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 реструктурира, 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 с 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 ѝ помага в постигане 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 заложили 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 – ИА). 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 (Auranci 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 създава 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 въткан 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