НАСОКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ЗА ОДИТОРИ

проф. д-р Али Вейсел

Дипломиран експерт-счетоводител,
регистриран одитор,
Преподавател във ВУЗФ – София

Ключови думи:

Лични данни

Общ регламент относно защитата на данните

Международни одиторски стандарти

Одитна документация

JEL: M42, M48

Резюме

В статията се изследват насоките за защита на личните данни за одитори на ICAEW (Института на дипломираните експерт-счетоводители в Англия и Уелс). Анализират се основните разпоредби на Общия регламент относно защита на данните (GDPR), включително приложимите облекчения. Набляга се на документирането на извършените процедури, както и на разработването на вътрешни правила за спазване на нормативните изисквания.

Регистрираните одитори са експерти по счетоводство и одит. Те трябва да изпълняват своите отговорности чрез използване на знанията си по счетоводните и одиторските стандарти. Прилагат се и други познания – по търговско, данъчно и осигурително законодателство, количествени методи, управленски, организационни и бизнес познания, умения по информационни технологии и други. Те са необходими за упражняването на професията. Но освен това постепенно се увеличават допълнителните задължения на одиторите. Сред тях са мерките за защита на личните данни, които са изключително актуални през последните години. Интересно е обаче, че те се представят от повечето „консултанти“ по начин, който създава впечатлението, че с новите изисквания основната дейност на одиторите (както и на повечето професии) ще бъде защита на данните. Така „от дърветата не може да се види гората“. Необходимо е разпоредбите да се представят в контекста на одита. За целта може да се анализират разработките по тези въпроси на професионалните организации на одиторите.

Международната федерация на счетоводителите няма публикувани материали за защита на личните данни. Но в интернет страницата на организацията може да се намери новина за публикувани

насоки от ICAEW (Института на дипломираните експерт-счетоводители в Англия и Уелс).[1]

В тези **насоки**[2] накратко са изяснени разпоредбите за защита на личните данни и са посочени основните изисквания, които имат значение за одиторите в Европейския съюз. Те представляват интерес и за българските одитори.[3] Към тях могат да се добавят някои допълнителни пояснения и примерни процедури, които могат да се използват на практика.

Задълженията за защита на личните данни са по ***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),[4] който е в сила от 25.05.2018 г. и е по-известен като GDPR (от наименованието на английски език – General Data Protection Regulation). За неговото разбиране е важно да се има предвид, че той **не поражда нови отговорности**, не създава нов подход, а представлява преработка на съществуващи разпоредби на Европейския съюз. Тези въпроси са обект на регламентиране от 1995 г. с *Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни.*[5] Българският *Закон за защита на личните данни* е в сила от 01.01.2002 г.[6] Целта на актуализацията е да се отговори на промените в технологията и използването на данните през последните двадесет години.[7] Според ICAEW регламентът не води до значителна промяна в „правилата на играта“, но той е **по-строг** и глобите за неспазване са значително увеличени. Затова е наложително да се вземат мерки от одиторите.

Одиторите са **администратори на лични данни**, защото определят целите и средствата за обработването на **лични данни** (всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, т.е. „субект на данни“).[8]

---

[1] https://www.ifac.org [Accessed September 23, 2020].

[2] GDPR for accountants: your questions answered. A GDPR Checklist, June 2018, ICAEW, https://www.icaew.com [Accessed September 23, 2020].

[3] През 2018 г. е представен проект на *Института на дипломираните експерт-счетоводители* в България (ИДЕС) за *примерни вътрешни правила за мерките за защита на личните данни, съгласно Регламент 2016/679*, който е използван в настоящото изследване. Проектът не е публикуван в окончателен вид.

[4] ОВ L 119/1, 04.05.2016 г.

[5] ОВ L 281, 23.11.1995 г., с. 31.

[6] Закон за защита на личните данни. В сила от 01.01.2002 г. Обн., ДВ, бр. 1 от 4 януари 2002 г., посл. изм., ДВ, бр. 93 от 26 ноември 2019 г.

[7] В условията на дигитализация все по-голямо значение има защитата на данните, особено в сферата на финансовите услуги, вж. Dimitrov St., Innovations in life insurance – the Bulgarian market and what to expect, VUZF Review, v.1, 2018, pp. 34 – 43.

[8] За преглед на понятието лични данни, примерни злоупотреби и други вж. Банкова, Д. За имплементирането на регламента за защита на лични данни в одиторската практика, списание ИДЕС, бр. 4/2018.

Затова според професионалната организация на Англия и Уелс трябва да се спазват насоките в следните области:

- определяне на лице, отговарящо за защита на личните данни;
- преглеждане и актуализиране на съществуващите мерки за защита на данните и мерките за киберсигурност;
- „картографиране“ на данните;
- преглед на договорите с клиенти, доставчици и служители;
- разработване на политики за защита на личните данни;
- обучаване на служителите.

Тези области са обект на разглеждане по-долу.

1. Определяне на лице, отговарящо за защита на личните данни

Регламентът изисква да се определя длъжностно лице по защита на данните, когато:[9]

а) обработването на лични данни се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;

б) дейностите по обработване изискват редовно и систематично мащабно наблюдение на субектите на данни; или

в) дейностите по обработване включват специалните категории данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице, и на лични данни, свързани с присъди и нарушения.

За целите на одита не е необходимо да се събират и обработват такива данни. Затова в своите вътрешни правила одиторът може да посочи следното:

> Одиторът не събира данни, отнасящи се до расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице, и на лични данни, свързани с присъди и нарушения.

[9] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година, чл. 37, т. 1.

Така одиторът няма задължение да определя длъжностно лице по защита на личните данни. Въпреки това обаче е по-добре да се определи отговорник. Самостоятелно практикуващите одитори, с по-малко служители, могат да поемат лично тези функции.

2. Преглеждане и актуализиране на съществуващите мерки за защита на данните и мерките за киберсигурност

Одиторите трябва да преглеждат съществуващите мерки за сигурност и да ги изменят или актуализират. Това се прави както при въвеждането на Регламента, така и периодично. Необходимо е вътрешните правила да включват изисквания в това отношение, например следните процедури:

Одиторът прилага следните мерки за защита на данните:

а) технически мерки за защита:

- използват се подходящи шкафове и каси, които позволяват строго ограничен достъп до съхраняваните в тях документи и технически носители;
- използва се подходяща сигнално-охранителна техника;
- предприемат се мерки за противопожарна охрана на документите и техническите носители;

б) мерки за защита на документите:

- получаването, обработването и съхранението на хартиените носители се извършва само от регистрирания одитор и другите одитори, които работят по ангажимента;
- документите се съхраняват на места, които ограничават достъпа на неоторизирани лица;
- документите се изваждат от специалните места за съхранение само когато това е необходимо за тяхната обработка; веднага след това те се връщат в мястото на съхранение;
- документите не се оставят без надзор или по начин, който би позволил визуален достъп от неоторизирани лица;

в) мерки за защита на информационните технологии:

- всички получени от външни източници данни в електронен формат се проверяват за наличието на вируси;
- информацията не се съхранява на сървъри, до които има широк достъп;
- достъпът до техническите средства е строго регламентиран;
- използваните софтуери не позволяват неоторизиран достъп до информацията в тях, както и неоторизирано копиране на бази с данни;
- винаги се използват пароли, известни само на лицето, което има право да изготвя и обработва работните документи.

Регламентът не задължава криптирането на личните данни. Трябва обаче да 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.[10]

Относно криптирането може да се посочат следните изисквания към мерките за защита на информационните технологии:

- файловете, прикачени към електронните пощи, задължително се криптират;

- ключовете за декриптиране се уговарят устно или се изпращат отделно.

Периодичният преглед трябва да се извърши при оценка на състоянието и целостта на личните данни съгласно следващата точка.

3. „Картографиране“ на данните

Чрез „картографиране“ се установява движението на всеки поток от информация. Оценява се какви лични данни се събират, как се обработват, как и колко дълго се съхраняват, на кого се предоставят и кога се унищожават.

Регламентът изисква при **събиране** на лични данни да се получи изрично подписано съгласие от субекта на данни и да му се предостави уведомление за дейността по обработване на личните данни, в което се посочват правата на субекта.

Когато се събират данни по изискване на нормативен акт, включително *Международни одиторски стандарти* (МОС), няма задължение за получаване на съгласие. В тези случаи данните се събират за целите на ангажимента, при спазване на изискванията за защита на личните данни. Затова във вътрешните си правила одиторът може да посочи, че събира и обработва само такива данни, които са необходими за постигане на законосъобразните цели.

При спазване на изискванията за мерки срещу изпирането на пари и финансирането на тероризма не е необходимо да се получава съгласие на субекта на данните и да му се предостави уведомление за дейността по обработването.[11]

В това отношение вътрешните правила могат да включват следния текст:

Одиторът събира само такива лични данни, които са необходими за постигане на законосъобразни цели на одиторския ангажимент, вкл. относно мерките срещу изпирането на пари и финансирането на тероризма.

---

[10] Пак там, чл. 32, т. 1.

[11] Закон за мерките срещу изпирането на пари. Обн., ДВ, бр. 27 от 27 март 2018 г., посл. изм. и доп., ДВ, бр. 69 от 4 август 2020 г., чл. 83, ал. 2.

Възможно е одиторът да получи лични данни без правно основание. В тези случаи в срок един месец от узнаването документите се връщат, а ако това е невъзможно или изисква несъразмерно големи усилия, се изтриват или унищожават по реда за унищожаване на лични данни.

Обработването на личните данни трябва да се извършва при спазването на следните задължителни минимални условия:

- обработват се от ограничен кръг оторизирани служители;
- обработват се по начин, който предотвратява достъпа до тях от неоторизирани служители и тяхното неправомерно разпространение;
- обработват се само такива данни, които са необходими за постигане на законосъобразни цели за конкретния случай.

Те са свързани с процедурите за събиране и мерките за защита на личните данни. Затова не водят до нови задължения. Но когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, одиторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.[12]

Данните трябва да се **съхраняват** чрез прилагане на мерките за защита, представени по-горе. Сроковете зависят от целите на тяхното събиране, с изключение на случаите, когато се определят от нормативен акт. Тук трябва да се имат предвид изискванията на *Закона за независимия финансов одит* и МОС, че одитната документация се съхранява за срок 5 години след датата на одиторския доклад.[13] Но за документите на одитора трябва да се прилагат и другите законови разпоредби, например:

- съгласно *Закона за счетоводството* ведомостите за заплати се съхраняват 50 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят;[14]
- съгласно *Данъчно-осигурителния процесуален кодекс* документи за данъчно-осигурителен контрол се съхраняват 5 години след изтичане на давностния срок за погасяване на публичното задължение, с което са свързани.[15]

В случаите на набиране и подбор на персонал одиторът трябва да спазва следните изисквания за съхранение:

---

[12] Банкова, Д. За имплементирането на регламента за защита на лични данни в одиторската практика, списание ИДЕС, бр. 4/2018, с. 8.

[13] Закон за независимия финансов одит. Обн., ДВ, бр. 95 от 29 ноември 2016 г., посл. изм. и доп., ДВ, бр. 18 от 28 февруари 2020 г., чл. 31, ал. 1, т. 10.

[14] Закон за счетоводството. В сила от 01.01.2016 г. Обн., ДВ, бр. 95 от 8 декември 2015 г., посл. доп., ДВ, бр. 26 от 22 март 2020 г., чл. 12, ал. 1, т. 1.

[15] Данъчно-осигурителен процесуален кодекс. В сила от 01.01.2006 г. Обн., ДВ, бр. 105 от 29 декември 2005 г., посл. изм. и доп., ДВ, бр. 69 от 4 август 2020 г., чл. 38, ал. 1, т. 3.

- данните се съхраняват в срок не по-дълъг от шест месеца след окончателното приключване на подбора, освен ако кандидатът е дал своето съгласие за съхранение за по-дълъг срок в случаите на участие в следващ подбор;
- след изтичането на установения срок одиторът унищожава съхраняваните документи с лични данни.

Относно сроковете за съхранение във вътрешните правила може да се посочи следното:

Личните данни се съхраняват според сроковете за съхраняване на одитна документация съгласно *Закона за независимия финансов одит* и съгласно сроковете *по Закона за счетоводството* и *Данъчно-осигурителния процесуален кодекс.* При набиране и подбор на персонал данните се съхраняват в срок не по-дълъг от шест месеца след окончателното приключване на подбора, освен ако кандидатът е дал своето съгласие за съхранение за по-дълъг срок в случаите на участие в следващ подбор.

Личните данни могат да се **предоставят на субекта на данни и на трети лица**, при изпълнение на целите, за които са събрани, според изискванията на нормативните актове. В тази връзка във вътрешните правила на одитора може да се посочи следното:

Субектът на данни има право на достъп до неговите лични данни, съхранявани от одитора, включително и да иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него. Правото се упражнява чрез подаване на заявление до одитора. Това право не може да се използва, когато за това са налице законови ограничения, например по *Закона за мерките срещу изпирането на пари.*

В срок от 10 работни дни от получаване на искането одиторът писмено уведомява субекта на данни дали са налице законовите основания за уважаване на искането. Ако установи, че са налице законовите основания да уважи искането, одиторът предоставя информацията.

Третите лица, получатели на лични данни, съгласно законовите изисквания, са длъжни да декларират писмено пред одитора, че ще спазват изискванията на нормативните актове, уреждащи материята.

Периодично се извършва оценка на състоянието и целостта на личните данни. В случаите, в които се налага унищожаване на носител на лични данни, се прилагат необходимите действия за заличаването на личните данни. Данните на електронен носител се **унищожават** чрез трайно изтриване. Хартиените носители се унищожават чрез нарязване или изгаряне. Тези процедури трябва да се документират, като се посочат следните изисквания във вътрешните правила:

Най-малко веднъж годишно одиторът извършва оценка на състоянието и целостта на личните данни.

В случаите, в които се налага унищожаване на носител на лични данни, се прилагат необходимите действия за заличаването на личните данни по начин, изключващ възстановяване на данните и злоупотреба с тях.

Данните на електронен носител се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите.

Хартиените носители се унищожават чрез нарязване или изгаряне.

Унищожаването се осъществява само от одитора по начин, по който се предотвратява предварителното копиране или разпространение на информацията.

За оценката и унищожаването се съставя ***протокол за оценка на състоянието и унищожаване на лични данни*** със следните реквизити: номер; дата; констатирани налични данни с рискове за тяхното правилно съхраняване; мерки за минимизиране на риска; констатирани данни, които не следва да бъдат съхранявани (описват се категориите данни и причините, поради които данните следва да бъдат унищожени); категории данни, които подлежат на унищожение; количество и субекти на данните, които подлежат на унищожаване; начини за унищожаване на данните; опис на останалите документи след унищожаване на данните; приложения; подпис на одитора.

Дейностите по обработка на личните данни се посочват в ***регистри***, които трябва да съдържат минимум следната информация:

- името и координатите за връзка на администратора и длъжностното лице по защита на данните;
- целите на обработването;
- описание на категориите субекти на данни и на категориите лични данни;
- категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
- когато се изисква, начина на предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация;
- предвидените срокове за съхранение и унищожаване на различните категории данни;
- общо описание на техническите и организационни мерки за сигурност.

Може да се поддържат регистри, например за служителите и контрагентите.

Задължението за регистри не се прилага по отношение на предприятие с по-малко от 250 служители, освен ако има вероятност извършваното от тях обработване да породи риск за правата и свободите на субектите на данни, ако обработването не е спорадично или включва специални категории данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице, и на лични данни, свързани с присъди и нарушения.

4. Преглед на договорите с клиенти, доставчици и служители

Договорите, които подписват одиторите, също трябва да съответстват на мерките за защита на личните данни.

В договора за одит (писмото за поемане на ангажимент) одиторът може да посочи, че декларира своето задължение за спазване на изискванията за защита на личните данни. Това може да се направи със следния текст:

> Одиторът събира и обработва лични данни, които са необходими за изпълнение на задълженията по спазването на нормативните актове и *Международните одиторски стандарти.*
>
> Личните данни се събират, обработват, съхраняват и унищожават при строго съблюдаване на изискванията за защитата на личните данни, вкл. сроковете за съхраняване на одитна документация съгласно Закона за независимия финансов одит. Отговорността за тези дейности е на одитора.

Необходимо е да се прегледат и договорите с доставчици, например за доставка на облачни (cloud) услуги. Много от тези доставчици съхраняват данните извън Европейския съюз. Затова трябва да се установи дали спазват изискванията на регламента.

Относно служителите трябва да се определят данните, които трябва да се събират съгласно българското законодателство.[16] Например в трудовия договор се включват имената на работника, единен граждански номер, постоянен адрес, вид и степен на притежаваното образование. По закон не се изисква да се посочва номерът на личната карта, от кого е издадена и кога изтича. Не се изисква и личните карти да се съхраняват в трудовите досиета.

Ако одиторът изисква допълнителни данни, той трябва да получи съгласието на лицето, като предостави на субекта на данни уведомление за дейността по обработване на личните данни, което включва:

- личните данни, които се събират, обработват и съхраняват;

[16] Какви лични данни имат право да обработват работодателите? 21.07.2017, https://www.economy.bg/ [Дата на достъпа: 25.09.2020 г.].

- целите за обработване на личните данни;
- основанието за обработване на личните данни;
- крайния срок за съхранение на личните данни;
- правата на субекта на данни (когато не са забранени от нормативен акт): получаване на информация кои лични данни са събрани, обработвани и съхранявани, оттегляне на съгласие за обработване и съхранение на личните данни, възможност за изискване да се коригират или изтрият, или да се ограничи обработването на личните данни; възразяване срещу определен начин на обработване на личните данни.

5. Разработване на политики за защита на личните данни

Регламентът въвежда принципа на отчетност. Това означава, че всички задължени лица трябва да са в състояние да доказват спазването на изискванията чрез документиране на политиките и процедурите. За целта трябва да се разработят **вътрешни правила**.

В тази връзка трябва да се има предвид, че одиторите поддържат система за контрол върху качеството, която трябва да осигурява разумна степен на сигурност, че се спазват професионалните стандарти и приложимите правни и регулаторни изисквания. Не е необходимо за прилагането на всеки закон или регламент да се приемат вътрешни правила като отделен документ. Те трябва да се включват в системата за контрол върху качеството.

Вътрешните правила относно защитата на лични данни, включени в системата за контрол върху качеството, следва да съдържат разгледаните по-горе:

- определяне на лице, отговарящо за защита на личните данни;
- мерки за защита на личните данни;
- изискванията за събиране, обработване, съхраняване, предоставяне и унищожаване;
- изисквания за подписване на договори с клиенти, доставчици и служители.

Освен това те трябва да регламентират процедурите при **нарушения**. Всяко отклонение от изискванията за защита на личните данни се документира. Предприемат се и мерки за елиминиране на възможностите за извършване на други подобни грешки. Когато нарушението може да доведе до риск за правата и свободите на субектите на данни, се уведомява *Комисията за защита на личните данни.*

Тези изисквания могат да се посочат във вътрешните правила по следния начин:

Отклоненията от изискванията за защита на личните данни, включително фактите, свързани с нарушението на сигурността, последиците от него и предприетите действия за справяне с него, се документират.

Предприемат се и мерки за елиминиране на възможностите за извършване на други подобни нарушения на защита на личните данни.

В случай на нарушение на сигурността на личните данни, което има вероятност да доведе до риск за правата и свободите на субектите на данни, одиторът без излишно забавяне, но не по-късно от 72 часа, след като е разбрал за нарушението, уведомява *Комисията за защита на личните данни*. Когато уведомлението е подадено след този срок, в него се посочват причините за забавянето.

За документиране на нарушението се изготвя ***протокол за установяване на нарушения за сигурността на личните данни*** със следните реквизити: номер; дата; открито нарушение; лице, което е разкрило нарушението; причини за извършване на нарушението; начин за осъществяване на нарушението; последствия от извършеното нарушение; количество и категории данни и засегнати субекти от нарушението; уведомяване на Комисията за защита на личните данни и субекта на данни; необходимост от преглед на вътрешните правила за защита на личните данни; приложения; подпис на одитора.

Правилата трябва да включват и изисквания за мониторинг, за да се гарантира, че съществуващите политики и процедури се следват, актуализират и допълват при необходимост. За тази цел може да се използва оценката за състоянието и целостта на личните данни, която се документира с ***протокола за оценка на състоянието и унищожаване на лични данни***. Всички протоколи трябва да се прилагат към системата за контрол върху качеството.

6. Обучаване на служителите

Редовното обучение на служителите е от решаващо значение за предприятията. То е важно за промяна на „знанията, уменията, поведенията и нагласите“[17]. Пропуските в това отношение могат да водят до съществени загуби. Затова и служителите, които изпълняват задълженията за защита на личните данни, следва да се запознаят с нормативната уредба в тази област. Необходимо е този процес да се документира. Не всички служители обаче трябва да разбират всички изисквания. Затова за някои обучението може да бъде ограничено.

Направеното изследване за насоките на ICAEW за защита на личните данни позволява да се **обобщи**, че одиторите трябва да вземат мерки за спазване на изискванията на *Регламент (ЕС) 2016/679*. Те са свързани със събиране, обработване, съхраняване, предоставяне и унищожаване на лични данни. Договорите с клиенти, доставчици и служители също

[17] Пейчева, М. Управление на човешките ресурси. София, Тракия-М, 2012, с. 140.

трябва да се съобразят с тези разпоредби. Има редица облекчения, които могат да се използват от одиторите. Трябва да се документират процесите и да се разработват вътрешни правила като част системата за контрол върху качеството.

Библиографска справка:

1. *Банкова, Д. За имплементирането на регламента за защита на лични данни в одиторската практика, списание ИДЕС, бр. 4/2018.*
2. *Данъчно-осигурителен процесуален кодекс. В сила от 01.01.2006 г. Обн., ДВ, бр. 105 от 29 декември 2005 г., посл. изм. и доп., ДВ, бр. 69 от 4 август 2020 г.*
3. *Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 23.11.1995 г., с. 31).*
4. *Закон за защита на личните данни. В сила от 01.01.2002 г. Обн., ДВ, бр. 1 от 4 януари 2002 г., посл. изм., ДВ, бр. 93 от 26 ноември 2019 г.*
5. *Закон за мерките срещу изпирането на пари. Обн., ДВ, бр. 27 от 27 март 2018 г., посл. изм. и доп., ДВ, бр. 69 от 4 август 2020 г.*
6. *Закон за независимия финансов одит. Обн., ДВ, бр. 95 от 29 ноември 2016 г., посл. изм. и доп., ДВ, бр. 18 от 28 февруари 2020 г.*
7. *Закон за счетоводството. В сила от 01.01.2016 г. Обн., ДВ, бр. 95 от 8 декември 2015 г., посл. доп., ДВ, бр. 26 от 22 март 2020 г.*
8. *Какви лични данни имат право да обработват работодателите? 21.07.2017, https://www.economy.bg/ [Дата на достъпа: 25.09.2020 г.].*
9. *Пейчева, М. Управление на човешките ресурси. София, Тракия-М, 2012.*
10. *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) [ОВ L 119/1, 04.05.2016 г.].*
11. *Dimitrov, St. Innovations in life insurance – the Bulgarian market and what to expect, VUZF Review, v.1, 2018, pp. 34 – 43.*
12. *GDPR for accountants: your questions answered. A GDPR Checklist, June 2018, ICAEW, https://www.icaew.com [Accessed September 23, 2020].*
13. *https://www.ifac.org [Accessed September 23, 2020].*

GUIDELINES FOR DATA PROTECTION FOR AUDITORS

Prof. Ali Veysel, PhD
Certified Public Accountant
Registered Auditor
Lecturer at VUZF University – Sofia

Keywords:

Personal Data

General Data Protection Regulation (GDPR)

International Standards on Auditing

Audit Documentation

Summary

The article examines the guidelines for data protection for auditors of ICAEW (Institute of Chartered Accountants in England and Wales). The main provisions of the General Data Protection Regulation (GDPR), including the applicable reliefs, are analyzed. Emphasis is placed on documenting the performed procedures, as well as on developing internal rules for compliance with regulatory requirements.