на настоящи потребители и потенциални клиенти. Същевременно с това гражданите все по-често правят личните си данни обществено достъпни, с цел достъп до информационни ресурси или като предпоставка за получаване на определена услуга, без да осъзнават напълно рисковете, свързани с това. Определено всичко това може да породи опасения и заплахи от злоупотреби, което налага правото на защита на данните да се разглежда като едно от основните средства, с които субектите на данни могат да се защитят от неправомерни действия, както от страна на държавните органи и институции, така и от различни частноправни субекти.

Изложение

Целта на правото на защита на личните данни е да се повиши ефективността на прилагане на правото на неприкосновеност на личността и личния живот, както и да се осигури защита, когато правата на личността са застрашени в информационното общество. Основната заплаха на правото на защита на данните се проявява в резултат на неправомерното събиране и използване на личните данни от различни правни субекти (държавни органи, юридически и физически лица), включително използването им с недобросъвестни и престъпни намерения. Чрез защитата на данните се дава възможност на физическите лица да контролират своите данни, както и да се предотврати неправомерното им използване. Тази защита е гаранция за осъществяване на по-общото право на личен живот (Кискинов 2005: 203). В редица държави идеята за неприкосновеност се слива със защитата на данните, която тълкува личния живот като управление на личната информация (Армстронг 2005: 7 – 19). С оглед контекста определенията са изключително разнообразни, което прави личния живот от всички международно гарантирани човешки права по-труден за определяне и обхващане. За разлика от повечето държави, българската Конституция не урежда изрично правото на защита на личните данни. Най-близка до обсъжданата тема е разпоредбата на чл. 32 от Конституцията на Република България (КРБ), която прогласява неприкосновеността на личния живот на гражданите. От една страна, неприкосновеността на личността и личния живот е в основата на човешкото достойнство и други ценности като правото на самоопределение, на свобода на изразяване, на свободно сдружаване и др., а от друга, е признато за основно човешко право,[1] което е **по-широко** от защитата на личните данни. Събирането, обработването и разкриването на лични данни е част от правото на неприкосновеност и намира приложение в най-разнообразни сфери на съвременния живот, между които тайната на лична кореспонденция, защитата на дома и семейството, физическа неприкосновеност и др. Нарушаването на правото на личността във връзка с разкриването на личните й данни е посегателство върху неприкосновеността на личността и личния живот. Както всички други основни права, правото на неприкосновеност и

[1] Чл. 8 от Европейската конвенция за защита правата на човека и основните свободи.

защитата на лични данни по дефиниция носят голяма степен на противопоставяне спрямо други основни човешки права, а също и налагат задължението да се осигури ефективна защита при обработването на данните.

Концепцията за защита на личните данни се простира до най-различни международни актове, които признават значимостта на защитата на правото на неприкосновеност на личността и личния живот като основно човешко право. Такива са: Всеобщата декларация за правата на човека; Хартата за основните права на Европейския съюз; Международният Пакт за граждански и политически права; Европейската конвенция за защита на правата на човека и основните свободи; Конвенция № 108 за защита на лицата при автоматизираната обработка на лични данни от 1981 г.; Директива 95/46/ЕО за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (повече за правната уредба за защита на личните данни вж. Александров 2016). Важно е да се отбележи, че директивата бе приета още в началото на развитието на интернет и информационната среда, поради което нормите й не успяваха да осигурят нужната ефикасност на правото на защита на данните. Поради това се наложи извършването на фундаментална реформа на правната рамка на ЕС за защита на данните. Важна стъпка в развитието на правото на защита на личните данни е приемането през 2016 г. на 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 (ОВ, L119/1 2016). Той е основният законодателен инструмент за защитата на личните данни, който замени Директива 95/46/ЕО и се прилага **пряко** от държавите членки на ЕС от 25 май 2018 г. С него се въвежда сериозно нарастване на правата на субектите относно техните лични данни спрямо действащата преди това правна рамка. Целта му е да гарантира последователно и еднородно прилагане в рамките на Съюза на правилата за защита на основните права и свободи на физическите лица във връзка с обработването на лични данни.

Като част от основното право правото на защита на личните данни се характеризира с формалните белези на основните човешки права. На първо място, по своята същност, правото на защита на данните е **субективно право** на физическото лице, тъй като дава възможност за ползване на определено социално благо, а именно право-

то на неприкосновеност на личността. Това право предоставя на своя носител възможността да изисква определено поведение от страна на администраторите/обработващите на лични данни. В тази връзка защитата на личните данни може да се определи като административно задължение, произтичащо пряко от Регламент (ЕС) 2016/679, на което съответства правото на физическото лице да иска предприемането на определени действия от задължените субекти, т.е. изпълнение на задълженията на администраторите/обработващите на лични данни при обработването на данните на физическите лица. Субектът на данни има право на ефективна защита срещу администратор или обработващ на лични данни, когато счита, че неговите права съгласно законодателството за защита на личните данни са били нарушени в резултат на обработване на данните му. Неспазването на задължението е скрепено с административни санкции.

Следващият белег, който правото на защита на данните разкрива като част от основното право на личността, е неговата **неотменимост**. Тя се изразява в опазване на личните данни, отнасящи се до дадено физическо лице от неговото раждане до неговата смърт. Това означава, че не може да се изгуби правото на защита на данните, тъй като то е свързано със самото човешко съществуване, то е присъщо на всяко човешко същество. Установяването на правата на личността като върховен принцип е и декларирането на тези права като неотменими. Съгласно чл. 57, ал. 1 от КРБ, основните права са неотменими.

Друг белег на правото на защита на данните е неговата **универсалност**. Тя се изразява в това, че правото на защита на данните има всеобщ характер (Стоилов 1999), тъй като се проявява независимо от гражданство, социално положение, етническа принадлежност и др. подобни признаци на човека, следователно то не е привилегия и трябва да се прилага за всеки. В тази връзка субекти на правото на неприкосновеност на личността и личния живот са **само физически лица**, независимо дали имат гражданство и какво е то и независимо на коя територия, в която действа правото на ЕС, пребивават. Те са определени като субекти на данни по чл. 4, т.1 от Регламент (ЕС) 2016/679 и защитата на законодателството в областта на личните данни се отнася само до тях, тъй като целта й е да защитава личността. Затова информацията, свързана с починали лица, не се счита за лични данни, регламентирани от регламента (съображение 27 от Регламент (ЕС) 2016/679). В определени случаи починалите могат да получат до

известна степен косвена защита – например генетичната информация за починалото лице може да се разглежда като свързана с неговите наследници и попада в приложното поле на регламента. Въпреки това регламентът допуска съществуването на национална уредба за обработване на данните на починали лица. В българското законодателство и по-конкретно в разпоредбата на чл. 25е от Закона за защита на личните данни (ЗЗЛД) са предвидени определени изисквания по отношение обработването на данни на починали лица. Съгласно посочената разпоредба администраторът или обработващият лични данни може да обработва лични данни на починали лица **само при наличие на правно основание** за това, както и да предприема подходящи мерки за недопускане на неблагоприятно засягане на правата и свободите на други лица или на обществен интерес. Ако обработването е започнало на основание договор с лицето, след неговата смърт администраторът може да продължи да обработва данните на същото основание, ако правата и задълженията по договора се наследяват. В случай че договорът е сключен с оглед на личността на физическото лице, администраторът може да съхранява данните и след смъртта на лицето, като се позове на законово задължение или на законния си интерес. От което следва, че ако приживе по отношение на лицето е било налице основание за обработване на данните му, то неговата смърт няма да промени факта на съществуване на това право. Единствено може да повлияе върху преценката на администратора доколко е целесъобразно обработването да продължи и в какви срокове да се осъществява съхранението на данните (Тошкова-Николова, Фети 2019: 65 – 66).

Информацията, свързана с юридическите лица, включително наименованието и правната форма на юридическото лице, както и данните за връзка на юридическото лице, **не се покрива** от регламента и предоставената от него защита не се прилага (съображение 14 от Регламент (ЕС) 2016/679).

Правото на защита на личните данни **не е абсолютно право** и може да бъде ограничено, когато определени обществени интереси налагат това. То трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност (съображение 4 от Регламент (ЕС) 2016/679). Намесата в неприкосновеността трябва да става само ако това е предвидено в закон и когато е необходимо за запазване

интересите, свързани с националната сигурност или икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето или морала или на правата и свободите на другите, както и ако съответства на поставената цел, съгласно чл. 8, пар. 2 от Европейската конвенция за защита правата на човека и основните свободи.

Много често, когато се засяга неприкосновеността на личността и личния живот, се посочват най-силните аргументи в полза на прилагането на ограничения спрямо други фундаментални права като например свободата на информацията. Конституцията на Република България поставя свободата на информацията в основата на комуникационните и политически права на гражданите. Съгласно чл. 41, ал. 1, изр. 1 от нея, всеки има право да търси, получава и разпространява информация. Това право е въздигнато като основно човешко право в Европейската конвенция за защита правата на човека и основните свободи.

Основен принцип на информационното общество е, че достъпът до информация е основно човешко право, а информационните и комуникационните технологии създават предпоставки за свободното му упражняване (Денчев 2019: 31). Прозрачността и неприкосновеността на личността и личния живот са основни градивни елементи за гарантиране на демократично общество, които са пряко обвързани с правото на достъп до информация. Като основна ценност на съвременното демократично общество правото на информация не е абсолютно и търпи ограничения. То не може да бъде упражнявано срещу правата и доброто име на другите граждани, както и срещу националната сигурност, обществения ред, народното здраве и морала (чл. 41, ал. 1, изр. 2 от КРБ).

Като съществена прилика може да се посочи, че както правото на неприкосновеност на личността, така и комуникационните права са от голямо значение за развитието на съвременното общество и са въздигнати като основни човешки права. Но характерно е, че защитата на личната неприкосновеност е право на *непубличност* и *интимност*, а свободата на словото, както и спадащите към нея право на обществена информация и свобода на медиите са пък права на *публичност* (Боев и др. 2010: 112). За разлика от правото на достъп до обществена информация, което принадлежи на всеки (физически и юридически лица) и определя задълженията на държавните органи,

защитата на личните данни определя правата само на физическите лица и задълженията на администраторите/обработващите на лични данни. Поначало тези права не са в конфликт, тъй като всяко едно от тях обслужва гражданите, като едновременно осигурява на всеки защита срещу неправомерна намеса в личната му сфера на живот и създава условия за засилен контрол на широката общественост чрез прозрачността в управлението. Но съществуват и случаи, в които защитата на личните данни, правото на достъп до обществена информация и свободата на словото се конкурират, и в тези случаи с упражняването на едното се възпрепятства другото. Така в определени моменти правото ни да изразим мнение и правото ни да бъдем информирани може да бъде ограничено от това на други лица да се защити техният личен и семеен живот, достойнство и чест (Боев и др. 2010: 113).

Заключение

Все по-широкото използване на информационните технологии във всички сфери на социалния и икономическия живот налага осигуряването на защитата на личните данни и възможността за злоупотреби с тях да бъде сведена до минимум. В тази връзка съществена последица от причисляването на правото на защита на личните данни към основните права е получаването на специализиран механизъм за защитата му. Целта на защитата е да предпази физическите лица от намесата в правото им на неприкосновеност и личен живот от неправомерното използване на техните лични данни в социален контекст – от държавни органи и от частноправни субекти. Нормите на защитата на личните данни очертават субективните права на лицата, както и тези, които обезпечават тяхната ефикасна административноправна защита, включително и чрез съдебен контрол. Тези правни норми уреждат защитата не изобщо, а във връзка с конкретното материално субективно право или конкретен законен интерес, а именно защита на личните данни. Същевременно с това трябва да се отбележи, че съществуването на изчерпателна правна уредба не гарантира само по себе си правото на защита на личните данни. Като цяло правилното прилагане на правилата за определянето на глобалните стандарти за защита на личните данни е необходимост както от гледна точка на осигуряването на стабилна регулаторна рамка за справяне с нововъз-

никващи технологии и проблеми на цифровизацията, така и спрямо осигуряването на по-високо ниво на защита на данните на физическите лица във всички области на съвременното общество.

Използвана литература

Александров, А. (2016). Защита на личните данни на работниците и служителите. София: Труд и право.

Aleksandrov, A. (2016). Zashtita na lichnite danni na rabotnitsite i sluzhitelite. Sofia: Trud i pravo.

Армстронг, Дж. (2005). Неприкосновеността: гласът на бизнеса. Защита на личните данни: Политики и практика на новите и бъдещи страни членки на ЕС (7-18). Център за модернизиране на политики. София: Интербулит ООД.

Armstrong, Dzh. (2005). Neprikosnovenostta: glasat na biznesa. Zashtita na lichnite danni: Politiki i praktika na novite i badeshti strani chlenki na ES (7-18). Tsentar za modernizirane na politiki. Sofia: Interbulit OOD.

Боев, Б., Кашъмов, К. Кънев, П. Русинова (2010). Свобода на изразяване. София: Сиби.

Boev, B., Kashamov, K. Kanev, P. Rusinova (2010). Svoboda na izrazyavane. Sofia: Sibi.

Денчев, С. (2019). Информация и сигурност. София: За буквите.

Denchev, S. (2019). Informatsia i sigurnost. Sofia: Za bukvite.

Кискинов, В. (2005). Българско и европейско информационно право. София: Сиела.

Kiskinov, V. (2005). Balgarsko i evropeysko informatsionno pravo. Sofia: Siela.

Стоилов, Я. Универсални ли са човешките права? // Съвременно право, 1999, №5, с. 7 – 20.

Stoilov, Ya. Universalni li sa choveshkite prava? // Savremenno pravo, 1999, №5, s. 7 – 20.

Сулев, Г. Електронен директен маркетинг и спам-регулацията. // Общество и право, 2012, №3, с. 26 – 38.

Sulev, G. (2012). Elektronen direkten marketing i spam-regulatsiyata. //Obshtestvo i pravo, 2012, №3, s. 26 – 38.

Тошкова-Николова, Д., Н. Фети (2019). Защита на личните данни. София: Труд и право.

Toshkova-Nikolova, D., N. Feti (2019). Zashtita na lichnite danni. Sofia: Trud i pravo.

За контакти: гл. ас. д-р Живка Матеева
Икономически университет – Варна
E-mail: jivkamateeva@ue-varna.bg

НОВИТЕ СТАНДАРТНИ ДОГОВОРНИ КЛАУЗИ ЗА ТРАНСФЕР НА ЛИЧНИ ДАННИ МЕЖДУ ДЪРЖАВИ-ЧЛЕНКИ НА ЕС И ДЪРЖАВИ ИЗВЪН ЕС

гл. ас. д-р Диана Димитрова
Икономически университет – Варна

THE NEW STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA BETWEEN EU AND NON-EU COUNTRIES

Chief Assist. Prof. Diana Dimitrova PhD
University of Economics – Varna

Резюме: В доклада е направен анализ на нововъведените с Решение за изпълнение (ЕС) 2021/914 на Комисията от 4 юни 2021 г. стандартни договорни клаузи като гаранция за защита на личните данни при трансфер между европейски държави и държави извън ЕС. Акцент е поставен на новите моменти. На базата на анализа и съпоставката с предходните общи договорни условия са направени обобщения и изводи.

Ключови думи: *трансфер на лични данни, стандартни общи условия, гаранция за защита при предаване на лични данни*

Abstract: In the report the new standard contractual clauses are analyzed, introduced with the Commission Implementing Decision 2021/914, and ensuring appropriate data protection safeguards in case of data transfers from the EU to third countries. Accent is put on the new moments. Based on the analysis and comparison with the previous standard contractual clauses summaries and conclusions are made.

Key words: *transfer of personal data, standard contractual clauses, safeguards in case of data transfer*

DOI: https://doi.org/10.36997/PPDD2021.106

Въведение

Развитието на нашето общество в технологична насока и дигитализацията, с което неминуемо е свързано и събирането и обмен на лични данни както от публични органи, така и от частни дружества, налага строгото регулиране на правилата за трансфер за лични данни. На ниво Европейски съюз с приемането на 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)[1] бяха въведени единни правила за защита на физическите лица във връзка с обработване на личните данни. Тези правила се прилагат за Европейското икономическо пространство (ЕИП), което включва всички държави от ЕС и държави извън ЕС – Исландия, Лихтенщайн и Норвегия. Такава защита следва да бъде осигурена и в случаите, когато лични данни се прехвърлят извън Европейското икономическо пространство. С цел гарантиране преминаването на защитата заедно с данните са предвидени редица специални предпазни мерки като например решение относно адекватно ниво на защита съгласно чл. 45 от регламента или разработване на общи договорни клаузи за трансфер на лични данни съгласно чл. 46, пар. 1, които са *предварително одобрени* от Европейската комисия.[2] При липса на решение на Комисията относно адекватното ниво на защита (чл. 45, пар. 3), съгласно чл. 46, пар. 1 от Регламент (ЕС) 2016/679 администраторът или обработващият лични данни може да предава лични данни на трета държава само ако е предвидил подходящи гаранции и при условие, че са налице приложими права на субектите на данни и ефективни правни средства за защита. Съгласно чл. 28, пар. 7 и чл. 46, пар. 2, буква „в“ от Регламент (ЕС) 2016/679 подходяща гаранция при предване на лични данни на трета държава или международна организация могат да бъдат стандартни клаузи за защита на данните, приети от Комисията в съответствие с процедурата по разглеждане, посочена в чл. 93, пар. 2. Именно такива са приети с Решение за изпълнение (ЕС) 2021/914 на Комисията от 4 юни 2021 г.

---

[1] ОВ, L 119, 2016, с. 1.

[2] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

относно стандартни договорни клаузи за предаването на лични данни на трети държави съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета.[3] Тези модернизирани стандартни договорни клаузи са издадени пет години след приемане на регламента и следва да заменят предходните такива съгласно Директива 95/46 за защита на данните.

Актуалността на темата е безспорна предвид скорошното приемане на новите стандартни договорни клаузи. Именно това провокира интереса на автора като в доклада те са изследвани и съпоставени с предходните такива в Решение на Комисията от 15 юни 2001 г. относно общите договорни клаузи за трансфера на лични данни към трети страни съгласно Директива 95/46/ЕО,[4] Решение на Комисията от 27 декември 2004 г. за изменение на Решение 2001/497/ЕО за въвеждане на алтернативен комплект общи договорни клаузи за прехвърляне на лични данни в трети страни[5] и Решение на Комисията от 5 февруари 2010 г. относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета.[6]

Разработката има за цел анализ на действащите стандартни договорни клаузи като гаранция за защитата на личните данни при трансфер. Акцентирано е върху новите моменти при тази защита. На база на анализа са направени обобщения и изводи.

Използвани са методите на индукция и дедукция, нормативен и сравнителноправен анализ за постигане на целта на разработката и свързаните с нея изследователски задачи. Предвид ограничения обем авторът не претендира за изчерпателност на изследвания въпрос.

Докладът е съобразен с регламентацията в законодателството на Европейския съюз (ЕС) към 30.09.2021 г.

Изложение

Свидетели сме на значителни промени в цифровата икономика, характерни за които са: използването на нови и по-сложни операции

[3] ОВ, L199, 2021, с. 31.
[4] ОВ, L181/19, 2001, с. 70.
[5] ОВ, L385/74, 2004, с. 72.
[6] ОВ, L 39, 2010, с. 5.

по обработване, множество вносители и износители на данни, дълги и сложни вериги на обработване и непрекъснато развиващи се стопански взаимоотношения. Бързото развитие обуславя и необходимостта от модернизиране на стандартните договорни клаузи, за да могат те да отразят адекватно тези реалности и да обхванат допълнителни ситуации на обработване и предаване. Приетите с решение за изпълнение на Комисията (ЕС) 2021/914 стандартни договорни клаузи (СДК) са съобразени както актуалните разпоредби на Регламент (ЕС) 2016/679, така и със Съвместно становище 2/2021 на ЕКЗД и ЕНОЗД във връзка с Решението за изпълнение на Европейската комисия относно общите договорни клаузи за трансфера на лични данни към трети държави по въпросите, посочени в чл. 46, пар. 2, буква „в“ от Регламент (ЕС) 2016/679.

В раздел едно са включени цел и обхват на клаузите, действие, трети страни – бенефициенти, тълкуване, йерархия, описание на предаването (в Приложение ІБ на договора), както и незадължителната клауза за присъединяване на други страни към договора. Подобно на новите и предходните СДК съдържат клауза в полза на трето лице и при тях описанието на предаването е предвидено да бъде направено в Допълнение 1 към договора. За разлика от предходните СДК, където в клауза 1 са дадени определения – лични данни, вносител на данни, износител на данни и т.н., в новите СДК има различен подход – в клауза 4 за тълкуване на използваните термини се препраща към Регламент (ЕС) 2016/679. Разлика има и при мястото на разпоредбата относно изменението на СДК – в предходните то е регулирано в последните договорни условия, в новите това е направено още в клауза 2. В клаузата за изменение на договора във варианта от 2001 г. е предвидено клаузите да не подлежат на изменение, а във варианта от 2010 г. – отново да не бъдат променяни или изменяни, а само при необходимост да бъдат прибавяни клаузи по търговски въпроси, които не им противоречат. Забраната за промяна е възприета и в новия вариант, като изменение се допуска с цел да се избере подходящият(ите) модул(и) или да се добави или актуализира информация в допълнението. И тук страните биха могли да добавят други клаузи или допълнителни гаранции, при условие че те не противоречат, пряко или непряко, на стандартните клаузи или не засягат основни права или свободи на субектите на данни, а също така и да включат стандартните договорни клаузи в по-широк договор. За разлика от предходните

варианти в новите СДК е дадена възможност и за по-гъвкав подход по отношение на броя на страните, които могат да се присъединят към такъв договор. Съгласно незадължителната клауза 7 за присъединяване: „структура, която не е страна по клаузите, може със съгласието на страните да се присъедини към тях по всяко време или като износител на данни, или като вносител на данни, като попълни допълнението и подпише приложение I.A.“ Това дава възможност за присъединяване на повече страни към СДК от момента на подписване на документите, като не се пораждат права или задължения за присъединяващата се структура за периода преди тя да стане страна.

В раздел II „Задължения на страните“ – новите стандартни договорни клаузи са предвидили нов модел, в който са съчетани, от една страна, общи клаузи, а от друга – модулен подход със създадени отделни модули за различни сценарии на трансфер на данни:

• Модул 1 – предаване на данни от администратор на администратор.

• Модул 2 – предаване на данни от администратор на обработващ лични данни.

• Модул 3 – предаване на данни от обработващ лични данни на обработващ лични данни.

• Модул 4 – предаване на данни от обработващ лични данни на администратор.

Направен е опит да бъдат обхванати различните възможности на предаване, като се отчита сложността на съвременните вериги на обработване. В зависимост от вариантите на предаване администраторите и обработващите лични данни следва да избират към общите клаузи приложимия модул, като по този начин задълженията им по СДК биват съобразени с тяхната роля и отговорности в този процес. Някои от клаузите са еднакви за всички модули – например клауза 14 „Местно законодателство и практики, засягащи спазването на клаузите“. При други се наблюдава групиране – например в клауза 12 „Отговорност“ – модулите са групирани в две групи: в едната – модул 1 и 4, в другата – модул 2 и 3, а при трети са предвидени отделни разпоредби за всеки модул – например клауза 8 „Гаранция за защита на личните данни“. За разлика от това ново решение в предходните варианти на СДК няма диференциране в модули, в зависимост от вида на предаването на данните, клаузите са еднакви за всички варианти.

В клауза 9 е регулацията за използване на подизпълнители, като има отделен набор за модул 2 и модул 3. И за двата модула се предвиждат по 2 варианта – със специфично писмено разрешение или с общо писмено разрешение. В първия случай вносителят на данни не предава за подизпълнение на дейностите си по обработване без специфичното предварително писмено разрешение на износителя на данни, а във втория вносителят на данни има общото разрешение на износителя на данни да включва обработващ(и) лични данни подизпълнител(и) от съгласуван списък. За разлика в предходните СДК от 2001 г. липсва разпоредба за подизпълнител, а от 2010 г. е предвидена само възможността за предаване за подизпълнение с предварително писмено съгласие.

В клауза 10 „Права на субектите на данни“ в различните 4 модули е регулирано процедирането при обработка на искане от субекта на данните, а в клауза 11 „Правни средства за защита“ – задължение за предоставяне на информацията за обработване на жалби за модули 1 – 3. Правната защита на субектите на данни следва да бъде улеснена, като в СДК се предвижда вносителят да уведомява субектите на данни за координати за връзка с точка за контакт, както и своевременното обработване на всички искания и жалби. Клауза 11, както и клауза 13 „Надзор“ не включват модул 4, а при клауза 12 „Отговорност“ са предвидени регулации за двете отделни групи – на модул 1 и 4 и на модул 2 и 3. За гарантиране на ефективен надзор вносителят на данни следва да приеме юрисдикцията и да си сътрудничи с компетентния надзорен орган и съдилищата и да се ангажира да спазва всяко задължително решение съгласно приложимото право на държавата членка. По-специално вносителят на данни следва да приеме да отговаря на запитвания, да бъде подлаган на одити и да спазва мерките, приети от надзорния орган, включително коригиращите и компенсаторните мерки.

В следващия раздел III – „Местно законодателство и задължения в случай на достъп на публични органи“ – отново са посочени модулите, но разпоредбите на клауза 14 „Местно законодателство и практики, засягащи спазването на клаузите“, както и клауза 15 „Задължения на вносителя на данни в случай на достъп от страна на публични органи“ важат за всички модули. Този раздел следва да предвиди гаранции за спазване на клаузите при правнообвързващи искания от публични органи в тази държава за разкриване на предадените

лични данни с оглед на съдебната практика на Съда на Европейския съюз.[7] Съгласно клауза 15.2 „вносителят на данни приема да провери законосъобразността на искането за разкриване, по-специално дали то продължава да е в правомощията, предоставени на отправилия го публичен орган, както и да оспори искането, ако след внимателна преценка стигне до заключението, че има разумни основания да се смята, че искането е незаконосъобразно съгласно законодателството на държавата на получаване, приложимите задължения съгласно международното право и принципите на международната вежливост. Вносителят на данни следва при същите условия да търси възможности за обжалване."

Раздел IV „Заключителни разпоредби" включва клауза 16 „Неспазване на клаузите и прекратяване" и клауза 17 „Приложимо право". В първата са предвидени възможностите за прекратяване, както и задължения за уведомяване от страна на вносителя при невъзможност да спазва клаузите – общо, без разделение по модули. В следващата отново има разделение по модули като за модули 1 – 3 приложимото право е това на страна – членка на ЕС, а за модул 4 следва да бъде посочено правото на държавата (не задължително страна – членка на ЕС).

Разпоредбите от раздели II, III и IV липсват в този обем и подробности в предходните СДК. В тях, в рамките на 11 – 12 значително по-семпло и кратко формулирани клаузи, е направено разделение на задължения на износител и задължения на вносител на данни, както има и клаузи по отношение на отговорност, посредничество и юрисдикция/медиация и съд, сътрудничество с надзорните органи, приложимо право, изменение на договора, предаване за подизпълнение и задължения след приключване на услугите по обработване.

Както беше посочено по-горе, и при предходните, и при новите СДК е предвидено част от информацията да бъде дадена в допълненията/приложенията към договора, а именно – описание на предаването и технически и организационни мерки, във варианта от 2001 г. липсват техническите и организационните мерки, но има задължителни принципи за защита на данните в допълнения 2 и 3. В предходните

[7] EDPB – EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, p. 7, (https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf).

СДК в допълнение 1 е включено описание на дейностите, свързани с предаването от износител и вносител, засегнатите категории физически лица, категориите данни, крайни цели на трансфера (СДК 2001 г.), специални категории данни (СДК 2010 г.)/чувствителни данни (СДК 2001 г.) и операции по преработване (СДК 2010 г.)/ адресати, пред които може да се разгласяват данните и ограничение на съхранението (СДК 2001 г.). В приложение I, за модули 1 – 4 на новите СДК са предвидени три части: „А“ – списък на страните; „Б“ – описание на предаването и „В“ – компетентен надзорен орган. В описанието на предаването освен категориите субекти на лични данни, предавани лични данни и чувствителни лични данни са включени и новите: честота на преработване (еднократно или текущо), естество на обработване, цели и срок, за който ще се съхраняват личните данни, а ако това е невъзможно — критериите, използвани за определяне на този срок. В приложение II „Технически и организационни мерки, включително технически и организационни мерки за осигуряване на сигурността на данните“ за модулите 1 – 3 са разписани изключително подробно примери за възможни мерки, като те трябва да бъдат описани конкретно, а не общо. Има и приложение III за модули 2 и 3 – списък на обработващите лични данни подизпълнители, като то се попълва в случай на специфично разрешение за използване на обработващи лични данни подизпълнители (клауза 9, буква „а“, вариант 1).

При направения сравнителен анализ бе установено, че в новите СДК е предвиден нов модел на съчетаване на модули с общи клаузи. Отделните клаузи са значително по-подробни и детайлни, те обхващат различните видове предаване на лични данни между администратори и обработващи лични данни и създават гаранции, че защитата на личните данни, осигурена на европейско ниво от Регламент (ЕС) 2016/679, преминава заедно с трансфера на данни към трети държави.

Заключение

Приемането на нови стандартни договорни клаузи е обусловено както от динамично променящите се обществени отношения, свързани с дигитализацията, така и от необходимостта те да са в съответствие с изискванията за предоставяне на подходящи гаранции на защитата на личните данни при трансфер съгласно разпоредбите на

Регламент (ЕС) 2016/679. На 4 юни 2021 г. съгласно чл. 46, пар. 2, буква „в“ и в съответствие с процедурата по разглеждане, посочена в чл. 93, пар. 2 от Регламент (ЕС) 2016/679 с Решение за изпълнение (ЕС) 2021/914 на Комисията бяха въведени новите стандартни договорни клаузи осигуряващи подходящата гаранция.

След проведения анализ се налага изводът, че при приемането им са отчетени както промените в обществените отношения във връзка с дигитализацията и промените в нормативната уредба, така и Съвместното становище 2/2021 на ЕКЗД и ЕНОЗД във връзка с Решението за изпълнение на Европейската комисия относно общите договорни клаузи за трансфера на лични данни към трети държави по въпросите, посочени в чл. 46, пар. 2, буква „в“ от Регламент (ЕС) 2016/679. Въведени са редица нови моменти като нов модел на съчетаване на модули с общи договорни клаузи, възможност и други страни да се присъединяват към договорните клаузи, възможност за използване на СДК при трансфер на лични данни към подизпълнител, улеснена правната защита на субектите на данни, гаранции за спазване на клаузите при правнообвързващи искания от публични органи, по-подробно и детайлно описание на предаването и на техническите и организационни мерки в приложенията. В Съвместно становище на ЕКЗД и Европейския надзорен орган по защита на данните (ЕНОЗД) относно СДК за трансфер на данни към трети страни се поставя въпрос във връзка с въведените модули за различни сценарии на трансфер – дали е възможно в едни СДК да се съдържат няколко модула в зависимост от ситуациите или за всяка ситуация и модул следва да сключат отделни договори. Предложението към Комисията е да се обърне внимание на това в рубрика „Въпроси и отговори“ и да се изясни, че комбинирането на различни модули в едни СДК не може да води до размиване на отговорността.[8] При приложението на СДК на практика ще възникнат и редица други въпроси и то ще покаже доколко ефективна гаранция и защита предлагат те. Предвид факта, че нуждите на заинтересованите страни могат да се променят, а технологиите и операциите по обработване се променят бързо в условията на дигитализация, Комисията следва да оценява действието

[8] EDPB-EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, p. 9, (https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf).

на стандартните договорни клаузи в светлината на натрупания опит като част от периодичната оценка на Регламент (ЕС) 2016/679, предвидена в член 97.

Използвана литература

EDPB – EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, (https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf, 30.09.2021).

ОВ, L 119, 2016, с. 1.

ОВ, L199, 2021, с. 31.

ОВ, L181/19, 2001, с. 70.

ОВ, L385/74, 2004, с. 72.

ОВ, L 39, 2010, с. 5

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

За контакти: гл. ас. д-р Диана Димитрова
Икономически университет – Варна
dianadim@ue-varna/bg

ЛИЧНИТЕ ДАННИ В КОНТЕКСТА НА ТРУДОВИТЕ ОТНОШЕНИЯ

гл. ас. д-р Павлина Иванова
Икономически университет – Варна

PERSONAL DATA IN THE CONTEXT OF EMPLOYMENT RELATIONS

Chief assist. Pavlina Ivanova, PhD
University of Economics – Varna, Bulgaria

Резюме: За целите на трудовото правоотношение по силата на законодателството работодателите събират, обработват и съхраняват определен обем лични данни на кандидатите за работа – работници и служители. Това поражда за тях съответни задължения и отговорности в качеството им на администратори на лични данни. В доклада са разгледани основанията за събиране и обработване на лични данни за целите на трудово правоотношение и са посочени необходимите мерки, гарантиращи поверителността на личните данни на персонала.

***Ключови думи**: трудови отношения, лични данни, съгласие, работодател, работник*

Abstract: For the purposes of the employment relationship under the law, employers collect, process and store a certain amount of personal data of job candidates and employees. This creates for them respective obligations and responsibilities in their capacity as controllers of personal data. The report examines the grounds for the collection and processing of personal data for the purposes of employment and sets out the necessary measures to ensure the confidentiality of personal data of staff.

***Key words:** employment relations, personal data, consent, employer, worker*

DOI: https://doi.org/10.36997/PPDD2021.116

Въведение

При предоставянето на работна сила отношенията между работодател и работник се уреждат като трудови правоотношения. Именно като вид обществено отношение трудовото правоотношение изразява връзката между хората по повод използването и въздействието на работната сила. Трудовото правоотношение „се характеризира със своя обект, страни, съдържание, както и с юридическите факти, основание за неговото възникване, изменение и прекратяване“ (Андреева, Йолова 2020). Основният нормативен акт, регламентиращ трудовите правоотношения в България, е Кодексът на труда (КТ), приет през 1986 г.

Трудовото правоотношение възниква при сключване на трудов договор, който регламентира съвкупността от права и задължения на страните, т.е. на работника или служителя и работодателя (Мръчков и др. 2009). Той има конкретно съдържание, включващо определени от закона данни за страните, определени в пар. 1, т. 10 от Допълнителните разпоредби на Кодекса на труда:

• за работодател – юридическо лице или едноличен търговец – наименование, седалище и адрес на управление на юридическото лице или едноличния търговец, ЕИК, имена на представляващия, единния граждански номер (личния номер – за чужденец); за работодател – физическо лице – името на лицето, постоянния адрес, единния граждански номер (личния номер – за чужденец);

• за работник или служител – името на лицето, постоянния адрес, единния граждански номер (личния номер – за чужденец), вида и степента на притежаваното образование, както и данни за притежаваната научна степен, ако е свързана с изпълняваната от него работа.

По своята същност този тип данни представляват лични данни. Такива работодателите събират, съхраняват и обработват още преди възникването на трудовото отношение, по време на неговото времетраене и след неговото прекратяване. В трудовото законодателство се съдържат относително ограничен брой разпоредби, определящи отговорността и границите на контрол на работодателя при администрирането, съхраняването и трансфера на лични данни на работещите. Нормативните актове, определящи изискванията към работодателите по отношение на събираните и съхранявани лични данни при и по повод на трудовите отношения, са Общият регламент относно

защита на личните данни (Регламент (ЕС) 2016/679), (ОРЗЛД) и Законът за защита на личните данни (ЗЗЛД).

Съгласно посочените актове лични данни са тези, които позволяват с тяхна помощ едно лице да бъде идентифицирано – лични данни могат да са името и фамилията, датата на раждане, адрес, номер на банкова сметка, информация относно образование и работен опит, телефонен номер, електронна поща, видео запис и т.н.

Националният надзорен орган по защита на личните данни е Комисията по защита на личните данни (КЗЛД). При изпълнение на своята контролна функция КЗЛД подпомага засегнатите лица, като събира служебно доказателства и възлага извършването на проверки (Матеева 2020).

В този контекст в настоящия доклад се разглеждат основанията за събиране и обработване лични данни за целите на трудово правоотношение, като се посочват и необходимите мерки, гарантиращи поверителността на личните данни на персонала.

Изложение

Работодателите, в качеството си на администратори на лични данни,[1] събират, обработват и съхраняват определен обем лични данни за целите на трудовото правоотношение по силата на Кодекса на труда, Кодекса за социалното осигуряване, Закона за счетоводството, както и други нормативни актове. Това определя законосъобразността на действията им, които в зависимост от хипотезата са законово задължение и/или са в съответствие с изпълнението на договор – „Обработването на лични данни от администратори както в публичната, така и в частната сфера е законосъобразно, ако е налице някое от следните алтернативни и равнопоставени основания: съгласие; изпълнение на договор; законово задължение; жизненоважни интереси; обществен интерес/официални правомощия; легитимни интереси“ (ttps://www.cpdp.bg).

[1] Администратор на лични данни – всяка организация, която определя целта и средствата за обработване на лични данни, извършва такова обработване и е отговорна за обработването или субект, който е задължен да извърши обработване на лични данни по закон.

Личните данни в процеса по набор и подбор на персонал

Събирането и обработването на лични данни от страна работодателите започва още в процеса по набиране и подбор на персонал. Кандидатите за работа, независимо от начина, по който адресират своята кандидатура, сами разкриват лични данни пред различните компании или институции. Представяните от тях данни са в съдържание и обем, определени от работодателя при обявяване на свободната работна позиция или обявяването на конкурс за съответната длъжност. Изхождайки от разпоредбите на ЗЗЛД и ОРЗЛД, потенциалният работодател следва да изисква само такива данни, които са съотносими към процеса на подбор, т.е. те да са важни и съществени по отношение вземането на решение за наемане на дадения кандидат.

Обичайно кандидатстването за работа изисква представянето на автобиография, съдържаща идентификационни данни (име, фамилия, дата на раждане), данни за контакт (адрес по местоживеене, телефонен номер, електронна поща), както и информация за образование, умения, професионален опит. Кандидатите сами решават каква точно информация да разкрият в автобиографията си, включително и дали да предоставят снимка (изискване за предоставяне на снимка не е изрично регламентирано в нормативен акт). В рамките на етапа по кандидатстване за дадена позиция няма и основание да се изисква банкова информация, както и копие от документ за самоличност.

Понякога компаниите включват към набора от документи за кандидатстване съгласие[2] за обработване на личните данни за целите на подбора. Това е възможно, но не е изрично необходимо, когато се кандидатства по конкретна обява и данните се предоставят директно на потенциалния работодател (Защита на неприкосновеността на работното място. Наръчник за служители, (https://www.cpdp.bg/). Кога обаче това все пак е необходимо? Наличието на съгласие от страна на кандидатите за работа е необходимо, когато работодателят предложи и кандидатът приеме автобиографията и останалият набор от документи да бъдат използвани при бъдещ подбор на персонал. Някои организации на базата на даденото съгласие включват личните данни на кандидатите, които не са назначени в своята база данни от потен-

[2] Съгласие – свободно, конкретно и информирано изразяване на волята на субекта на данни, което съдържа разрешение за обработване на лични данни, които се отнасят до него.

циални работници.

Част от процеса по подбор може да включва и провеждането на интервю. По време на интервюто работодателят, с цел да изясни конкретни обстоятелства от автобиографията на кандидата за работа, може да задава въпроси, които са свързани само със съответната работна позиция. Лицата имат право да не отговарят на въпроси, които ги смущават – например, отнасящи се до религиозни убеждения, политически възгледи, частен живот, семеен статус, сексуална ориентация, планове за създаване на семейство. Когато обаче има законово основание за това, работодателят има право да задава въпроси, касаещи чувствителни данни – например за съдебното минало на лицето, ако това е съотносимо към длъжността, или за здравословно състояние, ако има медицинска забрана за заемане на длъжността от лица с определени заболявания или конкретно състояние.

Работодателите биха могли да се сдобият и с допълнителна информация за търсещите работа от социалните мрежи, постовете им в интернет форуми, и това да повлияе решението им за наемане. Какво обаче е видно за лицата в интернет пространството и профилите им в социалните мрежи е тяхно лично решение. Ако те са позволили споделената от тях информация, снимки и преживявания да са публични, това създава предпоставка те да бъдат използвани за различни цели, т.е. онлайн неприкосновеността е отговорност на самите лица.

С промените в Закона за защита на личните данни от 2019 г. се регламентира срокът за съхранение на данните на кандидатите за работа. Разпоредбата е работодателят или органът по назначаването, в качеството си на администратор на лични данни, да определи срок за съхранение на личните данни. Този срок не може да е по-дълъг от 6 месеца, освен ако кандидатът не е дал съгласието си за съхранение за по-дълъг срок. След изтичането му работодателят трябва да изтрие или унищожи съхраняваните документи с лични данни, освен ако специален закон не предвижда друго. Той няма право да използва данните, съдържащи се в автобиографиите на лицата, за други цели. Друго изискване е, когато работодателят е поискал да се представят оригинали или нотариално заверени копия на документи, които удостоверяват физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, той да върне тези документи на кандидата, който не е одобрен за назначава-

не, в 6-месечен срок от окончателното приключване на процедурата, освен ако специален закон не предвижда друго.

Личните данни при назначаване и по време на трудовото правоотношение и след неговото прекратяване

С избраните в процеса на подбор кандидати се сключва трудов договор, което от своя страна инициира създаването на личното трудово досие. То съдържа документите, необходими за сключването на трудовия договор, една част от които са предоставени от лицата и други, подготвени от работодателя. Документите могат да бъдат класифицирани като задължителни – изискващи се съгласно Кодекса на труда и Наредба № 4 за документите, които са необходими за сключване на трудов договор и допълнителни. Повечето от тях съдържат лични данни за работещия, а някой от тях – и данни за трети лица (деца, съпруг, съпруга). Когато в рамките на трудовото правоотношение се налага събирането и обработването на специални категории (чувствителни) лични данни – религиозни убеждения, синдикално членство, биометрични данни, данни за здравословното състояние, сексуална ориентация и др., се съблюдават разпоредбите на чл. 9, пар. 2 от ОРЗЛД. Независимо че говорим за трудово досие, в него може да се съдържат освен данни за трудовото правоотношение и данни от личния живот на работника или служителя. Те се предоставят лично от него при настъпване на определени обстоятелства в неговия личен живот. Целта е работникът да се възползва от своите права, а работодателят – да изпълни своите административни задължения. Пример в това отношение са отпуските за бременност и раждане, за отглеждане на дете и отпуските за изпълнение на граждански, обществени и други задължения (встъпване в брак, кръводаряване, смърт на близък роднина).

В контекста на трудовите правоотношения работодателят е длъжен да не разкрива личните данни на работника или служителя на трети лица. Достъп до личните данни на персонала могат да имат служителите, които изрично са упълномощени да ги обработват. Те могат да бъдат разкривани на външни субекти, само когато за това има нормативно основание – например при проверка от Инспекцията по труда. Данните се предоставят и пред компетентните органи във връзка със социалното и здравно осигуряване, както и във всеки друг случай, предвиден в националното законодателство (чл. 6, (41), (45)

от Регламент (ЕС) 2016/679).

Тъй като основен принцип при защита на личните данни е те да бъдат съхранявани докато това е необходимо, важно за работодателите е да определят тези срокове според нормативните изисквания и спецификата на своята дейност. Една част от трудовото досие на работника, касаеща трудов и осигурителен стаж, следва да се съхранява за периода на съхранение на разчетно-платежните ведомости (50 години), друга част от документите е достатъчно да бъдат съхранявани до изтичане на определения в Кодекса на труда давностен срок за предявяване на искове по трудови спорове.

Личните данни на персонала могат да бъдат обработвани и след прекратяване на трудовото правоотношение. Правните основания за това са значително по-малко, обикновено са във връзка с целите на пенсионното и здравното осигуряване, данъчни и архивни цели, както и в случаите на възникнал трудов спор пред съда.

Мерки, гарантиращи поверителността на личните данни на работещите

Тъй като националното трудово законодателство не съдържа специфични разпоредби, необходимо е процесът по защита на данните и свързаният с това контрол да бъдат организирани от всеки работодател чрез разработване на вътрешни документи (Матеева 2018). Те трябва да отговарят на изискванията и принципите на ОРЗЛД и произтичащите от него конкретни задължения за администраторите на лични данни и в частност на работодателите. Обобщени конкретните мерки, които работодателите следва да предприемат са представени в таблица 1.

Таблица 1

Мерки, гарантиращи поверителността на личните данни на персонала

Изграждане на ясна система за обработка на личните данни
Създаване на вътрешни за организацията нормативни документи, които да регламентират обработката и съхранението на данните
Периодично ревизиране на въведената система
Използване на надеждни технологии с подходящи нива на защита на личните данни

Осигуряване на адекватни технически и организационни мерки за защита на личните данни, обработвани в рамките на трудовото правоотношение
Разработване на прозрачни фирмени политики за защита на личните данни
Ясна информация за събирането на лични данни
Уточняване на целите за обработка на лични данни
Дефиниране на правилата за запазване и изтриване на лични данни
Използване на подходяща защита за съхранението на личните данни
Уведомяване на властите за нарушения във връзка с лични данни
Получаване на подходящо съгласие за обработка на данни
Съхраняване на записи с подробна обработка на данните
Обучения на служители, които обработват лични данни
Одит и актуализиране на политиките за лични данни
Назначаване на DPO – Длъжностно лице по личните данни[3] (ако е необходимо)

В конкретика подходящите технически и организационни мерки за осигуряване на сигурност на данните се изразяват във:

- псевдонимизация на данните;
- криптиране на данните;
- осигуряване на постоянна поверителност на системите за обработване;
- в случай на физически или технически инцидент – своевременно възстановяване на наличността и достъпа до личните данните;
- провеждане на редовни изпитания на техническите и организационните мерки;
- сътрудничество с надзорния орган за защита на личните данни.

[3] Длъжностно лице по личните данни – служител на администратор на лични данни или външно за организацията на администратора физическо лице, натоварено с консултативни функции в областта на защитата на личните данни, надзор по спазването на регламента в организацията на администратора и повишаването на осведомеността и обучението на персонала.

Заключение

В контекста на изложеното може да се обобщи, че:

• Събирането, обработването и съхранението на лични данни за целите на трудовото правоотношение е в съответствие със законово задължение на работодателите или е във връзка с изпълнението колективния и/или индивидуалния трудов договор.

• Изрично съгласие от страна на кандидатите за работа, работниците и служителите се изисква само при определени обстоятелства.

• Субектът на данните (физическото лице, за което се отнасят данните) има право на информираност, достъп до собствените си лични данни, коригиране (ако данните са неточни), право на защита по съдебен или административен ред, в случай че правата му по отношение на личните данни са били нарушени.

• Работодателят може да съхранява лични данни на персонала за период, определен от съответните нормативни актове. След изтичане на този срок, данните следва да бъдат унищожени. Това поражда правото на кандидатите за работа и работещите „да бъдат забравени".

• Техническите и организационни мерки за защита на данните, които работодателите прилагат трябва да са адекватни на рисковете и на категориите данни.

Основният инструмент за доказване и удостоверяване на законосъобразното, добросъвестно, прозрачно и с подходящо ниво на сигурност и защита обработване на лични данни е отчетността, която е въведена като задължение на администраторите с ОРЗЛД. В Република България контролът по спазването на изискванията във връзка със защитата на личните данни се осъществява от Комисията за защита на личните данни, която има право да се произнася по жалби на физически лица, да проверява администратори и обработващи лични данни, да издава становища, задължителни предписания и да налага санкции.

Използвана литература

Андреева, А. Г. Йолова (2020). Трудово и осигурително право. Варна: Наука и икономика.

Защита на неприкосновеността на работното място. Наръчник

за служители, (https://www.cpdp.bg, 30.09.2020).

Мръчков, В., К. Средкова, А. Василев (2009). Коментар на кодекса на труда. София: Сиби.

Общ регламент относно защита на личните данни (Регламент (ЕС) 2016/679), (https://www.cpdp.bg, 30.09.2020).

Andreeva, A., Z. Mateeva (2018). Employers as Personal Data Administrators – Specifics and Requirements in the Context of the Information Society. Globalization, the State and the Individual. Varna: VFU Chernorizets Hrabar.

Mateeva, Z. (2020). Protection of Persons of Personal Data Before the National Supervisory Authority. Burgas: Miracle A Ltd.

За контакти: гл.ас. д-р Павлина Иванова
Икономически университет – Варна
e-mail: p.ivanova@ue-varna.bg

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В КОНТРОЛНИТЕ ПРОИЗВОДСТВА НА ИЗПЪЛНИТЕЛНАТА ВЛАСТ

гл. ас. д-р Пламена Недялкова
Икономически Университет – Варна

PROTECTION OF PERSONAL DATA IN CONTROL PROCEEDINGS OF THE EXECUTIVE BRANCH

Chief Assistant Dr. Plamena Nedyalkova
University of Economics – Varna

Резюме: По време на контролните производства, които се осъществяват от различни контролни институции в изпълнителната власт е от съществено значение запазване на личните данни на проверяваните физически и юридически лица. Основният обхват на този доклад е да се представят една значителна част от проблемите, които се проявяват в сложните контролни производства, при които съвместно участват няколко контролни институции. При тези сложни контролни производства често се налага предаване на информация от една контролна институция към друга контролна институция, което съответно поражда и проблемите относно съхраняване и защита на личните данни на проверяваните обекти.

Ключови думи: *контрол, изпълнителна власт, лични данни*

Abstract: During the control proceedings, which are carried out by various control institutions in the executive branch, it is essential to preserve the personal data of the inspected individuals and legal entities. The main scope of this report is to present a significant part of the problems that arise in complex control proceedings involving several control institutions. These complex control procedures often require the transfer of information from one control institution to another control institution, which accordingly raises problems regarding the storage and protection of personal data of the inspected objects.

Key words: *control, executive power, personal data*

DOI: https://doi.org/10.36997/PPDD2021.126

Изложение

Дигитализацията, която е предпоставка за приноса на входни данни, разработването и внедряването на нови преносими устройства, чрез които да се обработват първичните и вторичните данни, са все фактори, които оказват влияние върху трансфера на информация и в частност върху възможността тези данни бързо и лесно да попадат в лица, институции и организации с цел недобронамерено използване и неправомерно предоставяне на трети лица. Свидетели сме как през последните години този проблем започва да оказва влияние не само върху конкретните индивиди и лица, които са съставните единици на общността, но така също този проблем започна да въздейства и върху структурно- организационното развитие на всяка една организация. Проблематиката е много обхватна и в рамките на един доклад, не може да бъдат изследвани всички проблеми относно защитата на личните данни. Целта на настоящия доклад е да се изследва и анализира само един основен проблем, а именно проблемът за защитата на личните данни в контролните производства на изпълнителната власт. За осъществяване на така поставената цел, следва да се постигнат следните задачи:

1. Да се представи проблемът, засягащ политиките за сътрудничество между контролните институции относно постигането на пълна защита на личните данни на проверяваните обекти.

2. Да се представи оценка на въздействието върху защитата на данните на контролните обекти.

1.1. Специфики на политиките за сътрудничество между контролните институции относно постигането на пълна защита на личните данни на проверяваните обекти

В чл. 4 от Регламент (ЕС) 2016/679 е представена следната дефиниция за понятието „лични данни“, а именно „всяка информация, свързана с идентифицирано физическо лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на

това физическо лице“,[1] т.е. лични данни е всяка информация с която дадено лице може да се идентифицира от всички останали лица.

Общото между контролните производства на основните контролни институции от изпълнителната власт (Национална агенция за приходите, Агенция за държавна финансова инспекция, Комисия за финансов надзор и др.) е, че преминават през следните основни етапи:

1. Планиране и започване на контролното производство.

2. Осъществяване на контролното производство, чрез съответните контролни процедури и реализиране на цялостния контролен процес.

3. Съставяне на съответните контролни документи, удостоверяващи извършения контрол.

4. Преглед на правните и икономическите последици от осъществения контролен процес.

По време на всеки един етап контролните лице събират, обработват и анализират всякаква разнородна информация за проверявания обект, в т.ч. съответно се налага и обработване на лични данни. От гледна точка на Национална агенция за приходите „основната цел, за която се извършва обработване на лични данни на физически лица, е идентифицирането им по безспорен начин, във връзка с осъществяването на законоустановени функции на НАП – обслужване на лицата, установяване на данъци и задължителни осигурителни вноски, обезпечаване и събиране на публични вземания, в това число и установяване на имущественото и финансово състояние на задължените лица, установяване на административни нарушения и налагане на административни наказания, надлежно информиране на клиентите на НАП, както и други правомощия, предвидени в нормативната уредба“.[2]

Национална агенция за приходите (НАП), като водеща контролна институция в изпълнителната власт, си сътрудничи с останалите

---

[1] 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), (https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32016R0679&from=HU).

[2] Защита на личните данни. Национална агенция за приходите стриктно спазва основните принципи, въведени като задължителни при обработването на лични данни, (https://nra.bg/wps/portal/nra/za-nap/Zashtita-na-lichnite-danni).

контролни институции в изпълнителната власт, като това сътрудничество е с различно предназначение и зависи от целта на съответното контролно производство. В зависимост от това предоставянето на информация от НАП към останалите контролни институции е с различно съдържание, форма и се отнася до различни проверявани обекти (физически и юридически лица). Например при контролните производства, които са насочени към установяване на укриване на осигурителни вноски, информацията, която се предоставя от НАП към НОИ, съдържа лични данни на проверяваните обекти, тъй като следва да се установи дали са декларирани и изплатени съответните данъчно-осигурителни вноски на данъчно задължените лица. По същия начин стои и въпросът, когато се извършват контролни производства, които са насочени към идентифициране на престъпни схеми на данъчни измами. Обикновено тези контролни производства са съвместни с НАП, НОИ, Главната инспекция по труда, Министерството на труда и социалната политика и е възможно участие на контролни институции от изпълнителната власт към Министерството на вътрешните работи (Икономическа полиция, ДАНС и др.). В тези случаи проверките се осъществяват по икономически сектори, като се разглеждат приоритетно секторите, които са с най-голям риск.

През последните години, поради развитието на технологиите, между институциите по време на контролните производства се осъществява електронен обмен на информация, в т.ч. и лични данни. Този електронен обмен на информация цели да се оптимизират сроковете на производството, но това съответно е предпоставка за изтичане на лични данни от съответните контролни институции.

През 2019 г. НАП сключи споразумение за предоставяне на информация с Висшия съдебен съвет (ВСС) „за взаимодействие във връзка с осигуряването на достъп на органите на съдебната власт до електронни услуги на НАП, въз основа на което е предоставен достъп на служители от 179 съдилища“.[3] Също така през 2019 г. НАП сключи още „три нови двустранни споразумения за достъп до елек-

[3] Годишен отчет за дейността на Националната агенция за приходите за 2019, официално е публикуван отчета 2020 г., (https://nra.bg/wps/wcm/connect/nra.bg25863/4d5b4a64-3f1a-49a5-8cbd-b4cabf77bacd/Годишен_отчет_НАП2019.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE.Z18_PPGAHG8009LJC0QTR5C2HH30I6-4d5b4a64-3f1a-49a5-8cbd-b4cabf77bacd-nDZA1Dw).

тронни услуги с Агенцията по заетостта, Агенцията по вписванията и Министерството на земеделието, храните и горите. Въз основа на споразуменията лицата, притежаващи ПИК, издаден от НАП, могат да го използват като идентификатор за достъп до електронните услуги на други държавни и общински администрации“.[4] Въз основа на посочените споразумения още през 2019 г. са подадени заявления за предоставяне на достъп от 135 ведомства и държавни агенции до регистъра на НАП на задължените лица със „Справка за наличие или липса на задължения“ и от 132 ведомства и държавни агенции до Регистъра на уведомленията за сключване, изменение или прекратяване на трудовите договори и уведомления за промяна на работодател със „Справка за сключване, изменение или прекратяване на трудовите договори и уведомления за промяна на работодател“.[5]

Подготовката за електронния обмен на данни между институциите започна още през 2015 г., като през 2017 г. със свое решение № 357 от 29 юни 2017 г. Министерският съвет задължи всички административни органи в срок до 1 септември 2017 г. да приведат системите си за електронен обмен на документи с единен технически протокол, утвърден от председателя на Държавната агенция „Електронно управление“. Задължението за всички администрации да обменят документи помежду си единствено по електронен път е в сила от 1 ноември 2018 г. Административните органи трябва да използват само системи за електронен документооборот, които изпълняват този протокол.

Въпреки посочените споразумения и вътрешно утвърдени процедури за електронен обмен на данни между институциите, все пак ставаме свидетели за т.нар. изтичане на данни, като последният случай беше през 2019 г., когато хакери бяха се „сдобили с информация

---

[4] Годишен отчет за дейността на Националната агенция за приходите за 2019, официално е публикуван отчета 2020 г., (https://nra.bg/wps/wcm/connect/nra.bg25863/4d5b4a64-3f1a-49a5-8cbd-b4cabf77bacd/Годишен_отчет_НАП2019.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE.Z18_PPGAHG8009LJC0QTR5C2HH30I6-4d5b4a64-3f1a-49a5-8cbd-b4cabf77bacd-nDZA1Dw).

[5] Годишен отчет за дейността на Националната агенция за приходите за 2019, официално е публикуван и отчетът за 2020 г. (https://nra.bg/wps/wcm/connect/nra.bg25863/4d5b4a64-3f1a-49a5-8cbd-b4cabf77bacd/Годишен_отчет_НАП2019.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE.Z18_PPGAHG8009LJC0QTR5C2HH30I6-4d5b4a64-3f1a-49a5-8cbd-b4cabf77bacd-nDZA1Dw).

от един от сървърите на Министерството на финансите, в частност сървъра на Националната агенция за приходите“.[6] Скоро след този случай Комисията за защита на личните данни издаде наказателно постановление срещу НАП, с което се наложи имуществена санкция на институцията.

Разработените вътрешни контролни системи за защита на личните данни във всяка една от институциите, които осъществяват контролни дейности в изпълнителната власт (НАП, НОИ, ГИТ и др.), от една страна, са насочени към ефективното прилагане на регламента, а от друга страна – към установяване и осъществяване на задълженията на съответните администратори и лицата обработващи лични данни. Тези контролни системи са утвърдени чрез съответните процедури, кодекси, указания и др. и с тяхна помощ следва да се установява и оценява рискът, който е вероятно да произтече от обработването на данни.

1.2. Оценка на въздействието върху защитата на данните на контролните обекти

Всяка контролна институция в изпълнителната власт следва да извършва системно оценка на въздействието върху защитата на личните данни на контролираните обекти. Тази оценка е задължително да се извежда и да се установява, когато има вероятност при обработването или при електронния обмен на данните между институциите да настъпи висок риск, нарушаващ правата и свободите на гражданите. Съгласно изискванията на Регламент 2016/ 679 в една оценка могат да се разглеждат набор от сходни операции по обработване, които представляват сходни високи рискове. Съгласно посочения регламент „Оценката на въздействието върху защитата на данните се изисква, по-специално, в случай на:

1. Систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително профилиране и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице.
2. Мащабно обработване на специални категории данни.
3. Систематично мащабно наблюдение на публично достъпна

[6] Как спечелих дело за теча на данните ми от НАП, (https://www.dnevnik.bg/analizi/2021/01/15/4163037_kak_spechelih_delo_za_techa_na_dannite_mi_ot_nap/).

зона.

Оценката за въздействието върху защитата на личните данни следва да се направи преди обработването на данните. Следователно първо е необходимо да се установят и определят съответните рискове от данните, които рискове са присъщи за всеки един контролиран обект (в т.ч. за всяко едно физическо лице), а след това следва да се пристъпи към цялостния процес по оценяване. Основното европейско изискване, което се поставя чрез Регламент 2016/ 679[7] е оценката да съдържа:

1. Системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес.

2. Оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите.

3. Оценка на рисковете за правата и свободите на субектите на данни.

4. Мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

С оглед спазването на изискването на чл. 35 от Регламент 2016/679 и предвид факта, че Националната агенция за приходите извършва съвместни контролни дейности с останалите контролни институции на изпълнителната власт, чрез което се осъществява миграция на данни, като се използват нови технологии, агенцията системно прави оценка на въздействието върху защитата на личните данни. Също така, в изпълнение на изискванията на Регламент 2016/679 на Европейския парламент и на Съвета и Закона за защита на личните данни в структурите на НАП, от 2019 г. са определени длъжностни лица по защита на данните на всички структури на агенцията. В изпълнение на относимото действащо законодателство и утвърдените вътрешни актове на НАП длъжностните лица извършват регулярно

[7] 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). (https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32016R0679&from=HU).

мониторинг относно защитата на личните данни в НАП както по отношение на законоустановените функции на приходната администрация, така и по отношение на публикуваната информация в сайта. Въз основа на утвърдената политика при постъпване на сигнали от страна на граждани или институции за злоупотреба с данните се прави своевременна проверка, като резултатите от проверката се предоставят на Комисията по защита на личните данни.

При цялостния процес на оценяване на риска следва да се разгледа и да се изследва първо вероятността от настъпване на съответния риск, а така също неговата тежест. Въз основа на тази информация е необходимо да се определи и оцени дали рискът е висок, среден или нисък. След като определи неговата тежест и характер, може вече да се пристъпи към съответните организационни мерки по защита от съответните рискове.

Въз основа на всичко изложено дотук може да се приеме, че контролните институции, в т.ч. Националната агенция за приходите, се стремят при осъществяването на своята контролна дейност съвместно с останалите контролни институции от изпълнителната власт да гарантират и защитят личните данни на лицата. Новите технологии, колкото и да са необходимост и основен фактор за развитие, толкова са и съществен фактор, чрез който може да се въздейства в различни негативни насоки, включително чрез посегателство на личните данни. Всички институции, в т.ч. и ЕС, се стремят превантивно да обхванат всички възможни заплахи и да въздействат чрез налагането на различни мерки и изисквания, целящи да се гарантира защитата на личните данни на лицата.

Използвана литература

Защита на личните данни. Национална агенция за приходите стриктно спазва основните принципи, въведени като задължителни при обработването на лични данни, (https://nra.bg/wps/portal/nra/za-nap/Zashtita-na-lichnite-danni).

Регламент (ЕС) 2016/679 на Европейския парламент и на 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 относно защитата на данните), (https://eur-lex.europa.eu/

legal-content/BG/TXT/PDF/?uri=CELEX:32016R0679&from=HU).

Как спечели дело за теча на данните ми от НАП, (https://www.dnevnik.bg/analizi/2021/01/15/4163037_kak_spechelih_delo_za_techa_na_dannite_mi_ot_nap/).

Годишен отчет за дейността на Националната агенция за приходите за 2019, (https://nra.bg/wps/wcm/connect/nra.bg25863/4d5b4a64-3f1a-49a5-8cbd-b4cabf77bacd/Годишен_отчет_НАП2019.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE.Z18_PPGAHG8009LJC0QTR5C2HH30I6-4d5b4a64-3f1a-49a5-8cbd-b4cabf77bacd-nDZA1Dw).

За контакти: гл. ас. д-р Пламена Недялкова
Икономически университет – Варна
e-mail: plnedyalkova@ue-varna.bg

ПРАВНИ АСПЕКТИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В СЪВРЕМЕННОТО ДИГИТАЛНО ОБЩЕСТВО

гл. ас. д-р Даниела Петрова
Технически университет – Варна,
катедра „Социални и правни науки“

LEGAL ASPECTS OF PERSONAL DATA PROTECTION IN THE MODERN DIGITAL SOCIETY

Prof. Daniela Petrova, Ph.D.
Technical University – Varna,
Department of Social and Legal Sciences

Резюме: Целта на автора в настоящата публикация е да представи законовите и професионални изисквания при защитата на личните данни в модерното дигитално общество. Да се определят обхватът и основанията за боравене с личните данни, които всеки един от нас предоставя в гражданско-правния оборот на обществените отношения.

Ключови думи: *правен базис, дигитално общество, защита, лични данни*

Abstract: The purpose of the author in this publication is to present the legal and professional requirements for the protection of personal data in the modern digital society. To determine the scope and grounds for handling personal data that each of us provides in the civil law turnover of public relations

Key words*: legal basis, digital society, protection, personal data*

DOI: https://doi.org/10.36997/PPDD2021.135

Въведение

Технологиите са в основата на правната трансформация на дигиталното общество. Европа има дълга история при разработването на правни разпоредби за поверителност, но все по-нарастващото значение на интернет в живота на европейските граждани доведе до по-

явата на ново право на правото на поверителност, това е правото на защита на данните. Защитата на данните е въпрос, който вълнува обществото и се разглежда задълбочено и широко от Европейския съюз и Съвета на Европа – представен в общите договори, както и в по-специфичните директиви и регламенти на ЕС. Скоростта на напредъка в интернет изисква непрекъсната преоценка на това как най-добре да се защитят интересите на хората, като същевременно се използват максимално всички предимства, които интернет може да предложи и може би един от най-положителните аспекти на този случай е неговият ефект при генерирането дебат за това как най-добре да се регулира мрежата през следващите години.[1] Скоростното разрастване на интернет през последните двадесет години ни сблъсква с нови предизвикателства, отнасящи се до човешките права. Особено е положението в търсенето на баланс между свободата на медиите и свободата на изразяване, от една страна, и правото на неприкосновеност на личния живот и правото на защита на личните данни, от друга.[2]

Изложение

1. Национално и Европейско законодателство

1.1. Исторически преглед на правната рамка

Правото на неприкосновеност на личния живот е регламентирано в чл. 8 на Европейската конвенция за правата на човека (ЕКПЧ), който установява правото на зачитане на личния и семейния живот. Все по-технологизираното общество направи очевидна необходимостта от международен акт (Конвенция 108/1981) с изключителен акцент върху защитата на данните. Конвенция 108, приета през 1981 г.,[3] е първият правно обвързващ източник при защитата на данните.

---

[1] A. Pease 1. CNR-IRPPS – The „right to be forgotten“: Asserting control over our digital identity or re-writing history? The case of Google Spain and Google Inc. v. AEPD & Mario Costeja González.

[2] HTTPS://CITIZENRIGHTS.EUROALTER.COM/%D1%82%D0%B5%D0%BC%D0%B8/%D0%B4% D0%B8%D0%B3%D0%B8%D1%82%D0%B0%D0%BB%D0%BD%D0%B0-%D1%81%D0%B8 %D0% B3% D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82/?LANG=BG

[3] Конвенция за защита на лицата по отношение на автоматичната обработка на лични данни относно надзорните органи и трансграничните потоци, (http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm).

В Конвенцията за защита на лицата по отношение на автоматичната обработка на лични данни относно надзорните органи и трансграничните потоци са заложени минималните стандарти за защита на хората срещу незаконно събиране и обработка на данни, както и регулиране на транснационалния поток от лични данни. В нея е дадено определение за правото на личен живот и правото да се знае каква информация се събира за отделни лица (както и да бъде коригирана, ако е необходимо). Конвенция 108/1981 е ратифицирана от всички членове на ЕС и с това се даде възможност да се осигури обща рамка за защита на данните. В последващите стъпки на нормотворците на ЕС за защитата на данните е създаването на независими надзорни органи във всяка държава членка. За целите на тази конвенция в чл.2 са дадени легалните определения за: а) ***лични данни*** означава всяка информация относно определено или определяемо физическо лице **(*заинтересовано лице***); б) ***автоматизиран регистър с данни*** означава всеки набор от информация, подложен на автоматизирана обработка; в) ***автоматизирана обработка*** включва следните операции, извършени изцяло или отчасти чрез автоматизирани средства: запаметяване на данни, извършване на логически и/или аритметични операции по отношение на тези данни, тяхното изменение, изтриване, извадки или разпространение; г) ***администратор на регистъра*** означава физическо или юридическо лице, държавен орган, институция или друг орган, компетентен съгласно вътрешното право да решава каква е целта на автоматизирания регистър с данни, категориите лични данни, които могат да бъдат запаметявани, и операциите, на които могат да бъдат подлагани те.[4] Тази защита е гарантирана от правото на ЕС и Европейската конвенция за правата на човека. В тази гаранция влизат както неприкосновеността на личния ни живот, така и защитата на личните данни. Но тези права не са абсолютни, т.е. при определени обстоятелства и в определена степен те могат да бъдат ограничени.[5]

В първичното право на ЕС защитата на данните придобива ста-

---

[4] Конвенция за защита на лицата по отношение на автоматичната обработка на лични данни относно надзорните органи и трансграничните потоци.

[5] HTTPS://CITIZENRIGHTS.EUROALTER.COM/%D1%82%D0%B5%D0%BC%D0%B8/%D0%B4% D0%B8%D0%B3%D0%B8%D1%82%D0%B0%D0%BB%D0%BD%D0%B0-%D1%81%D0%B8 %D0% B3% D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82/?LANG=BG

тут на отделно основно право (чл. 8 от Хартата на основните права от 2009 г.). Тя е свързана и едновременно с това се отличава от правото на зачитане на личния и семейния живот (чл. 7). Основният инструмент на ЕС за вторично право за защитата на данните се явява Директивата за защита на данните (ЕО) 95/46/. Тя беше въведена през 1995 г., когато стана ясно, че четирите *свободи* (стоки, услуги, столици и хора) изискват хармонизиране на стандартите на ЕС за защита на данните в различните европейски страни.[6] Директивата предлага интегриран подход към защитата на данните в цяла Европа, установяване на редица права и задължения, въпреки че държавите членки носят отговорността да ги прилагат независимо на национално ниво. Директивата за защита на данните от 1995 г. гарантира, че физическите лица имат силни права върху обработката и контрола на данните, които ги засягат, включително правото да възразят срещу обработката на данни и правото на достъп до данни. *Администраторът* на данните трябва да гарантира, че информацията се събира за *конкретни, изрични и законни цел* [7] и трябва да положи всички усилия, за да гарантира, че данните са точни, и да ги поправи или изтрие, ако не са.[8] Директивата за защита обаче налага задължението на държавите членки да предоставят редица изключения в случаи на обществен интерес, например същите стандарти за защита на данните не се прилагат в случаите на журналистически или художествен или литературен израз. От **25 май 2018 г. във всички държави – членки на ЕС се прилага пряко Общият** 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)[9] – консолидиран текст, който включва Регламент (ЕС)

---

[6] Handbook on European data protection law, *European Agency for Fundamental Rights,* 2014, (http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law).

[7] Directive 95/46/EC, article 6 (1) (b).

[8] Пак там.

[9] Общ 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),ОВ на ЕС от 04.05.2016 г. и неговата поправка, 2018 г.

2016/679, публикуван в Официален вестник на ЕС от 04.05.2016 г. и неговата поправка, публикувана на 23.05.2018 г. С него:

• се определят правилата по отношение на защитата на физическите лица във връзка с обработването на лични данни, както и правилата по отношение на свободното движение на лични данни;

• се защитават основни права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни;

• не се ограничава свободното движение на лични данни в рамките на Съюза, нито пък се забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни.

Понятията с които борави регламента са подробно разписани в глава I, чл. 4. *Определения*, както следва, са: ***лични данни*** – означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано (***субект на данни***)**;** *физическо лице, което може да бъде идентифицирано,* е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице; ***обработване*** означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване; ***ограничаване на обработването*** означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще; ***профилиране*** означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение; ***псевдони-***

мизация означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано; ***регистър с лични данни*** означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип; ***администратор*** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка; ***обработващ лични данни*** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора; ***получател*** означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за *получатели*; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването; ***трета страна*** означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни; ***съгласие на субекта на данните*** означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени; ***нарушение на сигурността на лични данни*** означава нарушение на

сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин; ***генетични данни*** означава лични данни, свързани с наследени или придобити генетични белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице; ***биометрични данни*** означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни; ***данни за здравословното състояние*** означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние; ***задължителни фирмени правила*** означава политики за защита на личните данни, които се спазват от администратор или обработващ лични данни, установен на територията на държава членка, при предаване или съвкупност от предавания на лични данни до администратор или обработващ лични данни в една или повече трети държави в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност; ***трансгранично обработване*** означава или:а) обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или б) обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка; При неспазване на правилата и в съответстващите извършени нарушения се понасят административни наказания „глоба“ или „имуществена санкция“ в размер до 20 000 000 EUR или, в случай на нарушител предприятие – до 4 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока.

Дигитална среда и сигурност

От една страна, дигитализацията води до трансформация, която засяга всички сфери на живота (от личния до професионалния), като съпътстващо се променят и нормите на общуване (социални, правни, етични, морални). Този процес е с динамика, която трудно подлежи на всеобхватна правна регулация, но същевременно правният ред изисква, с оглед на стабилност в отношенията, да се даде нужната гаранция за защита на обществения интерес. В тази връзка процесът на дигитализация налага преосмисляне на утвърдени в различните отрасли на правото понятия, тяхната законова актуализация с оглед постигане на целта – адекватно регулиране на обществените отношения.[10] **От друга страна,** в процеса на еволюция в отношенията е естествено да се направи и нужното за развитието на нормативната уредба и теорията, които да осигурят стабилност в отношенията между страните. На този етап правото повече от всякога е обвързано и с етичната страна на въпросите.[11] Законовата уредба в националното ни законодателство е регламентирана в Закона за защита на личните данни/ЗЗЛД/, където в чл.1 , ал.3 е посочена целта на закона - да се осигури защита на физическите лица във връзка с обработването на лични данни в съответствие с Регламент (ЕС) 2016/679, както и във връзка с обработването на лични данни от компетентните органи за целите по ал. 2. В ал.2 от ЗЗЛД се определят и правила във връзка със защитата на физическите лица при обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване.[12] Съгласно закона (ЗЗЛД) ***лични данни*** са всяка информация,отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци. Информацията е най-ценният ресурс, с който всеки от нас борави. Ние полагаме усилия, за да намерим нужната ни информация, да я получим и за-

[10] А. Андреева, Г. Йолова. За свободата и дисциплината в трудовото право – съвременни аспекти в дигиталната ера. // Бизнес и право №. 3, 2020, с. 57, (https://mpra.ub.uni-muenchen.de/108871/).

[11] Пак там, с. 63.

[12] Закон за защита на личните данни. // ДВ, №1, 2002; посл.изм. ДВ, №93, 2019.

плащаме цена, която има времеви и стойностен израз. За да получи информация и/или търсена услуга, всеки се легитимира с лични данни. За целите на съответните дейности се събират, обработват и съхраняват лични данни на потребителите. Тук следва да откроим **най- важното правно основание при предоставяне на данни – даването на *съгласие*** от страна на отделният индивид. **Правната база черпим от чл. 6 (1) от GDPR където легитимният интерес е обоснован като законосъобразност на обработването на личните данни.**[13] Скорошно решение на Съда на ЕС постановява, че „правото на защита на данните не е (…) абсолютно право, но трябва да се разглежда във връзка с обществената му функция“ и също така следва да се разглежда с оглед на принципа на пропорционалността.Този принцип е ключов при взимането на решение за това дали едно право е нарушено или не. Например забраната за изтезание и забраната на робството са абсолютни права – безусловни. При тях не съществува обществен интерес, който би могъл да оправдае човешкото изтезание или поробване. Но от друга страна, свободата на словото и правото на защита на личните данни са относителни права, т.е. при определен обществен интерес те могат да бъдат ограничени – например свободата на слово не те защитава от това да издадеш държавна тайна, защото в този случай общественият интерес налага по-голяма защита на националната сигурност.[14]

Заключение

В своята работа в интернет всеки от нас остава отпечатък, който не изчезва, а с времето става по-трудно достъпен. Правото да бъдеш забравен не е изключително право **По делото Гонзалес –** Google Inc. и Google Spain Европейският съд постановява решение през 2014 г. Правните критики се фокусират върху липсата на ясни и по-подробни критерии за защита на *правото да бъдеш забравен*, което създава много неясноти при прилагането на решението. В допълнение се изтъква като критика и прекалено широкото определение на съда

[13] https://www.privacy-regulation.eu/bg/6.htm

[14] HTTPS://CITIZENRIGHTS.EUROALTER.COM/%D1%82%D0%B5%D0%BC%D0%B8/%D0%B4% D0%B8%D0%B3%D0%B8%D1%82%D0%B0%D0%BB%D0%BD%D0%B0-%D1%81%D0%B8 %D0% B3% D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82/?LANG=BG

за *администратор на данни*. И също така опита на Съда да създаде баланс между правото на личен живот и останалите основни права, като в този си опит Съдът de facto е дал предимство на правото на личен живот. От изложеното можем да направим следните изводи и да предложим мерки за подобряване защитата на личните данни при използване на цифрови инструменти:

1) Правните аспекти на защитата на личните данни са многоаспектни и същите простират действието си както на национална територия, така и представляват трансгранични предизвикателства. 2) Налице са: необходимост от разработване на политика за защита на личните данни от работодателите, която е неделима част от фирмената политика; необходимост от провеждане на информационни кампании с адресат лица от различни възрастови групи, съобразени със степента на образователното равнище и придобитите знания; необходимост от отговорно административно управление на информационните технологии. Само с отговорно и информирано поведение ще се постига правилно прилагане на правната рамка в областта на защитата на личните данни

Използвана литература

Alice Pease1, CNR-IRPPS – The „right to be forgotten“: Asserting control over our digital identity or re-writing history?The case of Google Spain and Google Inc. v. AEPD & Mario Costeja González.

Андреева А., Г. Йолова. За свободата и дисциплината в трудовото право – съвременни аспекти в дигиталната ера.// Бизнес и право, 2020, №3, с.57, (https://mpra.ub.uni-muenchen.de/108871).

Andreeva A., G. Iolova. Za svobodata I disciplinata v trudovoto pravo-savremenni aspekti v digitalnata era. // Biznes I parvo, 2020, №3, s.57, (https://mpra.ub.uni-muenchen.de/108871).

Андрияна Андреева,& Галина Йолова. За свободата и дисциплината в трудовото право- съвременни аспекти в дигиталната ера. // Бизнес и право, 2020, №3, с.63, (https://mpra.ub.uni-muenchen.de/108871/).

Andreeva A., G. Iolova. Za svobodata I disciplinata v trudovoto pravo-savremenni aspekti v digitalnata era. //.Biznes I parvo, 2020, №3, s.63 (https://mpra.ub.uni-muenchen.de/108871).

Директива 95/46 ЕО на ЕП на ЕС**.** // ОВ, L 281/31.

(Direktiva 95/46 EO na EP na ES. // OV, L 281/31).

Закон за защита на личните данни. // ДВ, №1, 2002; посл. изм. ДВ, №93, 2019.

Zakon za zachtita nalichnite danni. // DW, №1, 2002; posl. izm ДВ, №93, 2019.

Конвенция за защита на лицата по отношение на автоматичната обработка на лични данни относно надзорните органи и трансграничните потоци.

Konvencia za zachitta na licata po otnochenie na avtomatichnata obtabotka na lichni Danni otnosno nadzorni organi I transgranichni potoci.

Общ 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).

Obsht Reglament (ES) 2016/679 na evropeiskij parlament I na Saveta ot 27 april 2016g. otnosno zachitata na fizicheskite lica vav vrazka s obrabotvaneto na lichni Danni I otnosno svobodnoto dvijenie na takiva Danni I za otmjna na Direktiva 95/46 EO (Obsht Reglament otnosno zachtitata na dannite).

Наръчник по европейското законодателство за защита на данните (2014 г.). Европейска агенция за основните права

Narachnik po evropeiskoto zakonodatelstwo za zachtita na dannite,Evropeiska agencia za osnovnite prava

Интернет източници

https://www.privacy-regulation.eu/bg/6.htm

https://citizenrights.euroalter.com/

http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law.

http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm.

За контакти: гл.ас. д-р Даниела Петрова
Технически университет – Варна, кат.СПН
e-mail: daniela088@abv.bg

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ И ВЪТРЕШЕН ОДИТ

ас. д-р Недялка Александрова
Икономически университет – Варна

PERSONAL DATA PROTECTION AND INTERNAL AUDIT

Ass. Prof. Nedyalka Alexandrova, PhD
University of Economics - Varna

Резюме: В доклада се обосновава необходимостта и се очертават възможностите за вътрешен одит на защитата на личните данни. Изразява се разбирането, че одиторите от една страна оперират с лични данни и са задължени да прилагат изискванията по тяхната защита, а от друга – те имат ролята за проверяват ефективността на процедурите за защитата на личните данни в организациите. Очертани са конкретни насоки за неговото извършване.

Ключови думи: *защита на личните данни, вътрешен одит*

Abstract:. The report justifies the need and outlines the possibilities for internal audit of personal data protection. There is an understanding that auditors, on the one hand, operate with personal data and are obliged to comply with the requirements for their protection, and on the other hand, they have the role of verifying the effectiveness of personal data protection procedures in organizations. Specific guidelines for the implementation of audit of personal data protection are outlined.

Keywords*: personal data protection, internal audit*

DOI: https://doi.org/10.36997/PPDD2021.146

Въведение

Живеем във времена на промени, засягащи всички сфери на обществото – икономическа, здравна, правна, социална, екологична и др. Икономиката се преструктурира, веригите на доставки се променят, появяват се нови професии (Иванова 2020). В тази среда информацията като ресурс все повече засилва своята роля на условие за конкурентоспособност и на икономически ресурс (Алексан-

дрова 2017). Компаниите изграждат своите маркетингови стратегии на основата на управление на клиентски портфейли (Станчева 2017) и клиентски капитал (Павлова 2016), което предполага боравене с бази от данни, съдържащи информация за клиентите. Част от тази информация попада в обхвата на т.нар. лични данни, чиято защита от неправомерно използване е регламентирана законодателно.

Законодателството по защита на личните данни, макар и променено с въвеждането на Общия регламент на Европейския съюз за защитата на данните (ОРЗД) от 27 април 2016 г., известен като GDPR, има предходна история (Матеева 2012). Съвременното изменение на обществените и икономическите отношения обаче налага както нови правила относно защитата на личните данни, така и търсене на средства за гарантиране на тази защита. Организациите са изправени както пред необходимостта от изпълнение на изискванията на регламента, така и пред нуждата от гарантиране пред обществеността на това изпълнение. Зачитането на правото на личен живот е въпрос не само на спазване на нормативни изисквания, но също и на отговорност към потребителите и общността. В този смисъл защитата на личните данни е част от корпоративната социална отговорност, която в ерата на дигиталните технологии придобива нови измерения (Благойчева 2020). В този контекст организациите търсят начин да се уверят, че са защитени от изтичане на лични данни, от една страна, поради възможната загуба на конкурентно предимство, от друга – поради опасността от санкции, а от трета – поради стремеж да избегнат загуба на репутация, свързана е евентуални проблеми в тази област. Именно тук може да се търси ролята на вътрешния одит.

Международният институт на вътрешните одитори определя вътрешния одит като независима и обективна дейност за предоставяне на увереност и консултации, предназначена да допринася за добавянето на стойност и подобряване на дейността на организацията (The Institute of Internal Auditors, n.d.). Той добавя стойност за организацията като й помага в постигне на целите чрез прилагането на систематичен и дисциплинарен подход за оценяване и подобряване на ефективността на процесите на управление на риска, контрол и управление. В това си качество той може да бъде незаменим помощник в осигуряване на защита на личните данни.

Актуалността на представената проблематика е продиктувана от нарастващата сложност на процесите в организациите, в т.ч.

нарастващото значение за дейността им на базите от данни, съдържащи чувствителна лична информация, а така също и от нарасналата необходимост от осигуряване на съответствие с регламентациите по защита на личните данни.

Целта на настоящия доклад е чрез комплексен анализ на особеностите на вътрешния одит да се очертаят възможностите за неговото приложение по отношение осигуряване на защитата на лични данни в организациите.

Предмет на изследване е вътрешният одит в контекста на относимостта му към защитата на личните данни предвид съвременните му форми и развитие.

За постигането на целта авторът си поставя **следните задачи**: 1) очертаване на съвременните тенденции в развитието на вътрешния одит; 2) очертаване на възможното приложно поле на вътрешния одит за осигуряване на защитата на лични данни; 3) извеждане на предложения за подход към одитиране на процеса на защита на личните данни в организациите.

Методологията на изследването включва комплексното прилагане на методи, традиционни такива изследвания: литературен обзор, индукция и дедукция.

Анализирането на проблематиката, свързана с ролята на вътрешния одит за защитата на личните данни, е не само с теоретично, но и с голямо практическо приложение. От една страна, предприятията се стремят да си осигурят конкурентно предимство чрез изграждане или дори закупуване на клиентски бази от данни. От друга страна, в условията на все по-засилваща се конкуренция в неспазването на регламентацията или изтичането на чувствителни данни носят голям риск, свързан с понасянето на санкции и загубата на обществено доверие.

Изложение

Връзката между защитата на личните данни и вътрешния одити е двустранна. Одиторите, включително вътрешните одитори, боравят с лични данни и самите те трябва да спазват изискванията, свързани с тяхната защита. От друга страна, ролята на вътрешния одит е да дава на ръководството на организацията разумна увереност в изпълнението на поставените пред организацията цели. Доколкото сред

тези цели са ефективното въвеждане и изпълнение на дейностите по защита на личните данни от страна на организацията, както и опазването на нейната добра репутация, вътрешният одит е призван да даде разумна увереност на ръководството и в тази посока. А това означава, че от гледна точка на вътрешния одит защитата на личните данни е обект на интерес.

Изискванията за защита на личните данни са заложени в 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), в сила от 25.05.2018 г. Регламентът доби популярност под съкратеното наименование GDPR (General Data Protection Regulation).

Вътрешните одитори, по силата на своя служебен ангажимент, разполагат с много чувствителна информация, в т.ч. лични данни. В този смисъл те следва да прилагат всички мерки по тяхната защита – технически (подходящи шкафове, СОТ и др.); процедури за защита на документите, осигуряващи защита от достъп на неоторизирани лица; мерки за защита на информационните технологии (т.нар. киберсигурност) (Вейсел 2021). Въпросите, свързани с вътрешния контрол и вътрешния одит в контекста на дигитализацията изискват специфично внимание, в т.ч. регламентиране на спазването на определени етични стандарти (Nedyalkova et al. 2021).

Освен в качеството си на администратори на лични данни, вътрешните одитори имат отношение към защитата на личните данни именно като одитори, призвани да дават увереност на ръководството относно изпълнението на целите, поставени пред организацията. Доколкото GDPR не предписва точни правила и процедури по опазване на личните данни, а въвежда по-скоро принципна регулация, компаниите следва да разработят свои правила и процедури, което само по себе си би могло да е обект на одит (Dounis 2018). Необходимо е също така са се разграничава одит на процедурите (като такива) и одит на персонала (как се изпълняват процедурите).

Въпросът със защита на личните данни може да бъде погледнат през призмата на модела на Трите линии на защита (The Three Lines Model) на международния Институт на вътрешните одитори (The Institute of Internal Auditors – IIA). Този модел помага на организа-

циите да идентифицират процесите и структурите, които участват в постигането на целите им и подпомагат доброто корпоративно управление и управлението на риска. Съгласно модела ролите от първа линия са тези, които „комуникират с управителния орган, поддържат процесите за управление на операциите и риска и осигуряват съответствие“ (Dounis 2018). На практика това са структурите и процесите, които осъществяват дейността, за която е създадена организацията, те предоставят продукти и/или услуги на нейните клиенти. Към ролите на първата линия на защита принадлежат и всички поддържащи дейности, без които цялостната дейност по предоставяне на продукти и услуги не би могла да се осъществи. Като такива може да се определят администрация, поддръжка, човешки ресурси и др. (IAA 2020) Втората линия осигурява допълнителна експертиза за управление на риска и може да се съсредоточи върху конкретни въпроси като спазване на законодателството или на етичните стандарти, вътрешен контрол, информационна и технологична сигурност, осигуряване на качеството (IAA 2020) Така погледнати, ролите на първите две линии са преплетени една в друга и като цяло висшето ръководство е отговорно и за двете като част от цялостната организация на дейността.

Вътрешният одит е т.нар. Трета линия на защита. Той осигурява независима и обективна оценка на адекватността и ефективността на управлението на дейността и на управлението на риска, както и експертиза, свързана с подпомагане на организацията за изпълнение на нейните цели. Доколкото нарушаването на изискванията по защита на личните данни може да застраши нормалното функциониране на организацията, този риск следва да попадне в полезрението на вътрешния одит и той да стане обект на анализи и проверки.

Тъй като вътрешният одит е призван да даде обективна и независима увереност на ръководството в изпълнението на целите, а не да му осигури пълна сигурност, то неговите дейности трябва да са насочени към определени аспекти на дейността на организацията на базата на предварителна оценка на риска. Това означава, че рискът от неспазване на изискванията за защита на личните данни следва да бъде идентифициран и оценен, а одитът са се насочи към: 1) проверка дали това е било направено и 2) проверка и анализ на тези процеси в организацията, които са свързани с най-голям риск в тази област. При всички положения обаче одитът на въпросите, свързани със защита на личните данни, трябва да е насочен към това дали тя е организи-

рана по начин, осигуряващ спазване на основните принципи на тази защита (Mateeva 2020):

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

Като част от одита на процесите, свързани със защита на личните данни, следва да се направи анализ на текущата ситуация. При него се определя какви данни се обработват, за каква цел, с кои системи и на кого се предават тези данни. Важно също така е да се определят хората, на които *принадлежат* данните в предприятието (Ayranci et al. 2019).

При текущия анализ на ситуацията трябва да бъде извършена инвентаризация на личните данни. Това може да бъде електронна таблица или база данни с всички лични данни, собственост на бизнеса, както и свързана с тях информация,. Освен описание какви лични данни се използват, е необходимо определяне също и техното местонахождение и техните *собственици* – като конкретни лица или длъжности. Това може да стане чрез своеобразно *картографиране* (Вейсел 2021) на данните, с цел установяване движението на информационните потоци и показване на жизнения цикъл на личните данни. Инвентаризацията следва да отговори на въпросите: какви лични данни се обработват; от какви източници се получават тези лични данни; за какви цели се събират; от кои отдели, в кои процеси, с кои инфраструктури; на кого се прехвърлят; въз основа на какво основание (задължение по закон или съгласие); за колко време се съхраняват и обработват.

На следващ етап се извършва оценка на риска, свързан с обработване на личните данни, като правните и техническите рискове се обработват отделно. Провеждат се тестове за уязвимост и пробиви в сигурността, за да се идентифицират слабите места в системата. Проверяват се и т.нар. контроли за киберсигурност срещу ситуации, които могат да възникнат въпреки предпазните мерки и да повредят системата. Тези атаки могат да доведат до прекратяване на бизнес операциите. Ето защо е важно да се създадат планове за действие при извънредни ситуации.

На следващ етап вътрешният одит трябва да провери изпълнението на заложените контролни дейности и ефективността на вътрешния контрол. Одитът може да се насочи към въпроси като:

1) Взела ли е организацията необходимите предпазни мерки срещу злонамерен достъп до лични данни (вкл. чрез софтуер)?

2) Има ли организацията политики за поверителност?

3) Действа ли организацията в съответствие със съществуващата политика за поверителност?

4) Организацията защитава ли адекватно личните данни, които обработва?

5) Организацията има ли официална управленска структура в рамките на правилата за поверителност?

6) Организацията създала ли е план за реакция в случай на нарушение на личните данни?

7) Предоставила ли е организацията необходимото обучение на персонала относно информираността за поверителността, обработката на данни и информационната сигурност?

Вътрешните одитори включват в одитния доклад констатациите си относно защитата на личните данни в организацията. На етапа на последващо проследяване се проверява изпълнението на препоръките относно установените несъответствия по време на одита на защитата на данните.

На практика, за анализа на процеса на обработване на лични данни в организацията, вътрешният одит трябва последователно и системно да потърси отговор на следните въпроси:

1. Защо се обработват лични данни?

2. Какво е правното основание за това?

3. Кой отговаря за обработването на личните данни?

4. Какви видове лични данни се събират?

5. Кой ще получи личните данни (на кого ще бъдат предоставени и в какви случаи)?

6. Как и от кого ще бъдат съхранявани?

7. Как е осигурена тяхната защита от неоторизиран достъп?

8. Колко дълго ще бъдат съхранявани?

9. Как ще бъдат унищожени?

10. Има ли процедура за комуникация с лицата, чиито лични данни се събират, по отношение на техния достъп до личните им данни, искания за заличаване или оплаквания?

11. Има ли ефективен вътрешен контрол на процесите по защита на личните данни?

Вътрешният контрол често се бърка с вътрешния одит, но те имат различна роля и цели. Вътрешният контрол е допълващ процес, осъществяван от висшето ръководство и персонала в организацията и чрез него се следи дали контролните дейности се изпълняват. Като такъв той е част от т.нар. Втора линия на защита. Вътрешният одит представлява Третата линия на защита.[1] Той е независим, осъществява се от лица, които не са част от ръководството и персонала на организацията и чрез него се наблюдава систематично и се оценява системата за вътрешен контрол.

Удачно е тези отговор на горните въпроси да бъде потърсен при прилагане и на двата подхода за одит – по звена и по процеси. Особено място в одита в последните години заема вторият подход, който дава възможност да се проследи процеса и да се установи доколко той е управляем и къде са уязвимите места. Тук следва да се подчертае, че защитата на личните данни не е самостоятелен процес в организациите и той не бива да бъде одитиран като такъв. Защитата на личните данни по-скоро трябва да се разглежда като принцип, който следва да бъде втъкан във всички останали процеси в организацията на всеки техен етап. Това не означава, че защитата на личните данни не може да бъде одитирана самостоятелно, т.е. да бъде обект на целенасочена проверка. Тази целенасочена проверка обаче следва да бъде ориентирана към защита на личните данни като аспект на всеки отделен процес в организацията, а не към някакъв самостоятелен процес на защита на личните данни, отделен от цялостната дейност.

Заключение

В съвременните условия организациите са изправени пред необходимостта да боравят с огромни масиви от лични данни по начин, едновременно осигуряващ им възможност да ги използват в дейност-

[1] Цялостната роля на вътрешния одитор в компаниите е: 1) да даде увереност на ръководството, че активите на компанията са запазени, счетоводните документи и записвания са правилни, достоверни и надеждни и оценяването на активите и пасивите е в съответствие с приложимите счетоводни стандарти; 2) да изследва ефективността на дейността на организацията и да извършва разследвания в съответствие с искането на висшето ръководство. В допълнение вътрешните одитори могат (и трябва) да си партнират с външни одитори при необходимост.

та си и да ги защитават, спазвайки законодателството и опазвайки своята репутация. На този фон вътрешният одит играе роля на т.нар. Трета линия на защита, даваща увереност на ръководството, че тези цели са постигнати. За целта той следва да извърши специализирани одитни дейности по анализ на текущата ситуация по управление и защита на личните данни в организацията, оценка на риска, свързан с управлението и защитата на лични данни, и проверка на процеса по изпълнение на заложените контроли за минимизиране на риска и вътрешния контрол.

Използвана литература

Ayranci, B., S. Dogan, B. Tagran Mendi (2019). // An internal audit methodology within the framework of the protection of personal data, №6698.

Dounis, N. (2018). GDPR Regulatory Compliance and the Role of Internal Audit: Theoretical and Practical Approach. // International In-House Counsel Journal, 2018, №11.

IAA (2020). Модел на трите линии на защита, (https://na.theiia.org/translations/PublicDocuments/Three-Lines-Model-Updated-Bulgarian.pdf).

Mateeva, Z. (2020). Principles of personal data protection. *International Journal of Economic Research*, *28*(June), 95–104.

Nedyalkova, P., A. Andreeva, G.Yolova. Digitalization and the new legal and economic challenges to employers in implementing internal control. // Ikonomicheski Izsledvania, 2021, Vol. 30, №5, pp. 158 – 175.

The Institute of Internal Auditors. (n.d.). About Internal Auditing. (https://global.theiia.org/about/about-internal-auditing/pages/about-internal-auditing.aspx, 2.11. 2021).

Александрова, Н. (2017). Знанието като обект на счетоводството. // International Scientific Conference High Technologies. Business. Society, pp. 187 – 189.

Благойчева, Х. Корпоративната социална отговорност в света на цифровите технологии. Управление на човешките ресурси в ерата на дигиталните предизвикателства // Известия, 2021, том 65, №1, с. 54 – 60.

Вейсел, А. Насоки за защита на личните данни за одитори. // ИДЕС, 2021, №1, с. 1 – 13.

Иванова, М. (2020). Нови професии на пазара на труда. // Управление на човешките ресурси в ерата на дигиталните предизвикателства. Сборник с доклади. Варна: Наука и икономика, с. 67–73.

Матеева, Ж. За понятието „лични данни“ по Закона за защита на личните данни. // Управление и устойчиво развитие, 2012, том 36, №5, с. 100 – 105.

Павлова, Д. Методически аспекти при изучаването на клиентския капитал. // Управление и устойчиво развитие, 2016, том 58 №3, 69 – 73.

Станчева, В. Управление на клиентски портфейли: концептуални основи и емпирични резултати. // Известия на Съюза на учените – Варна, 2017, №1, с. 63 –71.

За контакти: ас. д-р Недялка Александрова
Икономически университет – Варна
e-mail: alexandrova.n@ue-varna.bg

ЕЛЕКТРОННА ИДЕНТИФИКАЦИЯ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Гергана Върбанова
Адвокатска колегия – Варна

ELECTRONIC IDENTITY AND PERSONAL DATA PROTECTION

Gergana Varbanova, Ph.D
Attorney at law

Резюме: Интернет общуването и дигиталните технологии са неизменна част от ежедневието ни. Предоставянето на електронни публични услуги, нарастващият обем от електронни трансакции и електронният оборот поставят редица въпроси за сигурността на информацията и електронната идентификация на субектите, така че да не съществува съмнение относно участниците в съответните производства или в дигиталния търговски оборот. Поставя се въпросът кой е аналогът на личната карта, който да служи за идентифициране на лицата и другите субекти в дигитална среда. Докладът изследва приложението на електронната идентификация и електронната идентичност в контекста на сигурността на личните данни и възможностите да минимализиране на злоупотребата с лични данни чрез процеса на електронна идентификация.

***Ключови думи**: електронна идентичност, сигурност, лични данни, електронна идентификация, дигитализация*

Abstract: Internet communication and digital technologies are an integral part of our daily lives. The provision of electronic public services, the growing volume of electronic transactions and electronic turnover raise a number of issues with the security of information and electronic identification of entities, so that there is no doubt about the participants in the relevant proceedings or in the digital trade. The question is what is the analogue of the ID card, which should be used to identify individuals and other entities in a digital environment. The report examines the application of electronic identification and electronic identity in the context of personal data security and the possibilities to minimize the misuse of personal data

through the electronic identification process.

***Key words**: electronic identity, security, personal data, electronic identification, digitalization*

DOI: https://doi.org/10.36997/PPDD2021.156

Въведение

Електронната идентификация ще бъде неизменна част от ежедневието на съвременния човек, който в условията на дигитално общуване предоставя ежедневно личните си данни в глобалната мрежа. Проучване на *Евробарометър* (Attitudes towards the Impact of Digitalisation on Daily, Lives) от месец декември 2019 г. показва, че голяма част от българските граждани използват за целите на електронната идентификация потребителските си профили в социалните мрежи или имейл акаунта си. Голяма част от анкетираните искат да имат контрол върху информацията, която предоставят в глобалната мрежа, в частност, да контролират обема от лични данни, които предоставят както на публично правните субекти, така и на частните лица, а 43% от респондентите заявяват, че не желаят да споделят каквато и да било лична информация и данни, независимо от целите, за които те се изискват. Проучването показва, че обществото подхожда с недоверие към споделяне на лични данни и информация в глобалната мрежа, но същевременно използва и споделя сериозно количество от тях, въпреки нагласите си тези лични данни и информация да останат несподелени. Ситуацията изглежда като *circulus vitiosus*, но достиженията на технологиите дават своето решение – *електронната идентификация*.

Изложение

Електронната идентификация има свое легално определение, което се съдържа в чл.3, т. 1 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО, а именно *електронна идентификация* е процес на използване на данни в електронна форма за идентификация на лица, които данни предста-

вляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице. Понятието *електронна идентификация* по смисъла на регламента е с *по-широк* обхват от понятието електронна идентификация, което влага законодателят в Закона за електронната идентификация (ЗЕИ). Законът регулира само *електронната идентификация на физическите лица* посредством държавна схема за електронна идентификация, докато регламентът предвижда и създаване на *частни схеми за електронна идентификация както на физическите лица, така и на юридически лица, или физически лица, представляващи юридически лица*.

Какво обаче е *електронната идентификация*? Защо изобщо има нужда от нея? Кое е това, което налага създаването на държавни и частни схеми за електронно идентификация, и как това ще повиши сигурността при споделяне на лични данни в интернет?

Концепцията на *електронната идентификация* възниква, за да преодолее един съществен недостатък на интернет. Свързвайки се чрез него с неограничен брой субекти, ние реално *не знаем с кого комуникираме*. Интернет е изграден така, че посредством протоколи се осигурява свързаност между различни устройства в мрежата. При тази свързаност ние *нямаме информация кои са субектите, които са отвъд „машината“* и в чиято правна сфера настъпват определени правни последици. Практически ние *не знаем дали в действителност комуникираме с определен субект*. Тази неизвестност излага потребителите на виртуалното пространство на *риск*, доколкото могат да станат *жертва на измама, кражба на самоличност и правата им да бъдат засегнати от недобросъвестни лица* (Preukschat, Reed, 2021). Нещо повече, макар и в мрежата определени устройства да се идентифицират посредством TCP/IP протокол, тази информация може лесно да бъде преднамерено променена, поради което и информацията за местонахождението на определено устройство в мрежата може да не бъде достоверна. Преодоляването на този проблем може да се осъществи чрез *електронната идентификация и създаването на електронна идентичност*.

Електронната идентичност на физическите лица не е нищо повече от електронно представяне на нашата физическа идентичност, тя е аналог на личната ни карта във виртуалното пространство. Електронната идентификация дава възможност на различните субекти във виртуалното пространство да идентифицират субекта, с който

комуникират (повече за електронната идентификация на https://blog.bozho.net, блог на Божидар Божанов). Концепцията за електронната идентичност и електронната идентификация залага на идеята, че информацията която споделят физическите лица в процесът на електронна идентификация е по-контролирана и изцяло зависи от тяхното съгласие. Така, ако трябва да удостоверим самоличността си при предоставяне на административна услуга (физически), ние споделяме цялата налична информация от личната си карта – ЕГН, постоянен адрес, данни за цвят на очите, ръст, място на раждане. В процеса на електронна идентификация обаче, идеята е субектът да сподели само онези лични данни, *които са необходими за предоставяне на определена услуга* и за процеса на електронната му идентификация (Kim Cameron's Identity Weblog 2005). В дадения пример, при заявяване на услуга по електронен път чрез средствата за електронна идентификация, ще бъде предоставена не цялата информация, която е налична и е свързана с дигиталната ни идентичност, а само тази, която е необходима за целите на административното производство – най-често това ще бъде ЕГН, като в процеса на електронна идентификация доверяващата страна получава само нужния й обем от идентифициращи данни. Такова лимитиране на предоставяне на личните данни трудно може да бъде постигнато в аналоговия свят, доколкото няма как да бъде отделена и селективно представена информацията от личната карта на физическите лица. Електронната идентификация и предоставянето само на определена информация от електронната идентичност на субектите намалява риска от злоупотреба с личните данни и на практика е много по-сигурна от физическата идентификация с документи за самоличност. При физическото използване на документи за самоличност рискът от злоупотреба с личните данни, кражбата на самоличност или дори изгубване на документите е по-голям отколкото при средствата за електронна идентификация и електронната идентичност. Освен че процесът на електронна идентификация е изцяло под контрола на субекта, той често е обвързан с технологии, които осигуряват допълнителна сигурност – например процеса на автентикация е обвързан с биометрични данни на субекта на електронната идентификация.

Електронната идентификация има за цел да предостави определена информация от електронната идентичност на даден субект, но самото предоставяне се осъществява чрез процеса на електронна

автентикация. Електронната автентикация има за цел да потвърди, че субектът е именно този, за който се представя, и по този начин неговата дигитална идентичност ще бъде потвърдена (Димитров 2020).

Често субектите ползват акаунт във Facebook, Instagram и др. за достъп и използване на интернет приложения, включително като средство за автентикация и достъп до приложение или игра. Подобен достъп обаче крие своите рискове, доколкото се ползва с ниска степен на сигурност и не използва същинска електронна идентификация и данни за електронната идентичност на съответния потребител. Потребителските профили в социалните мрежи по никакъв начин на гарантират, че лицето, което използва потребителския профил, е това за което се представя. Възможно е профилът в някоя социална мрежа да бъде нарочно създаден с цел кражба на самоличност и злоупотреба с лични данни. В този смисъл интегрирането и използването на електронната идентификация и електронната идентичност, която да бъде ползвана за всички онлайн услуги – публични и частни, биха свели до минимум възможностите за злоупотреба с лични данни. Изследване на Европейската комисия посочва, че малка част от субектите (физически и юридически лица) имат достъп до трансгранична услуга по електронна идентификация. Това мотивира и създаването на нова правна рамка, която задължава всяка държава членка да създаде сигурен, надежден и безпроблемен достъп до трансгранични публични и частни услуги, включително да започне издаването на *европейски портфейл за цифрова идентичност*.

Съгласно предложението за изменение на Регламент №910/2014 европейският портфейл за цифрова идентификация трябва да позволява на потребителите: 1. сигурно да изискват и получават, съхраняват, избират, комбинират и споделят по начин, който е прозрачен за и проследим от съответния потребител, необходимите идентификационни данни за юридическите лица и електронно удостоверяване на атрибути за удостоверяване онлайн и офлайн с цел използване на онлайн публични и частни услуги и 2. да подписват с квалифициран електронен подпис.

Предвижда се период от 12 месеца, в който държавите членки трябва да осигурят възможност за издаване на европейския портфейл за цифрова идентификация. В основата на предложението за изменение на регламента е заложено изискването за най-високо ниво на сигурност на личните данни, използвани за удостоверяване на

електронната идентичност, независимо дали тези данни ще бъдат съхраняват локално или чрез технологично, облачно решение. Предложението за изменение предвижда възможността за използване на биометрични данни като метод за идентификация. Биометричните данни представляват уникална характеристика на човек, поради което и обработването им трябва да отговаря на Общия регламент за защита на личните данни. Основната идея на предложението за изменение на регламента е да се гарантира висока степен на сигурност в областта на електронната идентификация, която да предостави на всички субекти от страните – членки на ЕС сигурна електронна идентификация, приложима както за публичния така и за частния сектор. Чрез европейския портфейл за цифрова идентификация субектите ще могат да се идентифицират свободно в дигитална среда, като сами преценят какви цифрови средства за идентификация ще включат в своя портфейл – професионална шофьорска книжка, професионални или образователни квалификации, паспорт и др. Портфейлът за цифрова идентификация ще осигури възможност за удостоверяване в електронна среда на самоличността на субектите, както и за потвърждаване на тяхно определено качество – управител на търговско дружество, професионална квалификация или придобита специалност. Идеята е тази дигитална идентичност да бъде използвана при предоставяне на публични и частни онлайн услуги, като лицата споделят информация от дигиталната си идентичност и то само толкова, колкото е необходима за предоставяне на услуга или удостоверяване на определено качество на субекта в дигитална среда (повече информация за европейския портфейл за цифрова идентификация е достъпна на: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664). Нещо което е невъзможно да бъде постигнато в аналоговия свят.

Заключение

Технологиите се променят, нуждите от сигурно установяване на дигиталната идентичност на субектите нараства в мащаби, които никой не е предполагал, когато интернет е бил създаден. Електронната идентификация и сигурното удостоверяване на електронната идентичност са предизвикателство не само в областта на технологиите, но и за действащия правов ред, който трябва да отговори своевременно

и адекватно на научния напредък и нуждата от регулация в областта на електронната идентификация и електронната идентичност.

Използвана литература

Димитров, Г. (2020). Автентикация, оторизация, електронна идентичност. Цифрови сертификати, електронни подписи, (http://eng-dimitrov.com).

Kim Cameron's Identity Weblog, 2005 The Laws of Identity (2005), (https://www.identityblog.com/).

Attitudes towards the Impact of Digitalisation on Daily Lives, (https://europa.eu/eurobarometer/surveys/detail/2228).

Preukschat, A., D. Reed (2021). Self-Sovereign Identity – Decentralized digital identity and verifiable credentials. New York: Manning Publications.

https://blog.bozho.net

https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664

За контакти: д-р Гергана Върбанова
Адвокатска колегия – Варна
e-mail: gergana@varbanova.bg

СРОКОВЕТЕ ЗА СЪХРАНЕНИЕ НА ЛИЧНИ ДАННИ, ОБРАБОТВАНИ В МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ ВЪВ ВРЪЗКА С ПРОВЕЖДАНЕ НА НАКАЗАТЕЛНО ПРОИЗВОДСТВО ПО РЕДА НА НАКАЗАТЕЛНО-ПРОЦЕСУАЛНИЯ КОДЕКС И НА ПРОВЕРКИ ЗА НАЛИЧИЕ НА ДАННИ ЗА ПРЕСТЪПЛЕНИЯ ОТ ОБЩ ХАРАКТЕР

докторант Елена Андреева
Университет за национално и световно стопанство

TIME LIMITS FOR STORAGE OF PERSONAL DATA PROCESSED IN THE MINISTRY OF INTERIOR IN CONNECTION WITH CONDUCTING CRIMINAL PROCEEDINGS UNDER THE PENAL PROCEDURE CODE AND WITH CHECKS FOR THE EXISTENCE OF DATA OF CRIMES OF A GENERAL NATURE

PhD student, Elena Andreeva
University of National and World Economy

Резюме: Докладът поставя на обсъждане ключови въпроси за съответствието на уредбата, установяваща сроковете за съхранение на личните данни, обработвани в МВР във връзка с провеждане на наказателни производства и на проверки за наличие на данни за престъпления от общ характер, с изискванията на ЗЗЛД и правото на ЕС.

Ключови думи: *лични данни, наказателно производство, проверка, МВР*

Abstract: The report discusses the compliance of the regulation establishing the time limits for storage of personal data processed by the Ministry of Interior in connection with criminal proceedings and inspections for data of crimes of a general nature with the requirements of the Personal Data Protection Act and EU law.

Key words: *personal data, criminal proceedings, inspection, Ministry of Interior*

DOI: https://doi.org/10.36997/PPDD2021.163

Въведение

За изпълнение на дейностите си органите на Министерството на вътрешните работи могат да обработват лични данни. Допуска се обработка и на лични данни, получени от други органи за целите, за които са предоставени, както и за защита на националната сигурност, опазване на обществения ред и противодействие на престъпността. Според изричната разпоредба на чл. 25 от Закона за Министерството на вътрешните работи обработването на лични данни трябва да се осъществява при условията и по реда на националното законодателство (Закон за защита на личните данни и Закон за Министерството на вътрешните работи) и обвързващите Република България актове на общностното право на Европейския съюз (Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016г. 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.[1] Въпросът, който се поставя с настоящата разработка, е отговаря ли в действителност нормативната уредба, регламентираща съхранението на лични данни от МВР, на изискванията на посочените актове в един неин аспект – продължителността на съхранението.

Според закона министърът на вътрешните работи е администратор на лични данни и може да възлага обработването им на определени от него длъжностни лица, а редът за обработване се определя с издадената от него Инструкция № 8121з – 1122 от 12.09.2015 г. за реда за обработка на лични данни в МВР[2] (чл.29, ал.1 и ал.2, ЗМВР).

Една от дейностите, във връзка с която се обработват лични данни, е тази по защита на националната сигурност, противодействие на престъпността, опазване на обществения ред и провеждане на наказателното производство. При обработка на данни, основано на тази необходимост, органите на МВР са поставени в привилегировано положение, тъй като по отношение на тях действат редица особени норми (чл. 26, ал.1, т.1 – 6, ЗМВР). Те могат да не искат съгласието на физическото лице и да не го информират преди и по време

---

[1] ОВ, L 119/1, 2016.

[2] ДВ, №73, 2015, (в сила от 25.09.2015 г).; доп.// ДВ, №. 3 , 2017, (в сила от 10.01.2017 г). Инструкцията е издадена на основание чл. 29, ал. 2 от Закона за Министерството на вътрешните работи (пар.3 ПЗР).

на обработването на личните му данни, могат да обработват всички необходими категории лични данни, могат да предоставят личните данни както на други правоохранителни органи, така и на органите на съдебната власт за нуждите на конкретно наказателно производство. Нещо повече, те имат право да предоставят личните данни на други администратори с оглед на обработването им за цели, различни от целите за защита на националната сигурност, противодействие на престъпността, опазване на обществения ред и провеждане на наказателното производство, в съответствие с Регламент (ЕС) 2016/679 и със ЗЗЛД и по ред, определен с Инструкция № 8121з – 1122 от 12.09.2015 г. Допустимо е още органите на МВР да обменят лични данни с компетентни органи и получатели от държави – членки на ЕС, органи и агенции на ЕС, трети държави или международни организации в съответствие с Регламент (ЕС) 2016/679 и със ЗЗЛД.

Така събраните данни се съхраняват в рамките на срокове, установени от администратора, и те могат да бъдат изтрити в изпълнение на акт на съда или на Комисията за защита на личните данни (КЗЛД). Администраторът установява и сроковете за периодична проверка на необходимостта от съхранение на данните (чл. 26, ал. 2 от ЗМВР).

Сроковете за съхранение са регламентирани в Инструкция № 8121з –748/20.10.2014 г. за определяне на срокове за съхранение на лични данни, обработвани в МВР във връзка с провеждане на наказателно производство по реда на Наказателно-процесуалния кодекс и на проверки за наличие на данни за престъпления от общ характер.[3] Актът урежда въпроса както по отношение на данните, събирани в хода на проверката като предпроцесуална дейност, така и в хода на наказателния процес. Регламентацията е приложима както за престъпления от общ характер, така и за престъпления от частен, публично-частен и частно-публичен такъв.

Въпреки че заглавието не подсказва това, всъщност подзаконовият акт, освен сроковете за съхранение на данните, урежда и други ключови въпроси като субектите на лични данни, основанията, които обуславят възможността за обработка и съхранение на техните данни, и условията, при които обработката и съхранението на данните може да се преустанови.

Що се отнася до субектите, в чл.2 от Инструкция № 8121з –

[3] ДВ, №88, 2014., (в сила от 01.11.2014 г.); изм. и доп. ДВ, №78, 2018.

748/20.10.2014 г. се сочи, че на обработка подлежат личните данни на *лица* във връзка с провеждане на наказателно производство по реда на НПК и на проверки за наличие на данни за престъпления от общ характер. Налага се изводът, че на обработка подлежат личните данни на *всички лица*, които имат касателство към водено наказателно производство или проверка. Разпоредбата на чл. 3 от Инструкция № 8121з –748/20.10.2014 г. назовава изрично само две категории лица – *пострадал* и *заявител на престъпление*. Легална дефиниция е дадена само на последното понятие – лице, което е подало съобщение, съдържащо данни за престъпление от общ характер и не е пострадало от престъплението (пар.1, т.2 от ДР). Лице по чл. 2 от инструкцията обаче е и лицето, срещу което е подаден сигналът за престъплението (ако може да бъде идентифициран към този ранен момент), т.е. извършителят на престъплението. При образувано наказателно производство и повдигнато обвинение субект на данни е и обвиняемият. Макар да не е посочено изрично, несъмнено е, че данните за тези лица също се обработват и са подчинени на режима на този акт.

Основанието за обработка и съхранение на личните данни на посочените категории лица е именно касателството им (отношението им, връзката им) с деянието, за което се води наказателното производство или се извършва проверката. Сроковете за съхранение и условията за заличаване са диференцирани според качеството, което лицето – субект на данни има в наказателното производство или проверката, с което данните на всяко отделно лице (пострадал, заявител или извършител/обвиняем) са поставени при различен режим.

Личните данни на пострадало лице, обработвани в информационните фондове на МВР, се заличават при настъпване на смъртта на лицето, но не по-рано от 10 години от датата на въвеждането им във фондовете на МВР (чл.4 от Инструкция № 8121з – 748/20.10.2014 г.), докато личните данни на заявител на престъпление се заличават при изтичане на 5 години от датата на въвеждането им във фондовете на МВР (чл.5 от Инструкция № 8121з – 748/20.10.2014 г.) Така определените срокове са еднакви както при проверките, така и при производствата по НПК.

Вписаните във фондовете лични данни на извършителите се заличават при условия, предпоставени от характера на производството във връзка с което се обработват – проверка за установяване на данни за престъпление от общ характер или наказателно производство по

смисъла на НПК и от основанието, на което производството е преустановено.

В хипотезата на проверка данните се заличават при постановен отказ от образуване на наказателно производство в случаите на чл. 24, ал. 1, т. 1 и 8а от НПК или, когато не е образувано наказателно производство в случаите на чл. 24, ал. 5 от НПК. При постановен отказ от образуване на наказателно производство на основание чл. 24, ал. 1, т.2 – 8, т.9 и 10 от НПК заличаването настъпва не като последица от акта, а след като е изтекъл давностния срок по чл. 81, ал. 3 във връзка с чл. 80 от Наказателния кодекс (НК) за престъплението, за което е водена проверката (чл.3, т.1 и т.2 и т.5, буква „а“ от Инструкция № 8121з – 748/20.10.2014г.).

В хипотезата на наказателно производство данните се заличават, ако то е прекратено на реабилитиращо основание по смисъла на чл. 24, ал. 1, т. 1 от НПК, когато деянието не е извършено или не съставлява престъпление или на чл. 243, ал. 1, т. 2 от НПК, когато обвинението не е доказано. И в двата случая заличаването може да се направи едва след изтичане на сроковете по чл. 243, ал. 10, изр. 2 от НПК за отмяна на постановлението за прекратяване. До заличаване на данните води прекратяването на наказателното производство на основание чл. 24, ал. 5 от НПК, на основание чл. 250, ал. 1, т. 2 от НПК или на основание чл. 24, ал. 1, т. 8а от НПК (чл.3, т.3 и т.5, буква „в“ от Инструкция № 8121з – 748/20.10.2014 г.) При прекратяване на наказателно производство на основание чл. 24, ал. 1, т.2 – 8, т.9 и 10 от НПК заличаването отново настъпва не като последица от акта, а след като е изтекъл давностният срок по чл. 81, ал. 3 във връзка с чл. 80 от НК за престъплението, за което е водено производството (чл.3, т.5, буква „б“ от Инструкция № 8121з – 748/20.10.2014 г.)

Основание за заличаване е фактът на влязла в сила оправдателна присъда (чл.3, т.4 от Инструкция № 8121з – 748/20.10.2014 г.) Личните данни подлежат на заличаване и ако е наложена глоба по административен ред на основание чл. 218б от НПК и е изтекла една година от датата на извършване на деянието или ако е реализирано освобождаване от наказателна отговорност с налагане на административно наказание по чл. 78а НПК (чл.3, т.6 и т.7 от Инструкция № 8121з –748/20.10.2014г.) Смъртта на лицето е основание за заличаване на данните, обработвани във връзка както с наказателните производства по НПК, така и с проверките (чл.3, т.8 от Инструкция № 8121з

– 748/20.10.2014 г.)

Основанията са изрично лимитативно посочени. Аргумент за това е формулировката на чл. 3, т.8 от Инструкция № 8121з – 748/20.10.2014 г., която сочи, че в неизброените в чл.3, т.1 –7 случаи единственото основание за заличаване на данните е смъртта на лицето. Съдебната практика също възприема изброяването за изчерпателно, като изтъкваните съображения са свързани със специфичните цели на обработката (чл.2, ал.2 от Инструкцията).[4] Следователно ако не се реализира някое от предвидените основания, обработката на личните данни продължава до смъртта на лицето – извършител или обвиняем.

Анализът на съдебната практика показва, че най-голям проблем за вписаните в масивите извършители съставляват два случая: постановяването на отказ да се образува досъдебно производство на основание чл. 24, ал.1, т.2 – 8, т.9 и т. 10 от НПК и приключването на делата с осъдителна присъда.

Първата хипотеза визира постановяване на отказ, когато, за да се заличат данните, следва да се изчака и изтичане на преследователната давност за престъплението. По мое мнение въпросът може ли регистрираният извършител да атакува основанието за отказа има отрицателен отговор. Постановлението за отказ се изпраща на лицата, посочени в чл. 213, ал.1 от НПК, а именно пострадалият, неговите наследници, ощетеното юридическо лице и лицето, направило съобщението. В понятийния апарат на НПК отсъства думата „извършител“, но не това е причината, поради която регистрираното като такова в информационните масиви на МВР лице не може да обжалва постановлението за отказ да се образува досъдебно производство. Причината е, че само изброените в чл. 213, ал.1, изр.1-во от НПК лица и нито едно друго не е правно легитимирано да получи препис от прокурорският акт и да обжалва същия пред по-горестоящата прокуратура. Само те имат признат и гарантиран от НПК правен интерес да оспорят отказа. Така за лицето, вписано в информационните масиви на МВР като извършител, не съществува правен способ, по който да инициира контрол върху основанието за отказа. А това основание засяга съществено именно неговата правна сфера.

Втората хипотеза очертава случаите, при които признато за ви-

[4] Решение № 67 от 13.01.2020 г. по а.д. № 1365/2019 г. на Административния съд София – област.

новно и осъдено от наказателния съд лице, изтърпяло наложеното му наказание, не може да се ползва от правото данните му да бъдат заличени от информационните фондове на МВР. Така дори настъпилата реабилитация за осъдено лице не е факт, който да служи като основание за заличаване на данните. Те могат да бъдат заличени едва със смъртта на лицето. С това на практика се постига неограничено във времето обработване на данните по чл. 2 от инструкцията.

Считам, че по този начин българското право влиза в остро противоречие с разпоредбите на Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета.[5] С чл.5 от същата държавите членки се задължават да предвидят определени подходящи срокове за изтриване на личните данни или за периодична проверка на необходимостта от съхранението на данните. Не се допуска възможността за безсрочно съхраняване и обработване на данни. В действителност обаче според българското право се постига точно този ефект по отношение на признатите за виновни лица. Това повдига въпроса имат ли всички лица – извършители, субекти на данни, право да бъдат забравени? По мое мнение отговорът е отрицателен, защото практически до смъртта на лицето неговите данни ще бъдат обработвани и съхранявани в информационните фондове, поддържани от МВР.

Според Съда в Страсбург продължителността на съхраняването на личните данни е обстоятелство, което макар да не е решаващо, е важно за оценката дали действията на държавните органи са пропорционални на преследваната цел. За непропорционално и оттам за нарушаващо стандарта на чл. 8 от Европейската конвенция за защита правата на човека и основните свободи е прието доживотно обработване на сведения за съдимостта (осъдителни и оправдателни съдебни актове), *предупреждения и порицания*, отнасящи се до едно лице,[6] запазване на личните данни за срок от 40 години за извършител на

[5] ОВ, L 119/89, 2016.
[6] M.M. v. United Kingdom, 2012.

нетежко престъпление[7] или за срок от 20 години при прекратено наказателно производство за насилие след решаване на делото чрез медиация[8] и т.н. Съдът приема, че съществува риск от стигматизация, когато лица, които не са осъждани за престъпление и имат право да се ползват от презумпцията за невиновност, се третират по същия начин като осъдените лица[9], защото са регистрирани в едни и същи информационни масиви и данните им се обработват при идентични условия.

Съдът приема, че доживотното вписване в полицейското досие на дадено лице е довело до установяване на нарушение на член 8 от ЕКЗПЧОС. Съдът счита, че осъждането на дадено лице в миналото, с течение на времето става неразделна част от личния му живот, който трябва да се уважава. Въпреки това съдът отчита, че данните за досието за съдимост са в известен смисъл обществена информация, което означава, че тя би могла да бъде разкрита много след осъждането, когато вероятно всички, освен субекта на данните, биха забравили случката. Нарушаваща основните човешки права ситуация е тази, при която критериите за преразглеждане на разрешаването на изтриването на данните са доста ограничителни и исканията за изтриване са удовлетворявани само в изключителни случаи.[10]

С оглед спазване изискванията на конвенцията съдът изтъква, че при установяване на сроковете държавите следва да се ръководят от тежестта на престъплението, обществената опасност на извършителя, неговата възраст и т.н. Подход като възприетия у нас, а именно на липса на такава диференциация, всъщност се намира в остра колизия с тези стандарти.

Внимание заслужава и въпросът за необходимостта от въвеждане на периодична проверка на необходимостта от съхранение на данните. Инструкция № 8121з –748/20.10.2014г. е издадена от министъра на вътрешните работи на осн. чл. 26, ал.1, т. 3 от ЗМВР (редакция към ДВ, №53, 2014.) По словесното си съдържание разпоредбата на чл. 26, ал.1, т. 3 от ЗМВР в посочената редакция частично съответства на чл. 26, ал.2, изр.1-во от ЗМВР от актуалната редакция (към // ДВ, №17, 2019) що се отнася до частта за сроковете за съхранение.

---

[7] Ayçaguer v. France, 2017.
[8] Brunet v. France, 2014.
[9] S. and Marper v. the United Kingdom, 2008.
[10] M.M. v. the United Kingdom, 2012.

С измененията от 2019 г. се въвежда посоченото по-горе изискване администраторът да установи и сроковете за периодична проверка на необходимостта от съхранение на данните. В Инструкция № 8121з – 748/20.10.2014 г. сроковете за такива проверки не са установени.

Привеждането на нормативната уредба по въпроса за съхранението на личните данни, обработвани от МВР във връзка с наказателни производства или проверки за установяване наличие на данни за извършени престъпления от общ характер, е въпрос от особена важност, тъй като актуалната регламентация засяга по недопустим начин правната сфера на субектите на данни.

Използвана литература

ДВ, №88, 2014., (в сила от 01.11.2014 г.); изм. и доп. ДВ, №78, 2018.

ДВ, №73, 2015; доп. ДВ, №. 3 , 2017.

ОВ, L 119/89, 2016.

Решение № 67 от 13.01.2020 г. по а.д. № 1365/2019 г. на Административния съд София – област.

Ayçaguer v. France, 2017.

Brunet v. France, 2014.

M.M. v. the United Kingdom, 2012.

S. and Marper v. the United Kingdom, 2008.

За контакти: Докторант Елена Андреева
УНСС
e-mail: elena_andreeva_@abv.bg

КОДЕКС ЗА ПОВЕДЕНИЕ ВЪВ ВРЪЗКА С ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ В СФЕРАТА НА ВИСШЕТО ОБРАЗОВАНИЕ

докторант Горан Проданов
Шуменски университет „Епископ Константин Преславски“

CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL DATA IN HIGHER EDUCATION

PhD Student, Goran Prodanov
Konstantin Preslavsky University of Shumen

Резюме: Обект на наблюдение и коментар са правната уредба, практическите ползи и необходимостта от разработването и евентуалното присъединяване от страна на администратори и обработващи лични данни в сферата на висшето образование към Кодекс за поведение по смисъла на чл. 40 от ОРЗД. Предложеният текст е част от научно изследване в момент на разработка, свързано с разглежданата проблематика, което е съсредоточено върху разработването на примерен Проект на кодекс за поведение. Целта на изготвянето му е да предизвика дискусия между заинтересованите страни и лица, при необходимост да бъде допълнен и изменен, а впоследствие да бъде внесен за одобрение от надзорния орган.

Ключови думи: *Кодекс за поведение, ОРЗД, висше образование, лични данни*

Abstract: The research objectives of this study are the legal framework, the practical benefits and the necessity for the development and possible adherence by controllers or processors of personal data in higher education to a Code of Conduct referred to in Article 40 of the GDPR. The study is part of an extended research at the time of development, related to the issues under consideration, which is aimed at developing a draft code. Its purpose is to provoke a discussion between stakeholders and interested parties, to be amended if necessary, and subsequently submitted for approval by the supervisory authority.

Key words: *Code of Conduct, GDPR, Higher Education, Personal Data*

DOI: https://doi.org/10.36997/PPDD2021.172

Въведение

За да осигурят своето хармонично съществуване, цивилизованите обществата са възприели подход за формализирането на определени принципи на поведение, свързани с тяхната култура, ценности и идеали, които наричаме закони, наредби и кодекси. Те са започнали да създават кодекси и правила за поведение много рано в своето развитие, като първите белези за това са открити в древна Месопотамия. Най-ранният съществуващ набор от закони е Кодексът на Ур-Наму[1] (наричан също Законник на Ур-Наму), който се смята за един от най-старите писани законници и датира от 2100 г. – 2050 г. пр.н.е. С развитието и усложняването на обществените взаимоотношения съвсем естествено възниква и необходимостта от осъвременяване на възприетите правила и мерки за тяхното регулиране. Така правната теория в древния свят се усъвършенства, като намира израз в няколко сборника от правни текстове – т.нар. кодекси, най-известният от които е Кодексът на Хамурапи. Той представлява набор от 282 закона, издялани върху каменна колона от Вавилонския цар Хамурапи, който завладява и властва над Месопотамия през периода 1792 г. – 1750 г. пр.н.е. Той се състои от икономически разпоредби (цени, тарифи, условия за осъществяване на търговска дейност), семейно право (брак и развод), гражданско право (робство, дълг), наказателно право (нападение, кражба) и т.н. Въпреки че не е първият, това е най-ясно дефинираният и структуриран към онзи момент кодекс, който оказва силно влияние върху законотворчеството и на други общества и култури (von Soden 2000).

Кодексите все още са важен елемент от нашата правна система. Те представляват организационни документи, които имат обект, предмет, цели и обхват и са носители на ценностите на организацията. Кодексите за поведение предоставят насоки относно поведението на членовете на организацията във връзка със специфичен проблем или ситуация. Фокусът на настоящата публикация е насочен към възможността за приемане и присъединяване от страна на висшите училища в България към Кодекс за поведение във връзка с обработването на лични данни в сферата на висшето образование по смисъла на чл. 40 от Общия регламент за защита на личните данни (ОРЗД). Подобен

[1] Ур-Наму е шумерски цар, основател на Третата династия на Ур, управлявала в земите на южна Месопотамия през периода 2119 г. – 2004 г. пр.н.е.

документ би имал значителни ползи за цялата академична общност – както за ръководния и административен състав на висшите училища, така и за ползвателите на образователни услуги в качеството им на субекти на данни.

Изложение

От 25 май 2018 г. във всички държави – членки на Европейския съюз започва прякото прилагане на Регламент (ЕС) 2016/679 на Европейския парламент и на съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни (Общ регламент относно защитата на данните), който задължава всички организации, обработващи лични данни, да приведат дейността си в съответствие с новите нормативни изисквания. С цел осъществяване на основната и спомагателните си дейности и в процеса на предоставяне на образователни услуги на обществеността, висшите училища също събират, съхраняват и обработват лични данни. По този начин, в качеството си на администратори на лични данни, те попадат в обхвата на регулацията и следва да осигурят подходящи нива на защита на данните чрез прилагането на адекватни технически и организационни мерки, възприемайки подход, основан на риска. При вземането на решения в този процес те трябва да отчитат фактори като: технологична обезпеченост; разходи за въвеждане на нови технологии; естество, обхват, контекст и цели на дейностите по обработване на лични данни; опасността от възникване на различни по вероятност и тежест рискове за правата и свободите на субектите на данни и т.н. В резултат на регулацията висшите училища носят отговорност за самооценка и самоопределяне на необходимото ниво на защита на личните данни, като за целта те трябва да отчетат характерните особености на упражняваната от тях дейност.

Настоящата публикация е част от научно изследване (дисертационен труд) в момент на разработка, в което се разглежда възможността за приемане на такъв кодекс, а в практическата си част е изготвено под формата на Проект на кодекс за поведение в сферата на висшето образование, какъвто е предвиден в чл. 40 от ОРЗД. Съгласно критериите и процедурите по одобряване, изменение или допълнение на кодекси за поведение, публикувани на институционалния сайт на Комисията за защита на личните данни (КЗЛД), Кодексът

за поведение е „доброволен инструмент, който има за цел да улесни ефективното прилагане на регламента, както и да спомогне за доказването на факта на спазване на нормативните изисквания в съответствие с принципа на отчетност, като се отчитат особеностите на обработването на данни в определени сектори или професии“. В същия документ се обръща специално внимание и на обстоятелството, че „Кодексът за поведение има добавена стойност само тогава, когато е изготвен специално за конкретен сектор или бранш, отразява неговите особености и съществуващите практики при обработването на лични данни...“ (КЗЛД 2018). Към този момент подобен документ в сферата на висшето образование не е изготвен, което мотивира изследователския интерес в тази посока. Той би имал значителни ползи за цялата академична общност в България и ще послужи не само като набор от вътрешни правила и насоки, но и като външно проявление на споделяните от висшите училища ценности и ангажименти. Преди всичко той би повишил доверието от страна на субектите на данни (студенти, докторанти, специализанти, преподаватели, служители и контрагенти) във връзка с адекватното прилагане на регламента. Също така би осигурил по-голяма степен на правна сигурност, а евентуалното му одобрение от страна на надзорния орган би спомогнало за установяване на единен стандарт в рамките на висшите училища, подобряване на хармонизацията и постигане на съответствие с действащите нормативни изисквания на европейското и националното законодателство в областта на личните данни.

Предмет на Кодекса за поведение следва да бъдат специфичните изисквания и практики в прилагането на Общия регламент относно защитата на данните и на Закона за защита на личните данни в рамките на висшите училища на територията на Република България.

Стремежът е приемането на Кодекс за поведение в сферата на висшето образование да допринесе за постигане на следните основни цели:

• Да предостави на потребителите на образователни услуги инструмент за оценка на нивото на защита на личните данни във висшите училища в страната.

• Да предостави на висшите училища, независимо от тяхната големина или профил, методологически насоки за оценка и постигане на съответствие с европейското и националното законодателство в областта на личните данни.

• Да предостави на висшите училища структуриран механизъм за демонстриране на прозрачност пред надзорните органи и всички други заинтересовани лица в сферата на висшето образование.

За да се очертае обхватът на Кодекса за поведение, е необходимо да се изясни ролята на висшите училища в процеса на събиране, обработване и съхраняване на лични данни, както и тяхното взаимоотношение със субектите на данни. Общият регламент относно защитата на данните прави разлика между *администратор на данни* (страната, която определя целите и средствата за обработване на личните данни) и *обработващ данни* (страна, която обработва лични данни от името на администратора). Същевременно е необходимо да се отчете и възможността за съществуване на по-комплексни ситуации, при които висшите училища възлагат определени дейности по обработване на обработващ данни (услуги от Служба по трудова медицина, обслужване и поддръжка на различни софтуерни приложения, чиито бази данни са достъпни за обработващия данни и т.н.). В определени ситуации самите те биха могли да бъдат в качеството си на обработващи или съвместни администратори (например при партньорства с други университети при изпълнението на различни програми и проекти).

Ролята на висшите училища в процеса на събиране, обработване и съхраняване на лични данни следва да се разглежда в контекста на осъществяваните от тях дейности. Изпълнението им е необходимо за нормалното протичане на учебния процес и те могат условно да бъдат категоризирани като основни и спомагателни. Основните дейности са предимно свързани с основните структурни звена (факултети) на съответното висше училище и обхващат учебно-преподавателската, научноизследователската, художественотворческата дейност и т. н. Спомагателните дейности се извършват от административните и обслужващите звена (отдели и центрове) и към тях могат да бъдат отнесени административно-стопанската дейност, финансово-счетоводната дейност, библиотечната и издателската дейност, управлението на човешките ресурси, охраната и видеонаблюдението и т.н.

Дефинирането на ролята на висшите училища в контекста на осъществяваните от тях дейности позволява по-лесното идентифициране на изискванията на приложимото законодателство в областта на личните данни и изясняване на отговорностите по отношение на тяхното прилагане. Един от основните стремежи е чрез изготвянето

на Кодекс за поведение да бъдат адресирани тези изисквания, като същевременно самият той следва да бъде периодично преразглеждан и при необходимост – актуализиран, отразявайки настъпилите промени в европейското и националното законодателство. В частност това включва Общия регламент относно защитата на данните и Закона за защита на личните данни в Република България. В него също следва да бъдат описани възможните регистри и съдържащите се в тях категории лични данни, както и целите, сроковете и правните основания за обработването им. Той трябва да съдържа общи критерии и механизми за извършване на оценка на риска и оценка на въздействието върху защитата на данните (ОВЗД), възможни технически и организационни мерки за защита, както и условията за тяхното прилагане. В него следва да фигурират и основните процедури и механизми за работа с личните данни, като се приложат образци на документи, които биха улеснили работата на висшите училища в процеса на тяхното администриране.

Подобен документ може условно да бъде разделен на два основни компонента. Първият компонент е практическият, който може да бъде разгледан като своеобразен технически стандарт, включващ набор от методологически насоки, мерки и процедури, които трябва да бъдат внедрени от присъединилите се към Кодекса за поведение висши училища, за да могат да постигнат съответствие с изискванията на ОРЗД. Вторият компонент е управленската структура, в която е описана дейността на акредитирания орган по наблюдение за спазването на Кодекса за поведение, критериите за присъединяване към него, описание на механизмите за присъединяване, прекратяване и временно спиране на присъединяването към кодекса, както и механизмите за извършване на задължително наблюдение за спазване на неговите разпоредби от висшите училища, които приемат да го прилагат.

Специфично ограничение за публичния сектор е забраната за определяне на акредитиран орган по наблюдение за спазването на съответния Кодекс за поведение. Освен това към момента съществуват и други правни ограничения по отношение на акредитирания орган по наблюдение, на които следва да се обърне внимание. Наличието на наблюдаващ орган по смисъла на чл. 41 от ОРЗД е задължително условие за окончателното одобряване на Кодекс за поведение, а правомощието да акредитира такъв орган има КЗЛД. В същото време, по

силата на чл. 41, пар. 3 от ОРЗД, проектокритериите за акредитацията му следва да бъдат одобрени от Европейския комитет по защита на данните (ЕКЗД) в съответствие с механизма за съгласуваност. Поради тази причина към настоящия момент съществува обективна пречка за формално одобряване на кодекси за поведение от страна на КЗЛД. Въпреки това, отчитайки значителния обществен интерес към този доброволен, но изключително полезен инструмент за практическото прилагане на ОРЗД, в свое становище от 22.02.2019 г. надзорният орган възприема принципен подход към представените за одобрение проекти на кодекси за поведение. Позицията на Комисията е, че „с цел придаване на положителна динамика на процеса при пълно зачитане на актуалната нормативна рамка [...] единствената възможност да се продължи работата по проектите на кодекси за поведение е КЗЛД да вземе отношение само по съдържанието на съответния кодекс, на основата на нормативните изисквания в чл. 40 от Регламент (ЕС) 2016/679 и критериите на КЗЛД, при отчитане и на Насоките на ЕКЗД, без да прави оценка на този етап на предложения наблюдаващ орган“ (КЗЛД 2019). Поради тази причина е разумно към настоящия момент фокусът да бъде съсредоточен върху методологическите насоки без да се засягат функциите и структурата на наблюдаващия орган.

Заключение

Кодексът за поведение във връзка с обработването на лични данни в сферата на висшето образование е необходим и изключително полезен инструмент. Той би позволил на ръководния и административния състав, както и на длъжностните лица по защита на данните, своевременното идентифициране на присъщите за висшите училища рискове, както и предприемането на подходящи действия за тяхното ограничаване. Съдържащите се в него предварително установени критерии, процедури и правила биха утвърдили единен стандарт при работа с личните данни и биха послужили като ориентир при вземането на ръководни решения в този процес. Също така той би осигурил високо ниво на защита на личните данни на студенти, преподаватели и служители, ангажирани в сферата на висшето образование в качеството им на субекти на данни.

Въпреки че Кодексът за поведение може да бъде важна стъпка

към удовлетворяване на изискванията на европейското и националното законодателство в областта на личните данни, той не е цялостно решение сам по себе си. Ефективното му прилагане трябва да се извършва последователно, изисква процес на запознаване с неговите принципи, а самият той трябва непрекъснато да бъде преразглеждан и усъвършенстван. Стремежът е изготвянето на Проект на Кодекс за поведение да послужи като основа за иницииране на дискусия между заинтересованите страни и лица, при необходимост да бъде допълнен и изменен, а впоследствие да бъде внесен за одобрение от надзорния орган.

Използвана литература

Закон за защита на личните данни (ЗЗЛД). // ДВ, №.1, 2002, (https://lex.bg/laws/ldoc/2135426048, 18.09.2021).

Комисия за защита на личните данни (КЗЛД). Критерии и процедури по одобряване, изменение или допълнение на Кодекси за поведение, (https://www.cpdp.bg/?p=element&aid=1167, 22.09. 2021).

Комисия за защита на личните данни (КЗЛД). Становище на Комисията за защита на личните данни рег. № НДМСПО-17-723/2018 г., гр. София, 22.02.2019 г., (https://www.cpdp.bg/index.php?p=element&aid=1192, 20.09.2021).

Регламент (ЕС) 2016/679 на Европейския парламент и на 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 относно защитата на данните), (https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434, 18.09.2021).

von Soden, W. History of Mesopotamia, (https://www.britannica.com/place/Mesopotamia-historical-region-Asia, 18.09.2021).

За контакти: докторант Горан Проданов
Шуменски университет „Епископ Константин Преславски“
e-mail: g.prodanov@shu.bg

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 спазят 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

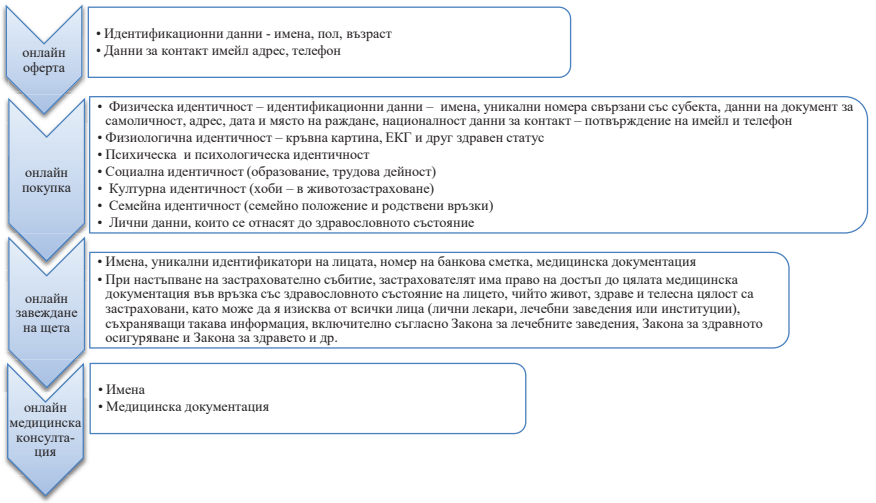
и съхранението на данни за дигитална продажба и след продажбено обслужване на медицински застраховки.

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, чиито 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 основанието за законосъобразно обработване на лични данни

Цели за обработването на лични данни на основание законови задължение	• Комплексна проверка (идентификация, верификация и приемане) на ползватели на застрахователни услуги • Изготвяне на отчети до регулаторни органи • Докладване до регулаторни органи съгласноразпоредбите 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	• Оценка на застрахователния риск и изчисляване на застрахователната премия • Изготвяне на индивидуално предложение за сключване на застраховка • Изготвяне на застрахователен договор и изпълнение на законовите задължение 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 обработването на лични данни на основание законни интереси на администратора	• 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	• 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).

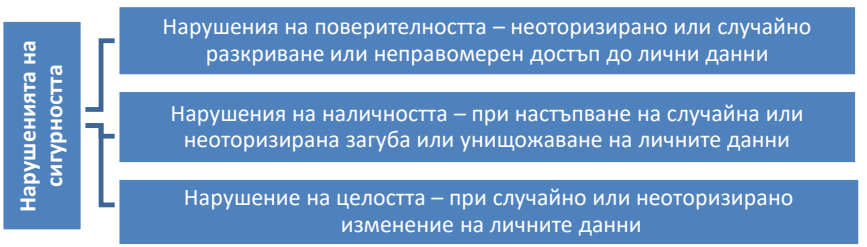
С цел директен маркетинг и предлагане на персонални продукти и услуги, посредством изготвяне на точен клиентски профил, е необходимо потенциалните и настоящите клиенти да дадат свободно изрично писмено съгласие на застрахователя да обработва личните данни при строга конфиденциалност и в съответствие 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 неправомерен 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 информирано 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 заплахи, 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.

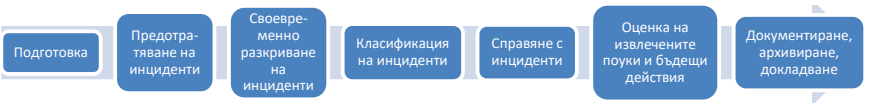
Източник: 2020 Harvey Nash/KPMG CIO Survey, KPMG International.

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

[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.

Заключение

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 подобрение 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., „Boyanov 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/resourses/world-insurance-report-2019, 15.05.2021).

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

ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ И ДИГИТАЛИЗАЦИЯТА – ПРЕДИЗВИКАТЕЛСТВА И ПЕРСПЕКТИВИ

Сборник с доклади

Редактор *Анелия Герчева*

Дадена за печат XI.2021 г. Излязла от печат XII.2021 г.
Печатни коли 11,9 Издателски коли 10,7
Формат 60x90/16 Тираж 120

Предпечатна подготовка *Екатерина Йорданова*
Издателство „Наука и икономика“
Икономически университет – Варна
ул. „Евлоги Георгиев“ 24
Печатна база на ИУ – Варна

ISBN 978-954-21-1002-3