ЗА ИМПЛЕМЕНТИРАНЕТО НА РЕГЛАМЕНТА ЗА ЗАЩИТА НА ЛИЧНИ ДАННИ В ОДИТОРСКАТА ПРАКТИКА

Д-р Дияна Банкова
Асистент одитор
Мур Стивънс България – Одит ООД
diyanabankova@gmail.com

Ключови думи:
Лични данни
Измами
Одит
Политика по GDPR

Резюме

Статията има за цел да изследва значението на политиката за защита на лични данни. В нея се представят някои примери за злоупотреби с лични данни, на които одиторите трябва да обръщат внимание.

Представят се варианти за разработването и внедряването на политики и процедури съгласно General Data Protection Regulation (GDPR) в одиторските дружества.

Възникнаха редица въпроси в одиторската общност по отношение на това как трябва да се разработва и внедрява политика съгласно *Регламента за защита на лични данни*. Какво точно представляват личните данни и финансовите данни също ли са лични данни? Тези неизвестности като цяло засегнаха и бизнеса, а те от своя страна отправиха запитванията си по тази тема към одиторите.

Целта на настоящата статия е да се изясни конкретно значението на понятието „лични данни“, какви ангажиментите имат одиторите към *Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година (GDPR)*, както и към *Закона за защита на лични данни (ЗЗЛД)* в България; да се представят някои примери за злоупотреба с лични данни и последиците от тези събития, както и какво може да включват в своята политика по защита на лични данни одиторите. Това може да се осъществи с изпълнението на следните **задачи**:

- ✓ терминологичен преглед на понятието „лични данни“;
- ✓ примери за злоупотреба с лични данни;
- ✓ модел на политика за защита на лични данни.

Поради неяснотите, свързани със значението на „личните данни”, е необходимо да се извърши терминологичен преглед на това понятие. Съгласно отговор на *Европейската комисия (ЕК)* „***лични данни***“ − „са всяка информация, свързана с **идентифицирано или идентифицируемо живо физическо лице.**

Отделни данни, които, когато се съберат заедно, могат да доведат до идентифициране на конкретно лице, също представляват лични данни“[1].

Съгласно посочения отговор от ЕК „лични данни, които са били деидентифицирани, кодирани или **псевдонимизирани**, но могат да бъдат използвани за повторно идентифициране на дадено лице, остават лични данни“[2] и отговарят отново на изискванията към *Общия регламент за защита на лични данни (ОРЗД)*.

Лични данни, които са **анонимни** и лицето не може да бъде идентифицирано чрез тях, от този момент не се считат за лични данни. Освен това друга специфика, свързана с личните данни, е техният веществен характер, които могат да бъдат – автоматично или ръчно въвеждани и съхранявани в дигитална система или на хартия.

„Примерите за лични данни включват:

- ✓ собствено име и фамилия;
- ✓ домашен адрес;
- ✓ имейл адрес, като например име.фамилия@дружество.com;
- ✓ номер на картата за самоличност;
- ✓ данни за местоположение (напр. функцията за данни за местоположение на мобилен телефон)*;
- ✓ интернет адрес (IP);
- ✓ данни, съхранявани от болница или лекар, които биха могли да бъдат символ, който идентифицира дадено лице“[3].

В тази връзка е важно да се представи и нормативната дефиниция, посочена в *чл. 2, ал. 1 от Закона за защита на личните данни (ЗЗЛД)*[4], а именно – съгласно българското законодателство **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“[5].

Позицията на C*loud Services Company Boxcryptor*[6] е, че за лични данни могат да се считат:

[1] Какво означава „лични данни“?, източник: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_bg>, последно влизане на: 25.10.2018/14:38.
[2] Пак там.
[3] Пак там.
[4] Закон за защита на личните данни, обн., ДВ, бр. 1 от 4 януари 2002 г., последно изм., ДВ, бр. 7 от 19 януари 2018 г.
[5] Пак там.
[6] Компания, която се занимава с криптирането и съхраняването на информация в облачно пространство (Cloud Services).

- ✓ „**Биографична информация или текущо състояние на живот**, включително дати на раждане, номера за социално осигуряване, телефонни номера и имейл адреси;
- ✓ **Визия, външен вид и поведение**, включително цвят на очите, тегло и характерни черти;
- ✓ **Данни за работното място и информация за образованието**, включително заплата, данъчна информация и факултетни номера;
- ✓ **Частни и субективни данни**, включително религия, политически възгледи;
- ✓ **Информация, свързана със здравния статут и генетика**, включително медицинска история, генетични данни и информация за използван отпуск по болест“[7].

Друго любопитно мнение е посочено от https://www.cnil.fr, свързано с дефинирането на понятието „**лични данни**“. Според този източник те могат да бъдат данни, които не са свързани пряко с името на дадено лице, но могат да послужат за неговото идентифициране. Примерите са следните: „притежателят на номер 01 53 73 22 00 често се обажда в Сенегал“ или „собственикът на превозно средство с номер 3636AB75 се абонира за списание“ или „социално осигуреното лице с № 1600530189196 посещава лекар повече от веднъж месечно“[8].

Мненията, анализите и хипотезите на понятието „*лични данни*“ могат да продължат да бъдат изследвани, но по-важното е, че с въвеждането на *Регламента* се въвеждат промени по отношение на политиките, които трябва да се спазват от лицата, използващи лични данни, в т.ч. и от одиторите.

В обобщение на терминологичния преглед на това широкообхватно понятие „*личните данни*” представляват – информация, свързана с физическо лице или „субект на данни“, която може да се използва за идентифицирането на дадено лице. Тя би могла да бъде „от име или адрес до пръстов отпечатък или банкови данни“[9].

За да се акцентира върху значението от въвеждането на *Регламента за защитата на лични данни*, ще се представят някои примери със злоупотреби за колосални суми на международно ниво. В тази връзка може да се акцентира върху значимостта на ИТ одита относно протекцията и превенцията на финансовата информация на една компания.

[7] The GDPR: What exactly is personal data?, Luke Irwin, 7th February 2018, <https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data>, last available on: 30.10.2018/ 10.49 a.m.

[8] Personal Data: definition, <https://www.cnil.fr/en/personal-data-definition> last available on: 30.10.2018/ 11.29 a.m.

[9] 13 Key GDPR Terms You Need to Know <https://www.dmnews.com/customer-experience/article/13034542/13-key-gdpr-terms-you-need-to-know>

Съгласно публикуваната информация от *Insurance Information Institute*[10] са отразени нови видове престъпления, свързани с личните данни. Това е кражбата на самоличност, която се осъществява чрез кибер престъпленията. Макар и с въвеждането на кредитни карти, оборудвани със специални микрочипове, които правят картите трудни за фалшифициране, през 2015 година в Съединените американски щати престъпниците извършват измами с нови акаунти. Измамата се осъществява, когато крадец открие кредитна карта или друга финансова сметка, използвайки името на жертвата и/или друга откраднатата лична информация. Според проучването на *Javelin Network*[11] загубите от този вид измами възлизат на стойност 5,1 милиарда долара.

Този вид престъпления се извършват и по други начини. *Cambridge Analytica (CA)*[12] споделят, че има сериозни злоупотреби с лична информация от онлайн платформата на *Facebook.* Приблизително около 87 милиона американски профили са подали оплаквания, че е използвана информацията им без тяхното разрешение. Злоупотребено е с информацията, включваща – имена, местоположения, имейл адрес. От съществено значение е спазването на разписаните политики и правила съгласно GDPR, както и съгласията, които дават потребителите от своя страна за обработката на тяхната информация.

Друг пример от *GDPR Associates* се свързва с онлайн поръчките на храна. Например това е станало с **Michelle Midwinter**, след като поръчала храна чрез сайта на *Just Eat.* Шофьорът, който „извършва доставката, впоследствие започва да ѝ изпраща неподходящи текстови съобщения“[13].

Посочените примери показват, че защитата на лични данни е изключително важна за една компания. Всяка политика е индивидуално разработена спрямо дейността на организацията. От примерите се изяснява, че злоупотребата с лични данни би могла да се извърши по различни начини и че не само хакерите са способни на това. Спазването на вътрешните правила от служителите в една организация е от фундаментално значение.

Тези мисли навеждат, че в одиторските компании се употребява, изисква и съхранява значителен обем от информация за клиенти. Затова разработването и имплементирането на подобна политика са много важни. Дигитализирането на одиторските документи и тяхното съхранение в облачни пространства също индикират за потенциални слабости. Затова по-долу в статията се представя примерен вариант за разработването на политика в одиторска компания спрямо **GDPR.**

Необходимо е да се разработят политики и процедури спрямо ***Регламент (ЕС) 2016/679* и *Закон за защита на личните данни,*** свързани с:

---

[10]Facts + Statistics: Identity theft and cybercrime, <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>, last available on: 02.11.2018/11:06 a.m.

[11] Компания за защита на софтуери.

[12] Facebook, data misuse and why it matters – A look in to the recent issues surrounding Cambridge Analytica and Facebook, 27 March 2018, <https://talkingtech.cliffordchance.com/en/cybersecurity/facebook--data-misuse-and-why-it-matters.html.html> last available on: 02.11.2018/11:36 a.m.

[13] **Delivering some clarity on personal data misuse, 26 January 2018,**
< https://www.gdpr.associates/delivering-clarity-personal-data-misuse/> last available on: 02.11.2018/01:03 p.m.

1. **Политика за защита на лични данни** – необходимо е да се резюмира дейността на компанията, както и да се опишат ключовите понятия и термини, като например какво представляват и включват за организацията следните понятия: ***„лични данни“; „специални категории лични данни“; „обработване“; „администратор“; „субект на данните“; „съгласие на субекта на данните“; „профилиране“; „нарушение на сигурността на лични данни“; „основно място на установяване“; „получател“; „трета страна“***.

2. **Политика за провеждане на обучения в компанията** – от лицата, натоварени с дейността по защита на лични данни, се изисква да разработят специализирани обучения на своите служители, като по този начин те ще бъдат запознати с изискванията и правилата на *Регламента,* които са длъжни да спазват спрямо разработената политика.

   Необходимо е да се разработят декларации, в които служителите на одиторското дружество декларират, че са запознати с правилата и процедурите съгласно *GDPR,* като по този начин гарантират за спазването на конфиденциалност по време на работа.

3. **Процедура за първоначален вътрешен анализ на личните данни и дейностите по обработване** – тази процедура има за цел да установи първоначалните стъпки по анализиране на дейностите по обработване на лични данни от администратора в компанията спрямо *чл. 5* и *чл. 30 от ОРЗД*.

   Извършва се от лицето, натоварено с общото управление, което делегира задължението за извършването на първоначален анализ на служителите от организацията на администратора. Това лице, въз основа на длъжностна характеристика или вътрешни правила, има задължения към компанията, които трябва да бъдат дефинирани. В този смисъл това важи и за външни за администратора лица – IT специалист, адвокат, актюер, счетоводител, лице, което извършва студен преглед за контрол на качеството на одиторски ангажимент.

   Важно е да се определят с въпросници и/или анкети – функционалните/бизнес процеси, при които се използват лични данни от одиторите. В немалка част от случаите личните данни, които употребяват регистрираните одитори, се съхраняват на хартиен носител или в електронни файлове на софтуерната система. Необходимо е да се дефинират в политиката всички процеси, свързани със съхраняването на документацията от одит клиенти. Използва ли се външен ИТ специалист в компанията, или има такъв назначен в самото дружество? Колко често се правят подобрения по системата и т.н. Освен това е важно да се определи: кой от служителите има достъп до тази информация, да има следа кой е влизал за последно, както и кой отговаря за поддържането ѝ.

   Поради значителното количество информация е задължително при започването на всеки един одиторски ангажимент да се попълват декларации за независимост и конфиденциалност (основен принцип за

етичното поведение в одиторската професия) от членовете на одит екипа. Тази процедура също е важно да бъде описана в политиката по **GDPR** от одиторите. Описанието на тези процедури може да се нарече „***картографиране на работните потоци***" – това представлява всички процедури, които се извършват от одит екипа, свързани с използването на лични данни. В т.ч. например са процедурите по назначаването на външни експерти за компанията, какви документи са необходими и изискванията, на които следва да отговарят кандидатите; какви допълнителни мерки за сигурност са предприети в одиторското дружество; ***длъжностно лице по защита на данните (ДЛЗД) – този процес е разгледан и определен с разработените Насоки на работна група по член 29[14],*** в които са определени и неговите задължения.

Споменатото по-горе лице със специални правомощия би могло да бъде и лице, което работи в дружеството, но е важно да се обърне внимание на юридическата документация, която е нужно да включва – *анекс към трудовите/гражданските договори, корекции в длъжностни характеристики на служителя към администратора, формуляр за съгласие, декларации за поверителност, вътрешни фирмени процедури (правила) и др. документи, които са необходими, с цел осигуряване на максимално ниво на защита на личните данни в съответствие с ОРЗЛД.*

4. **Процедура за прозрачност при обработване на лични данни** – настоящата процедура обхваща всички действия по събиране и обработване на лични данни от одиторското дружество ***(член 12, 13 и 14 от ОРЗД).***

   Назначеното *длъжностно лице по защита на данните (ДЛЗД)* или *отговорникът по защита на лични данни* има ангажимент да извести одит клиентите относно информацията, която са задължени да предоставят на одиторите при събиране на лични данни, за да бъде законосъобразен извършваният одит. От *ДЛЗД* се изисква да разработи и гарантира, че са създадени механизми за информиране, като например декларация за поверителност, която спазва одиторската компания, и е необходимо същата да се публикува на интернет страницата на дружеството. Освен това е необходимо да се качат на интернет страницата декларации за съгласие или за отказ от съгласие за обработване на лични данни. Също така при сключването на договор за одит е важно да се отбележи дали дружество спазва политиките по ***GDPR*** и къде са разписани тези политики и процедури, кое е *ДЛЗД* в компанията и как могат да попълнят своите декларации за съгласие или отказ от такова.

   Служителите на одиторската компания, които по силата на своите трудови задължения събират лични данни, са длъжни да спазват разработените политики, правила и процедури от компанията. За пример може да

[14]Насоки от Работна група по чл. 29 с оглед на началото на прилагането на Общия регламент за защита на данните, <https://www.cpdp.bg/?p=element&aid=1141> последно влизане на: 02.11.2018/10:20.

послужи проверяването на осчетоводените заплати при различни одиторски клиенти. Този процес е обвързан с използването на лични данни, като имена, първите две цифри от единния граждански номер на попадналото лице, за да се разбере начина на осчетоводяване спрямо начисляването на осигуровки (за родените преди или след 60-а година), и работната заплата на лицето. Тази процедура се изпълнява спрямо законовите изисквания, но е съществено да не се злоупотребява и да се запази конфиденциалност спрямо *Регламента*.

5. **Процедура за управление на исканията от субектите** *(членове 12, 15, 16, 17, 18, 20 и 21 от ОРЗД)* **–** необходимо е да се разработи форма, в която са описани изискуемите документи от одитора към неговия клиент, например (*клиентски номер – ЕИК, платежни и финансови документи, юридически документи и други доказателства за изпълнение на финансовия одит).* За тази документация е отговорно *ДЛЗД*, което се задължава да води *Регистър на исканията.* От страна на одитора е редно да се провери дали представената информация е вярна. Примерно да се направи справка в онлайн платформата на ***Търговския регистър*** дали данните на компанията съвпадат с представените от тях.

6. **Процедура за начините на комуникация при жалби и искания от субекта на данни** – това изискване се свързва с *член 12* от *Регламента.* Важно е да се осигури свободен достъп на клиентите до интернет страниците на одиторските дружества, на които да бъдат на разположение бланки за подаване на жалби спрямо личните данни. Също така от одиторите е необходимо определянето на срокове за отговор при подаването на жалба от клиент. Администраторът на лични дани се задължава да отговори и ако се установи нарушение, е необходимо да се обърне към *Комисията за защита на лични данни*, която е основната отговорна институция за България в това направление.

7. **Процедура за преносимост на данни** – това условие е представено в *член 12* от *ОРЗЛД.* Важно е при разпространяването на лични данни от клиент на друг член от одит екипа да не се получи изтичане на информация. Освен това *ДЛЗЛД* преценява дали данните са допустими, или не. Също така е нужно предоставените данни да се съхраняват по уместен начин, както и тяхното използване да бъде по предназначение (за целите на одита).

8. **Процедура по получаване на съгласие и по оттегляне на съгласието за обработване на данни** – тези две процедури могат да се представят и по отделно в политиката, но подходът е еднакъв:

   - ✓ *при съгласие* – създаване и имплементиране на *съгласие* относно изискванията на *член 4, точка 11*, *член 7 и член 8* от *ОРЗД;*
   - ✓ *при отказ от съгласие* – създаване и имплементиране *на съгласие към изискванията на член 7 и член 8* от *ОРЗД.* Съществено е този документ да бъде лесно достъпен за потребителите на одиторски услуги. От страна на клиентите е важно тези декларации да бъдат изпратени по

имейл или на хартиен носител до *ДЛЗЛД*. Практичен начин е да бъдат публикувани и двата варианта на сайта на одиторската компания.

9. **Процедура за съхраняване и унищожаване на данните** – съгласно *член 5, параграф 1, буква „д“* от *ОРЗД* личните данни се съхраняват за период, не по-дълъг от необходимия за целите, в случая изпълнението на независим финансов одит. Тази процедура засяга одиторите спрямо и други закони: *Глава III от Закона за националния архивен фонд; Наредба за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общинските институции; Закон за счетоводството; Закон за независимия финансов одит; Закон за ДДС.*

   От фундаментално значение е всяка одиторска компания да опише своите политики и процедури, свързани със събирането, съхраняването и унищожаването на лични данни. Например за унищожаването на документи с подобен характер одиторското дружество може да наема външна компания, която да осъществява тази процедура веднъж годишно.

10. **Процедура за управление на процесите по възлагане на работа на подизпълнители** – това условие е нужно да се изпълни съгласно *член 4, точка 8* и *член 28 от ОРЗД*. Важно е да се сключи договор между двете страни, като са описани детайлно задълженията на подизпълнителя. Например това може да бъде ИТ компания, която отговаря за облачното пространство на одиторската компания, в което са налични редица лични данни.

11. **Процедура за оценка на въздействието върху защитата на данните** – всички процедури, които се изпълняват от одитора, свързани с лични данни, са предмет на предварителна оценка на риска. При наличието на **висок риск** *е нужно преди обработката на данните да се приложи и оценка на въздействието върху защитата на личните данни.* Тази процедура се изпълнява спрямо изискванията на *член 35, § 3 от ОРЗД*. Лицата, отговарящи за защитата на лични данни, са длъжни да споделят опасенията си с мениджмънта при индикациите на висок риск. Администраторите на лични данни трябва да анализират вероятността от появата на несигурност на данните и да се определи нивото на въздействие. Нивото би могло да бъде*: ниско, средно, високо и изключително високо.*

    Например, ако даден служител в одиторската компания не качва системно своите файлове, съдържащи лични данни, от одит на сървъра, в този случай ще има висок риск, че дадената информация би могла да бъде изгубена и/или заличена и да се злоупотреби с нея.

12. **Процедура по приемане на план за технически и организационни мерки** – тази дейност се изисква спрямо *член 25* и *32* от *ОРЗЛД*.

    В случая за техническите мерки могат да послужат, като пример в одиторската професия, специфични информации, например при одитирането на банки и застрахователни дружества. Тук е необходимо да

се разпишат правила по отношение на: класифициране на данни, предотвратяване на загуба на данни, криптиране, получаване на съгласие за всяка конкретна цел, ограничения при пренасяне на данни и въвеждането им в технологични устройства, коригиране и заличаване на лични данни и други.

Технологическите мерки в одиторската професия е нужно да бъдат описани в политиката, като те могат да се свържат с внедряването на: защити с пароли; достъп до сайт и/или сървър, антивирусен софтуер, контрол на достъп на физически лица и т.н.

13. **Процедура по уведомяване за нарушение на сигурността на личните данни** – тази процедура се прилага, когато се установи нарушение на сигурността на личните данни съгласно *член 33* от *ОРЗД – „Уведомяване на надзорния орган за нарушение на сигурността на личните данни“*. Спрямо българското законодателство този орган е *Комисията за защита на лични данни (КЗЛД)*. Освен това *член 34* от *ОРЗД „Съобщаване на субекта на данните за нарушение на сигурността на личните данни“* изисква при установяване от ДЛЗЛД на нарушение, свързано с лични данни, да бъде подаден сигнал **до 72 часа** в КЗЛД.

    Изпълнява се само с предварителното одобрение от администратора на лични данни на компанията. Уведомлението трябва да съдържа задължително следната информация: естество на нарушението, категориите лични данни, приблизителен брой на засегнатите от нарушението.

14. **Процедура по предаване на лични данни на трети държави или международни организации** – настоящата процедура се прилага, когато администраторът на лични данни има намерения да предостави на трети държави (държави, които не са членки на Европейския съюз) или на международни организации лични данни за обработка съгласно изискванията на *член 44-49* от *ОРЗД* и *Ръководство относно Щита за личните данни в отношенията между ЕС и САЩ.*

    Например, когато се извършва консолидация на отчета на дадена компания, която има дъщерни дружества извън ЕС, е необходимо одиторската компания да има разписани правила и процедури спрямо *Регламента*.

    Всички изброени политики и процедури по-горе са примерни и биха могли да се приемат като един базисен минимум. Съответно те могат да бъдат съкращавани и/или разширявани спрямо дейността и прилаганите политики на дадената одиторска компания. Дори някои от тези процедури могат да бъдат и отстранени, ако не се прилагат в одиторското дружество.

От гореизложеното могат да се обобщят следните **изводи:** одиторите разполагат със съществена финансова информация за одитираните от тях предприятия и техните служители, затова е важно да бъдат спазвани правилата за конфиденциалност. Представиха се няколко примера, които доказаха съществеността на тази политика. Чрез внедряването и имплементирането на

процедурите, съгласно изискванията на **GDPR,** тази цел би могла да бъде постигната.

Както всяко едно ново законово изискване и *Регламент (ЕС) 2016/679* доведе до някои съществени промени. Една от тази промени е въвеждането на правила и процедури за употребяващите лични данни. Одиторите също са част от тази група, затова е важно да бъдат разписани правила и политики, които да се спазват.

Библиографска справка:

1. Закон за защита на личните данни, обн., ДВ, бр. 1 от 4 януари 2002 г., последно изм., ДВ, бр. 7 от 19 януари 2018 г.

Интернет страници:

1. Какво означава „лични данни“?, източник: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_bg>, последно влизане на: 25.10.2018/10:38.

2. Personal Data: definition, <https://www.cnil.fr/en/personal-data-definition> last available on: 30.10.2018/11.29 a.m.

3. 13 Key GDPR Terms You Need to Know <https://www.dmnews.com/customer-experience/article/13034542/13-key-gdpr-terms-you-need-to-know> last available on: 30.10.2018/ 10.29 a.m.

4. Delivering some clarity on personal data misuse, 26 January 2018, <https://www.gdpr.associates/delivering-clarity-personal-data-misuse/> last available on: 02.11.2018/01:03 p.m

5. Facts + Statistics: Identity theft and cybercrime, <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>, last available on: 02.11.2018/11:06 a.m.

6. The GDPR: What exactly is personal data?, Luke Irwin, 7th February 2018, <https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data>, last available on: 30.10.2018/ 10.49 a.m.

7. Facebook, data misuse and why it matters – A look in to the recent issues surrounding Cambridge Analytica and Facebook, 27 March 2018, <https://talkingtech.cliffordchance.com/en/cybersecurity/facebook--data-misuse-and-why-it-matters.html.html> last available on: 02.11.2018/11:36 a.m.

THE IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION IN AUDIT PRACTICE

Diyana Bankova, PhD
Audit Assistant
Moore Stephens Bulgaria Audit LTD

Key words:
Personal data
Frauds
Audit
GDPR Policy

Summary

The article aims to explore the importance of privacy policy. It provides some examples of misuse of personal data to which auditors should pay attention.

Variants are proposed for the development and deployment of policies and procedures under the General Data Protection Regulation (GDPR) in audit companies.