УТВЕРЖДЕНО
приказом директора
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»
от 28.05.2025 г. №22

ПОЛОЖЕНИЕ
о работе с персональными данными работников
Муниципального бюджетного учреждения культуры
«Одинцовская концертная организация»

1. Общие положения

1.1. Положение о работе с персональными данными работников Муниципального бюджетного учреждения культуры «Одинцовская концертная организация» (далее - Положение) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации (далее – ТК РФ), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон от 27.07.2006 № 152-ФЗ), Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённым постановлением Правительства Российской Федерации от 15.09.2008 № 687, Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждёнными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, Письмом Роскомнадзора от 19.10.2021 № 08-71063 «О разъяснении законодательства» (далее – Разъяснения Роскомнадзора), иными законодательными и нормативными правовыми актами.

1.2. Настоящее Положение определяет порядок обработки персональных данных работников, гарантии конфиденциальности сведений о работнике, предоставленных Муниципальному бюджетному учреждению культуры «Одинцовская концертная организация», далее именуемому учреждением - работодателем, от несанкционированного доступа и разглашения. Персональные данные работников являются конфиденциальной, строго охраняемой информацией.

Настоящее Положение является документом, определяющим политику работодателя - оператора в отношении обработки персональных данных работников.

1.3. В целях настоящего Положения используются следующие определения:

1) персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

2) субъект персональных данных – работник (физическое лицо, связанное с работодателем трудовыми правоотношениями (заключенным с работодателем трудовым договором) или соискатель - лицо, намеревающееся заключить трудовой договор с работодателем), а также лица, уволенные из учреждения-работодателя по основаниям, указанным в ТК РФ (в течение определённого законодательством Российской Федерации времени);

3) персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ;

4) оператор – это учреждение - работодатель, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных работников, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

5) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

6) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

7) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

8) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

9) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

10) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

11) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной

информации определить принадлежность персональных данных конкретному субъекту персональных данных;

12) использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом оператора в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

13) конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

14) информация - сведения (сообщения, данные) независимо от формы их представления;

15) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

16) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

17) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

18) угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

19) уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационной системе;

20) РКН (Роскомнадзор) - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - федеральный орган исполнительной власти, в задачи которого входят надзор в сфере связи, информационных технологий и СМИ, а также надзор по защите персональных данных и регулирование радиочастотной службы;

21) Комитет по культуре - Комитет по культуре Администрации Одинцовского городского округа Московской области;

22) органы местного самоуправления - органы местного самоуправления Одинцовского городского округа Московской области;

23) городской округ – муниципальное образование «Одинцовский городской округ Московской области».

1.4. В состав персональных данных, которые работник сообщает работодателю, входят:

1) фамилия, имя, отчество;
2) пол;
3) дата рождения;
4) место рождения;
5) возраст;
6) гражданство;
7) сведения об образовании с указанием наименования образовательной организации, года ее окончания, квалификации, специальности и (или) направления профессиональной подготовки, наименования и реквизитов документа об образовании, сведения о профессиональной переподготовке и (или) повышении квалификации;
8) сведения об ученой степени, ученом звании;
9) адрес места постоянной (временной) регистрации, фактического проживания;
10) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи;
11) отношение к воинской обязанности, сведения о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документов воинского учета, наименование органа, выдавшего его);
12) сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования или документе, подтверждающем регистрацию в системе индивидуального (персонифицированного) учета;
13) идентификационный номер налогоплательщика;
14) реквизиты страхового медицинского полиса обязательного медицинского страхования;
15) реквизиты свидетельства о государственной регистрации актов гражданского состояния;
16) сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших супругах);
17) сведения о трудовой деятельности, включая работу по совместительству, предпринимательскую и иную деятельность, военную службу;
18) сведения о государственных наградах, иных наградах и знаках отличия;
19) сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
20) сведения об аттестации работника, повышении квалификации, переквалификации;

21) сведения о доходах, об имуществе и обязательствах имущественного характера руководителя учреждения-работодателя, гражданина, претендующего на занятие должности руководителя учреждения-работодателя, сведения о доходах, об имуществе и обязательствах имущественного характера супруги (супруга) и (или) несовершеннолетних детей руководителя учреждения-работодателя, гражданина, претендующего на замещение должности руководителя учреждения-работодателя, а также сведения о расходах руководителя учреждения-работодателя, его супруги (супруга) и (или) несовершеннолетних детей;

22) контактная информация (номер телефона, адрес электронной почты или почтовый адрес).

23) специальные категории персональных данных:

а) сведения о состоянии здоровья;

б) сведения о наличии или отсутствии судимости, причём обработка персональных данных о судимости может осуществляться в случаях и в порядке, которые определяются в соответствии с федеральными законами Российской Федерации и Правилами внутреннего трудового распорядка оператора;

в) номер расчетного счета;

г) номер банковской карты;

24) биометрические персональные данные: фото (*лица, в полный рост*) в бумажном и электронном виде, видеоизображения;

25) иные сведения, которые субъект персональных данных пожелал сообщить о себе и которые отвечают целям обработки персональных данных.

1.5. Документами, которые содержат персональные данные работников, являются:

1) комплекты документов, сопровождающих процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

2) комплекты материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;

3) подлинники и копии приказов (распоряжений) по кадрам;

4) личные дела, трудовые книжки, сведения о трудовой деятельности работников;

5) дела, содержащие материалы аттестаций работников;

6) дела, содержащие материалы внутренних расследований, осуществления аудита, проверок вышестоящими или сторонними организациями;

7) справочно-информационный банк данных по персоналу (картотеки, журналы);

8) подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству оператора, руководителям структурных подразделений оператора, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, муниципальные и государственные вышестоящие и контролирующие органы;

9) документированная информация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства оператора);

10) документы по планированию, учету, анализу и отчетности в части работы с персоналом оператора.

Для осуществления кадровой деятельности оператора вышеуказанные документы создаются и хранятся по группам документированной информации, содержащей данные о работниках в единичном или сводном виде.

1.6. Вопросы, не урегулированные настоящим Положением, решаются в соответствии с законодательством Российской Федерации.

1.7. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных работников, к сведениям о реализуемых требованиях к защите персональных данных.

При этом, в случае сбора персональных данных с использованием информационно-телекоммуникационных сетей, оператор обязан опубликовать указанный документ в соответствующей информационно-телекоммуникационной сети, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети (далее - ИТС).

1.8. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии оператора, если иное не определено законодательством Российской Федерации.

1.9. Определение структурного и содержательного наполнения документа, определяющего Политику работодателя в отношении обработки персональных данных работников, отнесено к компетенции оператора.

1.10. Настоящее Положение и изменения к нему утверждаются и вводятся в действие приказом директора учреждения - работодателя. Все работники оператора должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.11. Настоящее Положение и изменения к нему в обязательном порядке публикуются на официальном сайте оператора в сети «Интернет».

2. Получение и обработка персональных данных работников

2.1. Персональные данные работников обрабатываются в целях обеспечения уставной деятельности учреждения-работодателя и профессиональной деятельности работника, содействия в выполнении осуществляемой работы, организации и прохождения конкурса на замещение вакантных должностей, формирования кадрового резерва руководителей учреждений-работодателей, обучения и должностного роста, учета

результатов исполнения работниками должностных обязанностей, поощрения и стимулирования их труда, обеспечения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, противодействия коррупции.

2.2. Оператор до начала обработки персональных данных обязан уведомить Роскомнадзор о своем намерении осуществлять обработку персональных данных (ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ). Работодатель обязан уведомлять о начале обработки персональных данных, даже если обрабатывает их в целях трудового законодательства. Если не отправить уведомление, оператора оштрафуют (письмо Роскомнадзора от 19.08.2022 № 08-75348).

2.3. Оператор должен уведомлять РКН о планах обрабатывать:

- личную информацию работников в рамках трудовых правоотношений;
- сведения для оформления разового пропуска на территорию работодателя;
- данные при заключении гражданско-правовых договоров.

Для каждой цели обработки перечисляются категории персональных данных и субъектов, чьи данные обрабатываются, правовое основание их обработки и перечень действий с этими данными в соответствии с частями 3 и 3.1 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ.

2.4. В случае изменения сведений, указанных в уведомлении, изменились, об этом сообщается в Роскомнадзор по установленной форме не позднее 15-го числа месяца, следующего за месяцем, в котором произошли изменения.

2.5. В случае прекращения обработки персональных данных, направляется уведомление об этом в Роскомнадзор в течение 10 рабочих дней с момента прекращения обработки сведений.

2.7. Персональные данные работника оператор получает, как правило, непосредственно от работника. Оператор вправе получать персональные данные работника от третьих лиц только при наличии письменного согласия работника или в иных случаях, прямо предусмотренных в законодательстве Российской Федерации.

2.8. Существует два вида согласий на обработку персональных данных:

1) согласие на обработку персональных данных (Приложение 1 к Положению);

2) согласие на обработку персональных данных, разрешенных работником для распространения (Приложение 4 к Положению).

2.9. Согласие на обработку персональных данных - документ, подписываемый работником, в текст которого включают перечень персональных данных и список действий оператора, которые он может совершать с указанными данными. В этом же документе при необходимости прописывают согласия на обработку специальных категорий персональных данных (о национальности, состоянии здоровья, религиозных взглядах), биометрических (отпечатки пальцев, фотографии, видеоизображения) и на трансграничную передачу данных.

2.10. Работодатель должен получить согласие на обработку персональных данных в следующих случаях:

1) запрашивает данных больше, чем ему нужно по трудовому законодательству;

2) получает персональные данные у третьей стороны, п. 3 ст. 86 ТК РФ.

До отправки запроса нужно получить у работника письменное согласие на получение перечисленных в запросе персональных данных;

3) обрабатывает информацию о национальности, состоянии здоровья, политических взглядах, религиозных убеждениях и иные специальные категории персональных данных, непосредственно связанные с вопросами трудовых отношений, п. 4 ст. 86 ТК РФ, п. 1 ч. 2 ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ;

4) сообщает персональные данные работника в коммерческих целях, абз. 3 ст. 88 ТК РФ;

5) обрабатывает биометрические персональные данные, ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ;

6) осуществляет трансграничную передачу персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, ч. 4 ст. 12 Федерального закона от 27.07.2006 № 152-ФЗ;

7) вносит персональные данные работников в общедоступные справочники, адресные книги, ч. 1 ст. 8 Федерального закона от 27.07.2006 № 152-ФЗ.

2.11. Согласие на обработку персональных данных, разрешенных работником для распространения, требуется, если оператор предоставляет (раскрывает) персональные данные работника неограниченному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ).

Это самостоятельный документ, оформляемый отдельно от согласия на обработку персональных данных.

Согласие на распространение персональных данных не требуется, если распространение персональных данных происходит по требованию действующего законодательства.

2.12. Оператор обязан предоставлять персональные данные граждан по запросам государственных органов в случаях, установленных федеральными законами (п. 2 ст. 88 ТК РФ).

2.13. При подписании работником согласия на получение персональных данных от третьих лиц оператор должен сообщить работнику о целях, предполагаемых источниках и способах получения работодателем персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение

2.14. Оператор не вправе требовать от работника представления персональных данных, которые не характеризуют работника как сторону трудовых отношений.

Запрещается получать, обрабатывать и приобщать к личному делу субъектов персональных данных персональные данные, не предусмотренные пунктом 1.4 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.15. Работник представляет оператору достоверные сведения о себе. Оператор проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами.

2.16. Согласие на обработку персональных данных может быть отозвано работником. В случае отзыва работником согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия работника при наличии оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ.

3. Использование персональных данных работников

3.1. Персональные данные работника используются для целей, связанных с выполнением работником трудовых функций. Учреждение - работодатель для этой цели запрашивает общие персональные данные: фамилию, имя, отчество, дату, месяц и год рождения, место рождения, адрес, сведения о семейном положении; сведения об образовании, профессии; специальные категории персональных данных: сведения о состоянии здоровья, сведения о судимости; биометрические персональные данные: фото (лица) в бумажном и электронном виде.

3.2. Содержание и объем персональных сведений должны соответствовать целям обработки. Объем информации, хранящийся у оператора, не должен выходить за рамки указанных целей. Лишние сведения, а также те сведения, которые РКН посчитает излишними, должны уничтожаться в установленном порядке.

3.3. В процессе работы с персональными данными нельзя подменять цели обработки.

3.4. В соответствии с ч. 1 ст. 6, ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ оператор должен запрашивать у работников (соискателей на заключение трудового договора) согласие на обработку персональных данных, как только получает к ним доступ.

3.5. Оператор вправе не получать согласия работников на обработку персональных данных в следующих случаях:

1) обрабатывают персональные данные для исполнения заключенного с работником трудового договора (пп. 5 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ);

2) специалист по кадрам вносит паспортные данные работника в трудовой договор, бухгалтерия сохраняет номер карты (счета) в банке для перечисления зарплаты, за исключением, если работодатель сообщает данные работника в банк для открытия зарплатной карты;

3) оператор обрабатывает персональные данные работника исключительно для исполнения возложенных на работодателя обязанностей, функций и полномочий (пп. 2 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ);

4) оператор передает персональные данные работника в налоговую инспекцию, Пенсионный фонд, Фонд социального страхования, трудовую инспекцию и военный комиссариат в порядке и объёме, предусмотренных законодательством Российской Федерации;

5) обработка сведений о состоянии здоровья работника, связанная с возможностью выполнения им своей трудовой функции (п. 2.3 и 3 ч. 2 ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ);

6) персональные данные необходимы по условиям коллективного договора, Правил внутреннего трудового распорядка, других локальных нормативных актов учреждения-работодателя;

7) обработка персональных данных работников для организации пропускного режима возможна без согласия работника, если порядок организации пропускного режима предусмотрен локальным нормативным актом учреждения-работодателя и работник с ним ознакомлен;

8) исполнение обязанности оператора по опубликованию определённых персональных данных работников (образование, стаж и т.п.) в сети «Интернет», предусмотренной действующим законодательством;

9) обработка персональных данных близких родственников работника для заполнения карточки Т-2, оформления социальных выплат, получения алиментов;

10) обработка персональных данных уволенных работников для выполнения требований налогового, бухгалтерского учета;

11) хранение без согласия заявлений уволенных работников о предоставлении налоговых вычетов с копиями свидетельств о рождении детей.

3.6. Персональные данные, представленные работником, обрабатываются автоматизированным и без использования средств автоматизации способами.

3.7. Анкеты соискателей на заключение трудового договора, которые не подошли, и другая информация о непринятых на работу соискателях, удаляется в течение 30 дней после отказа в приеме на работу.

3.8. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

3.9. Излишне накопленные персональные данные и персональные данные, срок хранения которых истёк, подлежат уничтожению оператором в установленном порядке.

4. Передача и распространение персональных данных работников

4.1. При передаче оператором персональных данных работник должен дать на это согласие в письменной или электронной форме. Если сотрудник оформил согласие на передачу персональных данных в электронной форме, то он подписывает согласие усиленной электронной цифровой подписью.

4.2. Оператор вправе передать информацию, которая относится к персональным данным работника, без его согласия, если такие сведения нужно передать по запросу государственных органов, в порядке, установленном законодательством.

4.3. Оператор не вправе предоставлять персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных законодательством.

4.4. В случае если лицо, обратившееся с запросом, не уполномочено Федеральным законом от 27.07.2006 № 152-ФЗ на получение информации, относящейся к персональным данным работника, оператор обязан отказать лицу в выдаче информации. Лицу, обратившемуся с запросом, выдается уведомление об отказе в выдаче информации, копия уведомления подшивается в личное дело работника.

4.5. Персональные данные работника могут быть переданы оператором представителям работников в порядке, установленном ТК РФ, в том объеме, в каком это необходимо для выполнения указанными представителями их функций.

4.6. Оператор не вправе распространять персональные данные работников третьим лицам без согласия работника на передачу таких данных, за исключением случае предусмотренных законодательством Российской Федерации.

4.7. Согласие на обработку персональных данных, разрешенных работником для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных (Приложение 4 к Положению).

4.8. Оператор обязан обеспечить работнику возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на распространение персональных данных.

4.9. В случае если из предоставленного работником согласия на распространение персональных данных не следует, что работник согласился с распространением персональных данных, такие персональные данные обрабатываются оператором без права распространения.

4.10. В случае если из предоставленного работником согласия на передачу персональных данных не следует, что работник не установил запреты и условия на обработку персональных данных или не указал категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, оператор

обрабатывает такие персональные данные без возможности передачи (распространения, предоставления, доступа) неограниченному кругу лиц.

4.11. Согласие работника на распространение персональных данных может быть предоставлено оператору:

- непосредственно;

- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

4.12. В согласии на распространение персональных данных работник вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении работником данных запретов и условий не допускается.

4.13. Оператор обязан в срок не позднее трех рабочих дней с момента получения согласия работника на распространение персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных работника для распространения.

4.14. Передача (распространение, предоставление, доступ) персональных данных, разрешенных работником для распространения, должна быть прекращена в любое время по его требованию. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) работника, а также перечень персональных данных, обработка которых подлежит прекращению.

4.15. Действие согласия работника на распространение персональных данных прекращается с момента поступления оператору требования, указанного в пункте 4.14 настоящего Положения.

4.16. Работник вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Федерального закона от 27.07.2006 № 152-ФЗ или обратиться с таким требованием в суд. Оператор или третье лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования работника или в срок, указанный во вступившем в законную силу решении суда. Если такой срок в решении суда не указан, то оператор или третье лицо обязаны прекратить передачу персональных данных работника в течение трех рабочих дней с момента вступления решения суда в законную силу.

4.17. Оператор должен уведомлять РКН о зарубежных поставщиках, которые получают доступ к личным данным работников (ст. 12 Федерального закона от 27.07.2006 № 152-ФЗ). РКН принимает решение,

можно ли передавать данные этим контрагентам или нельзя. О своем решении РКН уведомляет работодателя в течение 10 рабочих дней.

5. Хранение и защита персональных данных работников

5.1. Оператор при обработке персональных данных работников обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.2. Оператор принимает следующие меры по защите персональных данных:

1) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных, в первую очередь разработка политики в отношении обработки персональных данных, принятие и утверждение соответствующей документации;

2) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

3) применение сертифицированного антивирусного программного обеспечения с регулярно обновляемыми базами;

4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учет машинных носителей персональных данных;

6) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

7) назначение лица (лиц), ответственного(ых) за обработку персональных данных, которое(ые) осуществляет(ют) организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных;

8) установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными (должностными) обязанностями, соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;

9) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе мер по обнаружению, предупреждению и

ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

10) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

11) обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику оператора в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

12) осуществление внутреннего контроля и аудита;

13) определение типа угроз безопасности и уровней защищенности персональных данных при их обработке в информационных системах;

14) систематический контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Контроль за выполнением настоящих требований организуется и проводится оператором (ответственным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором.

5.3. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

5.4. Уровни защищенности персональных данных.

1) Первый уровень защищенности. Если оператор отнес информационную систему к первому типу угрозы или если тип угрозы второй,

но оператор обрабатывает специальные категории персональных данных более 100 тысяч физических лиц без учета работников;

2) Второй уровень защищенности. Если тип угрозы второй и оператор обрабатывает специальные категории персональных данных работников вне зависимости от их количества или специальные категории персональных данных менее чем 100 тысяч физических лиц, или любые другие категории персональных данных более чем 100 тысяч физических лиц, или при третьем типе угрозы оператор обрабатывает специальные категории данных более чем 100 тысяч физических лиц.

3) Третий уровень защищенности. Если при втором типе угрозы оператор обрабатывает общие персональные данные работников или менее чем 100 тысяч физических лиц, или при третьем типе угрозы оператор обрабатывает специальные категории персональных данных работников или менее чем 100 тысяч физических лиц, или при третьем типе угрозы оператор обрабатывает биометрические персональные данные, или при третьем типе угрозы оператор обрабатывает общие персональные данные более чем 100 тысяч физических лиц.

4) Четвертый уровень защищенности. Если при третьем типе угрозы оператор обрабатывает только общие персональные данные работников или менее чем 100 тысяч физических лиц.

5.5. При четвертом уровне защищенности персональных данных оператор:

1) обеспечивает режим безопасности помещений, в которых размещаете информационную систему;

2) обеспечивает сохранность носителей информации;

3) утверждает перечень работников, допущенных до персональных данных;

4) использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

5.6. При третьем уровне защищенности персональных данных дополнительно к мерам, перечисленным в пункте 5.5 настоящего Положения, оператор назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

5.7. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от руководителя оператора и подотчетно ему.

Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, следующие сведения:

1) цель обработки персональных данных;

2) описание мер, направленных на обеспечение выполнения оператором обязанностей по обработке персональных данных и обеспечению их безопасности.

5.8. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.9. В целях защиты персональных данных на бумажных носителях оператор:

1) приказом назначает работника, непосредственно ответственного за ведение кадровой документации и обработку персональных данных работников оператора;

2) ограничивает допуск в помещения, где хранятся документы, которые содержат персональные данные работников;

3) личные дела и личные карточки работников, иные документы, содержащие персональные данные работников, хранит в бумажном виде в папках, прошитые и пронумерованные по страницам, которые находятся у специалиста по кадрам в специально отведенном шкафу, запирающемся на ключ и обеспечивающем защиту от несанкционированного доступа. В конце рабочего дня все личные дела, личные карточки, иные документы, содержащие персональные данные работников, сдаются специалисту по кадрам.

4) хранит трудовые книжки работников в сейфе;

5) использование и хранение биометрических персональных данных работников вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

5.8. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только ответственным лицом.

5.9. Допуск к документам, содержащим персональные данные работников, внутри учреждения-работодателя осуществляется на основании локального нормативного акта и приказа учреждения-работодателя (Приложение 6 к Положению).

5.10. Ответственное лицо, иные работники учреждения, допущенные к персональным данным работников, подписывают обязательства о

неразглашении персональных данных (Приложение 5 к Приложению). В противном случае до обработки персональных данных работников они не допускаются.

5.11. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных (см. Раздел 4 «Передача и распространение персональных данных работников» настоящего Положения).

5.12. Передача информации, содержащей сведения о персональных данных работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

5.13. Персональные данные работников могут также храниться в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли устанавливаются специалистом по кадрам и сообщаются индивидуально работникам, имеющим доступ к персональным данным работников.

5.14. Изменение паролей производится специалистом по кадрам не реже одного раза в два месяца.

5.15. Доступ к персональным данным работника имеют директор учреждения - работодателя, его заместители, а также непосредственный руководитель работника, специалист по кадрам, делопроизводитель - к тем данным, которые необходимы для выполнения конкретных функций. Доступ специалистов других отделов к персональным данным осуществляется на основании приказа директора о разрешении работать конкретным лицам с персональными данными определённых работников с указанием цели и направлений обработки, а также объёма обрабатываемых персональных данных.

5.16. Копировать и делать выписки из персональных данных работника разрешается исключительно в служебных целях с письменного разрешения директора или его заместителя.

5.17. Все работники учреждения-работодателя, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с настоящим Положением, требованиями законодательства Российской Федерации.

5.18. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

5.19. При принятии решений, затрагивающих интересы работника, оператор не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного поступления.

5.20. Оператор не вправе принимать решения, затрагивающие интересы работника, основываясь на данных, допускающих двоякое толкование. В случае если на основании персональных данных работника невозможно достоверно установить какой-либо факт, оператор предлагает работнику представить письменные разъяснения.

6. Гарантии конфиденциальности персональных данных работников

6.1. Информация, относящаяся к персональным данным работника, является служебной тайной и охраняется законом.

6.2. Работник - субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.3. Сведения, должны быть представлены субъекту персональных данных оператором в доступной форме.

6.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом от 27.07.2006 № 152-ФЗ;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

8) наименование, должность или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена таковому лицу;

9) иные сведения, предусмотренные настоящим Федеральным законом или другими Федеральными законами.

6.5. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта

персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных абзацем вторым настоящего пункта.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

Оператор обязан рассмотреть возражение, указанное в абзаце третьем настоящего пункта, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

6.6. Оператор обязан оценивать вред, который может возникнуть, если будут нарушены правила обработки персональных данных. В соответствии с Требованиями к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», утверждёнными приказом Роскомнадзора от 27.10.2022 № 178 (далее – Требования).

6.7. Степени вреда: высокая; средняя; низкая.

6.8. В соответствии с Приказом Роскомнадзора от 27.10.2022 № 178 потенциальный ущерб оценивает: сотрудник, ответственный за обработку персональных данных в учреждении-работодателе или комиссия.

Оператор определяет степень потенциального вреда: высокую, среднюю или низкую (см. Памятку в Приложении 7 к Положению).

Высокая, если:

1) обрабатываются сведения, характеризующие биометрические персональные данные (физиологические и биологические особенности), которые используются для установления личности;

2) обрабатываются специальные категории персональных данных (национальная принадлежность, состояние здоровья, сведения о судимости и др.);

3) производится обработка данных несовершеннолетних лиц для договоров, в которых они являются контрагентами, поручителями или выгодоприобретателями;

4) персональные данные обезличиваются;

5) обработка персональных данных российских граждан осуществляется иностранным лицом;

6) осуществляется сбор персональных данных с использованием баз за границей.

Степень средняя в случаях:

1) распространение персональных данных в интернете или их предоставление неограниченному кругу лиц;

2) если персональные данные обрабатываются в целях, которые отличаются от первоначальных;

3) когда согласие на обработку персональных данных получено на сайте в сети «Интернет»;

4) продвижения товаров (услуг) с использованием базы потребителей, которой владеет другой оператор.

Степень определяется как низкая при условии:

1) ведения источников персональных данных, которые являются общедоступными (адресные книги или справочники). Сведения в такие источники включаются с письменного согласия субъекта (ст. 8 Федерального закона от 27.07.2006 № 152-ФЗ);

2) назначения ответственным за обработку персональных данных внештатного сотрудника.

Если в процессе деятельности могут быть причинены разные степени ущерба, то применяется более высокая. После проведения оценки составляется акт, который закрепляет её результаты.

6.9. Для проведения оценки вреда руководитель учреждения-работодателя издает приказ «О проведении оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (Приложение 7 к Положению).

6.10. Для отнесения вреда к какой-либо степени, оператору требуется составить специальный Акт оценки вреда (образец Акта в Приложении 8 к Положению).

Акт оценки вреда должен содержать:

а) наименование или фамилию, имя, отчество (при наличии) и адрес оператора;

б) дату издания акта оценки вреда;

в) дату проведения оценки вреда;

г) фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;

д) степень вреда, которая может быть причинена субъекту персональных данных, в соответствии с подпунктами 2.1-2.3 пункта 2 Требований.

6.11. Акт оценки вреда в электронной форме, подписанный в соответствии с федеральным законом электронной подписью, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью.

6.12. Оператор обязан уведомить в бумажном или электронном виде Роскомнадзор в течение 24 часов, если зафиксирует утечку персональных данных, и начать внутреннее расследование. В уведомлении необходимо указать информацию об инциденте, предполагаемые причины, вред и меры, которые приняты, чтобы устранить последствия. Для внутреннего расследования приказом руководителя создается рабочая группа из заместителя руководителя учреждения, работника, ответственного за обработку персональных данных, специалиста по кадрам, бухгалтера (если есть), IT-специалиста. О результатах расследования в течение 72 часов после того, как выявлен инцидент уведомляется Роскомнадзор.

7. Порядок уничтожения персональных данных

7.1. Порядок уничтожения персональных данных работников определяет процедуру уничтожения персональных данных, хранящихся на бумажных носителях, на съёмных машинных носителях, в виде файлов на персональных компьютерах (далее – ПК) и сетевых папках, а также в составе баз данных информационных систем с обработкой персональных данных (далее – ИСПДн) в учреждении – работодателе.

7.2. Под уничтожением персональных данных понимают действия, в результате которых становится невозможным восстановить содержание ранее полученных персональных данных.

7.3. Данный порядок применяется:

1) ко всем процессам в учреждении-работодателе, в которых ведется обработка персональных данных;

2) ко всем структурным подразделениям и работникам учреждения-работодателя, принимающим участие в процессах обработки персональных данных и осуществляющих поддержку функционирования ИСПДн;

3) к сотрудникам, непосредственно обрабатывающим персональные данные.

7.4. Персональные данные, обрабатываемые оператором, подлежат уничтожению в следующих случаях:

1) при необоснованном получении персональных данных (например, обработка персональных данных, найденных в сети «Интернет», или получение пересланных персональных данных физлица без его согласия);

2) при выявлении факта неправомерной обработки персональных данных (незаконная передача персональных данных третьим лицам, необеспечение сохранности данных и т.д.);

3) при достижении целей обработки персональных данных (например, при истечении срока действия ранее исполненного договора) или в случае утраты необходимости в достижении цели обработки персональных данных, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ;

4) при отзыве субъектом персональных данных согласия на обработку его персональных данных, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ;

5) при истечении сроков хранения персональных данных, установленных нормативным правовым актом (НПА) Российской Федерации;

6) при получении соответствующего указания Роскомнадзора;

7) при изменении, признании утратившими силу нормативных правовых актов, устанавливающих правовые основания обработки персональных данных;

8) иных установленных законодательством Российской Федерации случаях.

7.5. Должностным лицом, ответственным за документооборот и архивирование, осуществляется систематический контроль за выявлением документов, содержащих персональные данные с истекшими сроками хранения.

7.6. Инициатором уничтожения персональных данных выступает заместитель директора.

7.7. Вопрос об уничтожении документов, содержащих персональные данные с истекшими сроками хранения либо персональных данных в соответствии с п. 7.4 Положения, рассматривается на основании приказа руководителя учреждения - работодателя на заседании экспертной комиссии учреждения - работодателя (далее - Комиссия) в составе не менее чем трёх человек, персональный состав которой утверждается приказом руководителя учреждения - работодателя. Председателем Комиссии является должностное лицо, ответственное за обработку персональных данных. В случае уничтожения персональных данных на машинных носителях информации, файлов на ПК и сетевых папках, в состав Комиссии дополнительно включается работник, отвечающий в учреждении за функционирование информационных технологий.

7.8. По итогам заседания Комиссии составляются протокол и Акт о выделении к уничтожению документов, прилагаемую к нему опись уничтожаемых дел. Акт о выделении к уничтожению документов подписывается председателем и членами Комиссии и утверждается руководителем учреждения-работодателя.

7.9. Комиссия определяет перечень персональных данных (документов, их содержащих), подлежащих уничтожению, удостоверяется в обоснованности уничтожения персональных данных и включает уничтожаемые персональные данные и/или их носители в Акт об уничтожении персональных данных (Приложение 9 к Положению).

7.10. Руководитель подразделения, в котором обрабатывались запланированные к уничтожению документы (носители), содержащие персональные данные, проверяет перечень уничтожаемых персональных данных в подготовленном комиссией Акте об уничтожении персональных данных (далее – Акт).

7.11. В срок, не превышающий 10 (десяти) рабочих дней с даты приказа, предусмотренного п. 7.7 Положения, Комиссия способами, определёнными в п. 7.12, осуществляет уничтожение персональных данных (их носителей), по окончании которого все члены комиссии подписывают Акт. Руководитель учреждения - работодателя утверждает данный Акт.

7.12. Уничтожение предполагает, что персональные данные станут непригодными для дальнейшего использования, обработки и передачи. Уничтожение персональных данных по окончании срока их обработки на электронных носителях производится путем механического нарушения их целостности, не позволяющим произвести считывание и восстановление персональных данных, или удаления с электронных носителей методами и средствами гарантированного удаления остаточной информации.

Персональные данные работников в электронном виде стираются с информационных носителей, либо физически уничтожаются сами носители, на которых хранится информация. Цифровые носители будут зачищены, а материальные носители безвозвратно уничтожены.

Уничтожение носителей, содержащих персональные данные субъектов персональных данных, производится в присутствии всех членов Комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в Акте об уничтожении персональных данных или их носителей.

Кадровые документы, которые имеют длительные сроки хранения, нельзя уничтожать без оснований. Каждый документ необходимо проверить. После истечения срока нормативного хранения документы, которые содержат персональные данные работника, подлежат уничтожению.

Уничтожение бумажных носителей персональных данных, а также компакт дисков осуществляется путём измельчения на мелкие части с помощью специализированного уничтожителя (шрёдера).

Уничтожение части персональных данных, если это допускается бумажным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

Уничтожение персональных данных, содержащихся на машиночитаемых сменных носителях, осуществляется путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления данных. Вышеуказанное достигается путем деформирования или нарушения целостности носителя.

В случае уничтожения персональных данных на машиночитаемых сменных носителях, допускающих многократную запись, допускается применение специализированных программ многократной перезаписи удаляемой информации (Eraser, PrivaZer, CCcleaner, Secure Erase, Crypto Erase и подобные) с количеством циклов перезаписи не менее семи.

Уничтожение персональных данных, содержащихся в файлах на ПК или сетевых папках осуществляется с применением специализированных программ многократной перезаписи удаляемой информации (Eraser, PrivaZer, CCcleaner, Secure Erase, Crypto Erase и подобные) с количеством циклов перезаписи не менее семи.

Уничтожение персональных данных, хранящихся в базах данных ИСПДн, осуществляется непосредственно оператором или ответственным администратором ИСПСДн с использованием встроенных механизмов ИСПДн или серверов, на которых размещены ИСПДн, и должно предусматривать:

1) удаление соответствующих записей или значений полей таблиц в основной базе данных;

2) удаление записей или значений полей таблиц в резервных (тестовых) копиях базы данных;

3) очистка swap-файла операционной системы при завершении работы сервера или перезагрузке;

4) удаление снэпшотов соответствующих виртуальных машин, на которых размещены сервера с ИСПДн;

5) наличие механизма выгрузки из журнала регистрации ИСПДн информации об уничтоженных персональных данных в соответствии с требованиями настоящего пункта.

7.13. Оператор обязан фиксировать факт того, что уничтожил персональные данные, двумя документами:

1) актом об уничтожении персональных данных;

2) выгрузкой из журнала регистрации событий в информационной системе персональных данных.

Если оператор обрабатывает персональные данные вручную, - для подтверждения их уничтожения будет достаточно одного Акта.

В случае если обработка персональных данных осуществляется оператором одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение ПДн субъектов ПДн, являются Акт об уничтожении персональных данных (Приложение №1) и Выгрузка из журнала ИСПДн.

Приказом руководителя учреждения-работодателя утверждаются формы документов: Акта об уничтожении персональных данных и Выгрузки из журнала регистрации событий в информационной системе персональных данных (Приложение 9 к Положению).

7.14. Акт об уничтожении персональных данных должен содержать следующие обязательные реквизиты:

1) наименование оператора персональных данных;

2) адрес оператора персональных данных;

3) ФИО и должности лиц – работников оператора, входящих в Комиссию и непосредственно уничтоживших персональные данные;

4) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

5) перечень категорий уничтоженных персональных данных;

6) наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

7) наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

8) способ уничтожения персональных данных;

9) причину уничтожения персональных данных;

10) дату уничтожения персональных данных.

7.15. Обязательные реквизиты выгрузки из журнала регистрации событий в информационной системе персональных данных содержат:

1) ФИО субъектов персональных данных или иная информация, относящаяся к определённым физическим лицам, чьи персональные данные были уничтожены;

2) перечень категорий уничтоженных персональных данных;

3) наименование информационной системы персональных данных, из которой они были уничтожены;

4) причину уничтожения персональных данных;

5) дату уничтожения персональных данных.

7.16. В случае если Выгрузка из журнала ИСПДн не позволяет указать отдельные сведения, предусмотренные данным Положением, недостающие сведения вносятся в Акт об уничтожении персональных данных.

7.17. Акт об уничтожении персональных данных и выгрузка из журнала ИСПДн подлежат хранению не менее 3 (трёх) лет с момента уничтожения персональных данных у работника, ответственного за обработку персональных данных в учреждении - работодателе.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

8.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, в соответствии со ст. 24 Федерального закона от 27.07.2006 № 152-ФЗ привлекаются к дисциплинарной, материальной ответственности в порядке, установленном п/п «в» п. 6 ч. 1 ст. 81, ст. 90, 191 ТК РФ, гражданско-правовой ответственности (ст.ст. 15, 151 Гражданского кодекса Российской Федерации),

административной ответственности (ст.ст. 5.39, 13.11, 13.12. – 13.14, 19.7 Кодекса Российской Федерации об административных правонарушениях), иными федеральными законами, а также привлекаются к уголовной ответственности (ст.ст. 137, 138, 140 Уголовного кодекса Российской Федерации).

Характер ответственности зависит от состава и тяжести правонарушения, степени вреда, причиненного субъекту персональных данных.

8.2. Руководитель оператора за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные работника.

8.3. РКН осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

8.4. Субъект персональных данных вправе обжаловать действия (бездействия) оператора, осуществляющего обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ или иным образом нарушающего его права и свободы, в уполномоченный орган по защите прав субъектов персональных данных (РКН) или в судебном порядке.

8.5. Учреждение-работодатель, являющееся оператором по смыслу настоящего Положения, в обязательном порядке уведомляет Комитет по культуре о результатах проверки соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных и о всех принятых Управлением решениях.

Приложение 1 к Положению о работе с
персональными данными работников
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»

Типовая форма согласия
на обработку персональных данных работника
(гражданина, претендующего на заключение трудового договора)

_____
(наименование учреждения культуры)

Я, _____
_____
_____
_____
(фамилия, имя, отчество, паспортные данные, адрес регистрации)

в соответствии со ст.9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю свое согласие Муниципальному бюджетному учреждению культуры «Одинцовский Центр культурного развития» (МБУК «ОЦКР») (далее по тексту – Оператор) ИНН 5032201414, адрес местонахождения: Московская область, г. Одинцово, ул. Маршала Жукова, д.36 на обработку своих персональных данных с целью:

- обеспечения соблюдения требований законодательства Российской Федерации;
- трудоустройства;
- оформления и регулирования трудовых отношений;
- отражения информации в кадровых документах;
- обеспечения безопасных условий труда;
- исполнения трудового договора;
- обеспечения личной безопасности, защиты жизни и здоровья;
- идентификации личности.

Перечень персональных данных, на обработку которых даю согласие:

- дата и место рождения;
- биографические сведения;
- сведения об образовании;
- сведения о местах работы;
-сведения о семейном положении, детях (фамилия, имя, отчество, дата рождения);
-сведения о ближайших родственниках и свойственниках;
- сведения о месте регистрации, проживания;
- контактная информация (номера телефонов, профили в социальных сетях);
- адрес электронной почты;
- реквизиты документа, удостоверяющего личность (копия паспорта);
- биометрические данные;

- сведения о доходах.

Оператор вправе осуществлять следующие действия с указанными выше персональными данными путем автоматизированной обработки и обработки без использования средств автоматизации, предусмотренных пунктом части первой статьи 3 федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных»[2]:

- сбор;
- систематизацию;
- накопление;
- хранение;
- уточнение (обоснование, изменение);
- использование;
- распространение/передачу;
- блокирование;
-уничтожение.

Настоящее согласие действует со дня его подписания до дня его отзыва в письменной форме.

«_____» _____ 20___ г. _____ _____

Подпись *ФИО*

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

«_____» _____ 20___ г. _____ _____

Подпись *ФИО*

Настоящее согласие может быть отозвано Субъектом в любой момент. Согласие отзывается путем направления письменного заявления субъекта персональных данных Оператору.

Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст.14 Федерального закона от 27.06.2006 г. №152-ФЗ)

Приложение 2 к Положению о работе с
персональными данными работников
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»

Типовая форма разъяснения
субъекту персональных данных юридических последствий отказа
предоставить свои персональные данные

Мне, _____,
(фамилия имя отчество (при наличии)
разъяснены юридические последствия моего отказа предоставить свои персональные данные работодателю:
_____
_____.
(наименование учреждения культуры)

В соответствии со статьями 57, 65, 69, 86 Трудового кодекса Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» работодателем определен перечень персональных данных, которые субъект персональных данных обязан предоставить работодателю в связи с поступлением, прохождением и прекращением работы.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений трудовой договор не может быть заключен.

«_____» _____ 20__ г.

_____
(подпись) (фамилия, имя, отчество (при наличии)

Приложение 3 к Положению о работе с
персональными данными работников
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»

Типовая форма отзыва согласия на обработку
персональных данных работника

Я, _____,
(фамилия, имя, отчество)
в соответствии с частью 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» отзываю у работодателя: Муниципального автономного (бюджетного) учреждения культуры (дополнительного образования) «_____
_____»
согласие на обработку моих персональных данных.
Мне разъяснено, что в случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных, необходимых для исполнения трудового договора, соблюдения требований трудового законодательства, иных законодательных и нормативных правовых актов Российской Федерации, локальных актов учреждения - работодателя, при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

«_____» _____ 20__ г.

_____
(подпись) (фамилия, имя, отчество (при наличии)

Приложение 4 к Положению о работе с персональными данными работников Муниципального бюджетного учреждения культуры «Одинцовская концертная организация»

Примерная форма
согласия на обработку персональных данных,
разрешенных субъектом персональных данных для распространения

Я, _____, паспорт серии _____№ _____, выдан ХХ.ХХ.20___ _____, код подразделения ХХХ-ХХХ, , руководствуясь статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», заявляю о согласии на распространение работодателем – Муниципальным автономным (бюджетным) учреждением культуры (дополнительного образования) «_____» ОГРН _____ (далее – учреждение), моих персональных данных с целью размещения информации обо мне для получения работниками учреждения информации о моей профессиональной деятельности, а также размещения информации во внутренней рабочей сети учреждения в следующем порядке:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
Персональные данные	Фамилия	Да	Да		
	Имя	Да	Да		
	Отчество	Да	Да		
	Год рождения	Нет			
	Месяц рождения	Да	Нет	*Только сотрудникам отдела кадров и бухгалтерии*	
	Дата рождения	Да	Нет	*Только сотрудникам отдела кадров и*	

				бухгалтерии	
	Место рождения	Да	Нет	*Только сотрудникам отдела кадров и бухгалтерии*	
	Адрес	Нет			
	Семейное положение	Да	Нет	*Только сотрудникам отдела кадров и бухгалтерии*	
	Образование	Да	Нет	*Только сотрудникам отдела кадров и бухгалтерии*	
	Должность	Да	Нет	*Только сотрудникам отдела кадров и бухгалтерии*	
	Социальное положение	Нет	Нет		
	Доходы	Да	Нет	*Только сотрудникам отдела кадров и бухгалтерии*	
	...				
Специальные категории персональных данных	Состояние здоровья	Да	Нет	*Только сотрудникам отдела кадров и бухгалтерии*	
	Сведения о судимости	Да	Нет	*Только сотрудникам отдела кадров и*	

				бухгалтерии	
	…				
Биометрические персональные данные	Цветное цифровое фотографическое изображение лица	Да	Да		
	…				

Сведения об информационных ресурсах учреждения, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
https://_____@_____ru	Предоставление сведений работникам учреждения, допущенным к обработке персональных данных в учреждении
Официальный сайт учреждения	Предоставление сведений: фамилия, имя, отчество, об образовании, квалификации, должности, стаже работы в профессии, наградах, званиях, победах в конкурсах. Размещение цветных фотографий, видео о профессиональной деятельности с моим изображением

Настоящее согласие дано мной добровольно и действует со дня его подписания до отзыва в установленном законом порядке.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования работодатель обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)

Приложение 5 к Положению о работе с
персональными данными работников
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»

Примерная форма обязательства
ответственного лица (иного работника) о неразглашении
персональных данных работников

Я, _____,
(ФИО)
_____,
(паспортные данные)

работающий в Муниципальном автономном (бюджетном) учреждении культуры «Одинцовская концертная организация» (далее – учреждение), в должности _____поним
аю, что в соответствии с трудовым договором, должностной инструкцией, приказом директора учреждения получаю доступ к персональным данным физических лиц, в том числе работников учреждения, а именно:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о трудовом и общем стаже;
- сведения о квалификации (повышении квалификации, переквалификации) работника;
- сведения об аттестации работника;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- сведения о состоянии здоровья работника;
- сведения о наличии (отсутствии) судимостей;
- адрес места жительства;
- контактные данные;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;

- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- дела, содержащие материалы внутренних расследований, осуществления аудита, проверок вышестоящими или сторонними организациями;
- информация справочно-информационного банка данных по персоналу (картотеки, журналы);
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству оператора, руководителям структурных подразделений оператора, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, муниципальные и государственные вышестоящие и контролирующие органы;
- документированная информация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства оператора);
- документы по планированию, учету, анализу и отчетности в части работы с персоналом оператора.

Я также понимаю, что во время исполнения своих обязанностей мне предстоит заниматься сбором, обработкой, накоплением, хранением и обновлением персональных данных физических лиц.

Я обязуюсь хранить в тайне известные мне конфиденциальные сведения, информировать руководителя учреждения о фактах нарушения порядка обращения с персональными данными, о ставших мне известным попытках несанкционированного доступа к персональным данным.

Я обязуюсь соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц, знакомиться только с теми служебными документами, к которым получаю доступ в силу исполнения своих должностных обязанностей.

Я понимаю, что разглашение такого рода информации может нанести прямой или косвенный ущерб физическим лицам. В связи с этим даю обязательство при обработке персональных данных соблюдать все описанные в Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных», постановлении Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных актах, требования.

Я предупрежден(а) о том, что в случае разглашения мной персональных данных, их повреждения или их утраты по моей вине или неосторожности я несу ответственность в соответствии с действующим законодательством Российской Федерации.

«_____» _____ 20____ г.

_____/_____

Подпись Расшифровка подписи

Приложение 6 к Положению о работе с
персональными данными работников
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»

ОБРАЗЕЦ ПРИКАЗА
Об обработке и защите персональных данных

«____»_____20__г. № _____

В целях обеспечения защиты прав и свобод работников при обработке персональных данных, во исполнение положений Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных _____
(должность и ФИО работника)

2. Допустить к обработке персональных данных следующих работников:

№	ФИО и должность работника	Группа обрабатываемых персональных данных
1		
2		
3		

3. Возложить на лиц, указанных в пунктах 1 и 2 настоящего приказа, персональную ответственность за работу по защите персональных данных работников.

4. Ответственному за обработку персональных данных в срок до «____»_____20____г. предоставить на подпись работникам, осуществляющих обработку персональных данных, обязательство о неразглашении персональных данных.

Директор
_____/_____
(подпись) (расшифровка подписи)

С приказом ознакомлены:
_____ _____
(подпись) (расшифровка подписи)

_____ _____
(подпись) (расшифровка подписи)

Приложение 7 к Положению о работе с
персональными данными работников
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»

ОБРАЗЕЦ ПРИКАЗА

О проведении оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Создать Комиссию по проведению оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

2. Включить в состав Комиссии следующих лиц:

председатель Комиссии — *должность, ФИО*;

заместитель председателя Комиссии — *должность, ФИО*;

секретарь Комиссии – *должность, ФИО*;

члены комиссии:

— *должность, ФИО;*

— *должность, ФИО*;

— *должность, ФИО*;

— *должность, ФИО*.

3. Комиссии в целях оценки степени вреда, который может быть причинен субъектам персональных данных:

1) составить перечень информационных систем, используемых в Муниципальном бюджетном учреждении «Одинцовская концертная организация» (далее - учреждение), в которых обрабатываются персональные данные;

2) составить перечень персональных данных, которые обрабатываются в данных системах;

3) оценить степень вреда, который может быть причинен субъектам персональных данных - работникам учреждения при обработке

в информационных системах в соответствии с требованиями, установленными приказом Роскомнадзора от 27.10.2022 №178;

4) оценить систему защиты персональных данных в учреждении при их обработке в информационных системах персональных данных на соответствие степени вреда, который может быть причинен субъектам персональных данных.

4. По результатам работы Комиссии оформить Акт оценки вреда не позднее XX.XX.202_.

5. Контроль исполнения настоящего приказа возложить на председателя комиссии *ФИО.*

Директор _____ _____

(подпись) (ФИО)

С приказом ознакомлены:

_____ _____

(подпись) (ФИО)

_____ _____

(подпись) (ФИО)

Приложение 8 к Положению о работе с
персональными данными работников
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»

АКТ № _____

оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

г. Одинцово Московской области «____»_____202__г.

№ 1

Комиссия Муниципального автономного (бюджетного) учреждения культуры (дополнительного образования) «_____» (далее – учреждение), действующая на основании приказа от ХХ.ХХ.202__ № _____, в составе:

- председатель комиссии — должность, ФИО;
- секретарь комиссии - должность, ФИО;
- члены комиссии

должность, ФИО;
должность, ФИО;
должность, ФИО;

провела ХХ.ХХ.202_ оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», и установила следующее:

1. Персональные данные субъектов персональных данных обрабатываются в следующих информационных системах *(перечислить по факту):*

1.1. *Официальный сайт учреждения.*

1.2. Кадрово-бухгалтерская система «1С».

1.3._____.

2. Учреждение осуществляет обработку следующих персональных данных:

— сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить личность для целей пропускной системы на основе биометрических персональных данных;

— специальных категорий персональных данных — состояния здоровья, сведений о судимости для целей трудоустройства на работу и соблюдения требований трудового законодательства;

— персональных данных, предполагающих получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц.

3. Степень вреда, который может быть причинен субъектам персональных данных, — высокая.

4. Защищенность информации в информационных системах учреждения соответствует требованиям, установленным постановлением Правительства РФ от 01.11.2012 №1119.

Содержание Акта подтверждаем своими подписями:

Председатель комиссии _____ _____
(подпись) (ФИО)

Секретарь комиссии _____ _____
(подпись) (ФИО)

Приложение 9 к Положению о работе с
персональными данными работников
Муниципального бюджетного
учреждения культуры
«Одинцовская концертная организация»

ОБРАЗЕЦ ПРИКАЗА
Об утверждении документов, подтверждающих уничтожение персональных данных

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить следующие прилагаемые формы документов:

1) Акт об уничтожении персональных данных - при неавтоматизированной обработке персональных данных (Приложение 1 к приказу).

2) Выгрузка из журнала регистрации событий в информационной системе персональных данных - при автоматизированной обработке персональных данных (Приложение 2 к приказу).

2. Назначить работников, ответственных за уничтожение персональных данных и составление подтверждающих документов:

1) Должность, ФИО - при неавтоматизированной обработке данных.

2) Должность, ФИО - при автоматизированной обработке данных.

3. При уничтожении персональных данных руководствоваться требованиями Федерального закона «О персональных данных» и приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

4. Контроль исполнения настоящего приказа возложить на *заместителя директора ФИО либо указать иное лицо.*

Директор _____ _____
(подпись) (ФИО)

Приложение 1
к приказу от _____ №_____

ФОРМА АКТА

УТВЕРЖДАЮ
Директор МБУК «ОКО»
_____ _____
(подпись) (ФИО)
М.П.

Акт № ____
об уничтожении персональных данных работников
Муниципального бюджетного учреждения культуры
«Одинцовская концертная организация»

г. Одинцово Московской области «_____»_____202__г.

Настоящим актом подтверждается прекращение обработки и уничтожение ХХ.ХХ.20ХХ следующих персональных данных работников Муниципального бюджетного учреждения культуры «Одинцовская концертная организация»:

№ п/п	Ф.И.О. сотрудника, чьи перс-данные уничтожены	Перечень категорий уничтоженных перс-данных	Наименование материального носителя перс-данных	Наименование информационной системы, из которой удалили перс-данные	Способ уничтожения перс-данных	Дата и причина уничтожения перс-данных
1						
2	...	...	...	...	...	...

Уничтожил персональные данные работников в соответствии с настоящим актом:
Должность, ФИО работника _____ _____

Приложение 2
к приказу от _____ №_____

ФОРМА ВЫГРУЗКИ

Выгрузка из журнала регистрации событий в информационной системе персональных данных

Ф. И. О. субъекта персональных данных	**Перечень категорий уничтоженных данных**	**Наименование информационной системы**	**Причина уничтожения персональных данных**	**Дата уничтожения персональных данных**
ФИО	Общие персональные данные	«1С: Зарплата и кадры»	Достижение цели обработки	XX.XX.20XX

Должность, ФИО работника _____ _____