**«Приведение информационной системы Аудиторской компании**

**в соответствие требованиям законодательства**

**в области обработки персональных данных»**

1. Согласно подпункта 1 пункта 1 статьи 7 Федерального закона N 115-ФЗ субъекты антиотмывочного контура (в частности, аудиторские организации) обязаны до приема на обслуживание идентифицировать клиента, представителя клиента и (или) выгодоприобретателя.

Сведения, подлежащие установлению при идентификации клиентов – физических лиц, представителей клиента и бенефициарном владельце:

Сведения о физическом лице – представителе / бенефициарном владельце клиента в том числе:

1 Фамилия, имя, отчество

2 Дата рождения

3 Гражданство

4 Реквизиты документа, удостоверяющего личность: Общегражданский паспорт РФ

4а серия (при наличии) и номер

4б дата выдачи

4в наименование органа, выдавшего документ

4г код подразделения (при наличии)

5 Адрес места жительства (регистрации) или места пребывания

6 Идентификационный номер налогоплательщика (при наличии)

7 Контактная информация (при наличии): номер телефона / факса

8 адрес электронной почты

9 почтовый адрес

другая информация

10. Основания для определения лица как бенефициарного владельца

Согласно Федеральному закону от 27.07.2006г. № 152-ФЗ «О персональных данных» вышеуказанные сведения связанные с физическими лицах являются персональными данными.

**Когда речь идет о выполнении требований законодательства о персональных данных, большинство операторов считают, что речь идет только о тех персональных данных, которые обрабатываются в электронном виде.**

Учитывая вышеизложенное, мы пришли к выводу, что

Автоматизированная обработка персональных данных это:

1. Наличие в Организации 1С ЗУП, 1С Бухгалтерия, отчетность передается с использованием сетей передачи данных (Расчет по страховым взносам – ежеквартально, Персонифицированные сведения о физических лицах – ежемесячно, Расчет сумм налога на доходы физических лиц).
2. Наличие локальной вычислительной сети (распределенная обработка данных), есть подключение к интернет (распределенная обработка данных), обмен информации на флэшках – способ передачи информации при ее распределенной обработке.).

Согласно статье 1 Федерального закона № 152-ФЗ «О персональных данных»: «Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных… с использованием средств автоматизации…, или без использования таких средств…».

Именно за нарушения при обработке персональных данных без использования средств автоматизации Роскомнадзор РФ (орган по защите прав субъектов персональных данных) выписывает больше всего предписаний.

Федеральный закон № 152-ФЗ «О персональных данных» почти не разделяет требования для разных видов обработки персональных данных, кроме статьи 19, в которой почти в каждом пункте части 2 речь идет об обработке в информационных системах.

Главное, чтобы обработка персональных данных без использования средств автоматизации выполнялась с соблюдением принципов и в случаях, установленных законом.

Кроме ФЗ № 152 «О персональных данных», существует подзаконный акт, специально регулирующий обработку персональных данных без использования средств автоматизации – Постановление Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» № 687 от 15.09.2008г.

Хочу обратить внимание на некоторые пункты Постановления Правительства №687, несоблюдение которых чаще всего приводит к нарушениям:

- пункт 6. В нем говорится: «Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, …, категориях обрабатываемых персональных данных, …, а также об особенностях и правилах осуществления такой обработки…»;

- пункт 7 (который часто игнорируется операторами, так как не все понимают, что же такое типовая форма):

*При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:*

*а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;*

*б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;*

*в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;*

*г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.*

- Пункт 13 определяет наличие трех перечней:

1) перечня персональных данных,

2) перечня мест хранения носителей персональных данных.

3) перечня лиц, осуществляющих обработку персональных данных.

Операторы часто забывают, что места хранения нужно определить в отношении каждой категории персональных данных.

- 14 пункт обязывает нас обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

- Пункт 15 обязывает нас соблюсти условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Данный пункт содержит требование определить: перечень мер, порядок их принятия, перечень лиц ответственных за их реализацию.

Таким образом, обработка персональных данных без использования средств автоматизации имеет свои секреты и нюансы.

**30 ноября 2024 г. Президент РФ подписал Федеральный закон № 420 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (далее — Закон № 420-ФЗ), который вступит в силу 30 мая 2025 г., и Федеральный закон № 421 «О внесении изменений в Уголовный кодекс Российской Федерации» (далее — Закон № 421-ФЗ), который вступил в силу 11 декабря 2024 г.**

**Большинство положений Закона № 420-ФЗ посвящены дальнейшей диверсификации видов правонарушений и ужесточению административной ответственности в сфере законодательства РФ о персональных данных. Законом № 421-ФЗ вводится специальный состав преступления в этой сфере.**

Законом № 420-ФЗ внесены существенные изменения в ст. 13.11 Кодекса об административных правонарушениях (далее — КоАП). Субъектами соответствующих административных правонарушений являются **граждане, должностные лица и юридические** лица.

Увеличены размеры административных штрафов за обработку персональных данных в случаях, не предусмотренных законодательством РФ в области персональных данных, либо обработку персональных данных, несовместимую с целями сбора персональных данных (за некоторыми исключениями), если такие действия не содержат признаков преступления.

В частности, размер штрафов:

* для **граждан** составит от 10 000 до 15 000 руб. (ранее — от 2 000 до 6 000 руб.),
* для **должностных лиц** составит от 50 000 до 100 000 руб. (ранее — от 10 000 до 20 000 руб.),
* для **юридических лиц** составит от 150 000 до 300 000 руб. (ранее — от 60 000 до 100 000 руб.).

Выросли штрафы и за повторные нарушения. Например, штраф для юридических лиц составит от 300 000 до 500 000 руб. (ранее — от 100 000 до 300 000 руб.).

**Ст. 13.11 КоАП дополнена новыми видами административных правонарушений.**

***Вводится ответственность за невыполнение или несвоевременное выполнение оператором обязанности по уведомлению уполномоченного органа по защите прав субъектов персональных данных о намерении осуществлять обработку таких данных. Размер штрафа для юридических лиц — от 100 000 до 300 000 руб.***

**За невыполнение или несвоевременное выполнение оператором обязанности по уведомлению уполномоченного органа по защите прав субъектов персональных данных в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) таких данных, повлекшей нарушение прав субъектов персональных данных, также установлена ответственность. Например, юридические лица могут быть подвергнуты штрафу в размере от 1 до 3 млн руб.**

Вводится административная ответственность за действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей специальную категорию персональных данных (например, сведения о состоянии здоровья). Юридическое лицо может быть наказано штрафом в размере от 10 до 15 млн рублей.

Наконец, будут наказываться действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей биометрические персональные данные, за исключением случаев, предусмотренных ст. 13.11.3 КоАП. Размеры штрафов составят:

* для граждан — от 400 000 до 500 000 руб.,
* для должностных лиц — от 1 300 000 до 1 500 000 руб.,
* для юридических лиц — от 15 до 20 миллионов руб.

**Уголовный кодекс РФ дополнен ст. 272.1, которая касается незаконного использования и (или) передачи, сбора и (или) хранения компьютерной информации, содержащей персональные данные, а также создания и (или) обеспечения функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения.**

Предусмотрены следующие виды преступлений:

* незаконные использование и (или) передача (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей персональные данные, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование либо иным незаконным путем (далее — **часть 1**);
* те же деяния, совершенные в отношении компьютерной информации, содержащей персональные данные несовершеннолетних лиц, специальные категории персональных данных и (или) биометрические персональные данные (далее — **часть 2**);
* деяния, предусмотренные частями 1 или 2, совершенные из корыстной заинтересованности, с причинением крупного ущерба, с использованием служебного положения, группой лиц по предварительному сговору (далее — **часть 3**);
* деяния, предусмотренные частями 1-3, сопряженные с трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей информации, содержащих персональные данные (далее — **часть 4**);
* деяния, предусмотренные частями 1-4, если они повлекли тяжкие последствия либо совершены организованной группой (далее — **часть 5**);
* создание и (или) обеспечение функционирования информационного ресурса (сайта в сети Интернет и (или) страницы сайта в сети Интернет, информационной системы, программы для электронных вычислительных машин), заведомо предназначенных для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, полученной незаконным путем.

Самое строгое наказание в виде **лишения свободы на срок** **до 10 лет** со штрафом в размере до 3 млн рублей или в размере заработной платы или иного дохода осужденного за период до 4 лет, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового установлено за преступления, предусмотренные **частью 5**.

**Уведомление в Роскомнадзор об обработке персональных данных.**

С 01 сентября 2022 года действует норма, по которой работодатели обязаны подать уведомление в Роскомнадзор об обработке **персональных данных,** **которые обрабатываются в электронном виде.**

Согласно ч.1.ст.22 ФЗ-152 «О персональных данных» от 27.07.2006 г. **оператор до начала обработки персональных данных обязан уведомить** уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных [частью 2](https://www.consultant.ru/document/cons_doc_LAW_482686/d996966e22e1320c9de1ab82d9f6be12c3d9d765/#dst100163) настоящей статьи.

Уведомлять ведомство нужно как в начале проведения обработки, так и по ее завершению.

Роскомнадзор ведет реестр операторов персональных данных. Уведомление об обработке персональных данных подается по защищенным (доверенным) каналам по форме, размещенной **на сайте Роскомнадзор.**

<https://pd.rkn.gov.ru/operators-registry/operators-list/>

После проверки уведомления Роскомнадзор отражает организацию, подавшую уведомление, в реестре операторов персональных данных.

Уведомление подразумевает заполнение уведомительного бланка стандартного образца. Есть три варианта его подачи:

- В электронном виде с цифровой подписью через сайт Роскомнадзора.

- На бумажном носителе. Форма можно заполнить на сайте Роскомнадзора, распечатать ее, подписать и отнести лично либо направить почтовым отправлением в региональное отделение органа Роскомнадзор.

-через подтвержденную учетную запись на портале «Госуслуги».

В течении 30-ти дней с момента получения извещения Роскомнадзор добавляет информацию в реестр операторов ПД. Если извещение поступает в бумажном виде, срок считают со дня его получения соответствующим региональным управлением.

В силу ч. 2 ст. 22 ФЗ -152 «О персональных данных» от 27.07.2006 г. оператор **вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных** в случае, если оператор осуществляет деятельность по обработке персональных данных **исключительно без использования средств автоматизации.**

В ст.3 п. 4 ФЗ-152 прямо указано, что автоматизированная **обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.**

**Пример обработки персональных данных без использования средств автоматизации был рассмотрен в постановлении Арбитражного суда Московского округа от 27.03.2025г. по делу №А40-12676/2024.**

В постановлении Арбитражного суда Московского округа от 27.03.2025г. по делу №А40-12676/2024 указано, что:

- Обработка персональных данных (сбор персональных данных) с использованием сайта сети «Интернет» не приравнивается к использованию средств автоматизации, а по смыслу приведенных положений **применение вычислительной техники при обработке персональных данных не относится к использованию средств автоматизации, если такая обработка осуществляется непосредственно человеком**. (как записная книжка)

- Если информация вносится, изменяется, передается и уничтожатся персонально по каждому субъекту персональных данных вручную, обработка считается неавтоматизированной, в то время как если используемые оператором **программы могут самостоятельно переформатировать данные, выбирать их по установленным параметрам, передавать внешним пользователям без необходимости просмотра и проверки персональных данных по каждому субъекту в отдельности, то такая обработка является автоматизированной. (1С предприятие, 1С ЗУП)**

*По мнению суда сбор персональных данных СНТ «Якорь» (в силу имеющейся у СНТ «Якорь»* ***обязанности по*** ***ведению реестра в соответствии с положениями*** *ст. 12.15 Федерального закона от 29.07.2017г. №217-ФЗ «О ведении гражданами садоводства и огородничества для собственных нужд и о внесении изменений в отдельные законодательные акты РФ») осуществляется с помощью вычислительной техники* ***через сайт в информационно-телекоммуникационной сети Интернет****, однако каких-либо доказательств, подтверждающих,* ***что товариществом используется программа, осуществляющая обработку персональных данных в автоматизированном режиме без участия человека, материалы дела не содержат.***

По мнению суда СНТ «Якорь» осуществлял деятельность по обработке персональных данных (**ведению реестра садоводов СНТ «Якорь»)** без использования средств автоматизации.

**Хранение персональных данных**

**Согласно ст.5 п.**7 [Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных"](https://www.consultant.ru/document/cons_doc_LAW_61801/) **Персональные данные хранятся не дольше, чем этого требуют цели их обработки**. Если срок хранения не установлен федеральным законом или договором, то данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Некоторые сроки хранения персональных данных работников, установленные в Перечне типовых управленческих архивных документов, утверждённом приказом Росархива от 20.12.2019 № 236:

* **Подлинные личные документы сотрудников** (трудовые книжки, дипломы, аттестаты, удостоверения, свидетельства) — **до востребования** (невостребованные — 50 лет; 75 лет — если оформлены до 2003 года).
* **Документы по личному составу** (трудовые договоры, личные карточки сотрудников, лицевые карточки, счета работников) — **50 лет** (75 лет — если оформлены до 2003 года).
* **Личные дела** (заявления, копии приказов и выписки из них, листки по учёту кадров, анкеты, аттестационные листы и др.) — **50 лет** (75 лет — если оформлены до 2003 года).
* **Приказы, распоряжения по личному составу**, а также дополнения к ним (докладные записки, справки, заявления) — **50 лет** (75 лет — если оформлены до 2003 года).
* **Согласие на обработку персональных данных** после истечения срока его действия или его отзыва — **3 года** ([4](https://www.kdelo.ru/art/383880-qqq-16-m11-srok-hraneniya-personalnyh-dannyh) года).

Срок хранения персональных данных 75 лет установлен для документов длительного хранения, делопроизводство в организации, по которым закончено до 1 января 2003 года.

**Приняла меры по защите персональных по автоматизированной и ручной обработки:**

**-сейф;**

**- Антивирус;**

**- разграничение прав доступа.**

**Уведомление в Роскомнадзор об обработке персональных данных.**