Приложение 1

к приказу комитета

по культуре города Барнаула

от 21.04.2023 №50

ПОЛОЖЕНИЕ  
об обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных комитета по культуре города Барнаула

1. Общие положения
   1. Положение об обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных комитета по культуре города Барнаула (далее – Положение) разработано во исполнение Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и других нормативно-правовых актов, регулирующих правоотношения, связанные с обеспечением безопасности персональных данных (далее – ПДн) при их обработке в информационной системе персональных данных (далее – ИСПДн) комитета по культуре города Барнаула (далее – Оператор).
   2. Настоящее Положение определяет политику Оператора по обработке ПДн и является общедоступным документом.
   3. Требования настоящего Положения являются обязательными для исполнения всеми сотрудниками Оператора, получившими доступ к ПДн.
   4. В настоящем Положении используются следующие понятия:
      1. ПДн – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);
      2. Оператор – комитет по культуре города Барнаула, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку ПДн, а также определяющий цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;
      3. обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;
      4. автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники;
      5. распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц;
      6. предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;
      7. блокирование ПДн – временное прекращение обработки ПДн   
         (за исключением случаев, если обработка необходима для уточнения ПДн);
      8. уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн;
      9. обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;
      10. информационная система ПДн – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;
      11. трансграничная передача ПДн – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
   5. Обработка персональных данных осуществляется Оператором по адресам: Алтайский край, г.Барнаул, пр-кт Ленина, 6, пр-кт Социалистический, 34 с 26.11.1997 на основании включения в реестр Операторов, осуществляющих обработку персональных данных, регистрационный номер 09-0064941 от 10.09.2009.
   6. Срок обработки ПДн работников Оператора составляет 75 лет.
2. Общие принципы и условия обработки ПДн
   1. Оператор осуществляет обработку ПДн своих работников и лиц, не являющихся таковыми.
   2. При обработке ПДн Оператор руководствуется следующими принципами:
      1. обработка ПДн должна осуществляться на законной и справедливой основе;
      2. обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;
      3. содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;
      4. при обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн;
      5. хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.3. При обработке ПДн Оператор выполняет следующие условия их обработки:

2.3.1. обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн за исключением случаев, определенных пп. 2-11 ч.1 ст. 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

2.3.2. обработка специальных категорий ПДн осуществляется в случаях, предусмотренных ч.2. ст. 10 Федерального закона от 27.07.2006 №152-ФЗ   
«О персональных данных»;

2.3.3. обработка биометрических ПДн осуществляется только при наличии согласия в письменной форме субъекта ПДн за исключением случаев, предусмотренных ч.2. ст. 11 Федерального закона от 27.07.2006 №152-ФЗ   
«О персональных данных»;

2.4. Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора либо путем принятия соответствующего акта (далее – поручение Оператора). Лицо, осуществляющее обработку ПДн по поручению Оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные действующим законодательством, соблюдать конфиденциальность ПДн. В поручении Оператора должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со ст. 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

2.5. Оператор самостоятельно определяет содержание, объем, цели обработки и сроки хранения ПДн.

2.6. Принятые Оператором документы, определяющие политику Оператора в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений доводятся до сотрудников Оператора в части касающихся их.

1. Правовые основания обработки ПДн
   1. Оператор осуществляет обработку ПДн на основании следующих нормативно-правовых актов Российской Федерации:
      1. Федеральный закон от 16.07.1999 №165-ФЗ «Об основах обязательного социального страхования»;
      2. Федеральный закон от 06.12.2011 №402-ФЗ «О бухгалтерском учете»;
      3. Трудовой кодекс Российской Федерации;
      4. Налоговый кодекс Российской Федерации;
      5. Федеральный закон от 15.12.2001 №167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
      6. постановление Правительства Российской Федерации от 02.06.2008 №420 «О Федеральной службе государственной статистики».
2. Цели обработки ПДн
   1. Обработка ПДн осуществляется в целях:
      1. осуществления бухгалтерского и налогового учета, ведения документооборота с Межрайонными инспекциями Федеральной налоговой службы по Алтайскому краю, отделениями Фонда пенсионного и социального страхования Российской Федерации по Алтайскому краю, Управлением Федеральной службой государственной статистики по Алтайскому краю и Республике Алтай;
      2. оплаты труда работников Оператора;
      3. осуществления полномочий органа местного самоуправления города Барнаула.
3. Категории обрабатываемых ПДн, источники их получения

5.1. В ИСПДн Оператора обрабатываются следующие категории ПДн работников Оператора: фамилия, имя, отчество, номер расчетного счета, сведения о заработной плате, паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ), идентификационный номер налогоплательщика, сведения о лицевом счете в системе индивидуального (персонифицированного) учета, адрес регистрации по месту жительства.

5.2. Персональные данные предоставляются субъектом ПДн лично или представителем субъекта ПДн.

1. Сведения о третьих лицах, участвующих в обработке ПДн
   1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки Оператор с согласия субъектов ПДн в ходе своей деятельности предоставляет ПДн следующим организациям:

6.1.1. межрайонным инспекциями Федеральной налоговой службы по Алтайскому краю;

6.1.2. отделениям Фонда пенсионного и социального страхования Российской Федерации по Алтайскому краю;

6.1.3. Управлению Федеральной службой государственной статистики по Алтайскому краю и Республике Алтай

6.1.4. при получении мотивированных запросов органам прокуратуры, правоохранительным органам, органам безопасности, Государственной инспекции труда в Алтайском крае, иным органам, уполномоченным запрашивать информацию о работниках Оператора в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

1. Права и обязанности Оператора
   1. Оператор обязан немедленно прекратить по требованию субъекта ПДн обработку его ПДн.
   2. Оператор обязан разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.
   3. При сборе ПДн Оператор обязан предоставить субъекту ПДн по его просьбе информацию, предусмотренную ч.7 ст. 14 Федерального закона от 27.07. 2006 № 152-ФЗ «О персональных данных».
   4. Если предоставление ПДн является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.
   5. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта ПДн или его представителя.
   6. Оператор обязан предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие ПДн. Оператор обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.
   7. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) по запросу этого органа необходимую информацию в течение 10 рабочих дней с даты получения такого запроса.
   8. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн Оператор обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Оператор обязан осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.
   9. В случае подтверждения факта неточности ПДн Оператор на основании сведений, предоставленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.
   10. В случае выявления неправомерной обработки ПДн, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Оператора. В случае, если обеспечить правомерность обработки ПДн невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.
   11. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.
   12. В случае отзыва субъектом ПДн согласия на обработку его ПДн Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Оператором и субъектом ПДн либо если Оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.
   13. В случае отсутствия возможности уничтожения ПДн в течение установленного срока, Оператор осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.
2. Права субъектов ПДн
   1. Субъект ПДн имеет право на получение сведений об обработке его ПДн Оператором.
   2. Субъект ПДн вправе требовать от Оператора, который их обрабатывает, уточнения этих ПДн, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
   3. В случае, если сведения, указанные в ч. 7 ст. 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 ст. 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», и ознакомления с такими ПДн не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.
   4. Субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в ч. 7 ст. 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в ч. 4 ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.
   5. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с ч. 8 ст. 14 Федерального закона от 27.07.2006 №152-ФЗ   
      «О персональных данных».
   6. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
3. Меры по обеспечению безопасности ПДн при их обработке
   1. Оператор при обработке ПДн принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.
   2. Обеспечение безопасности ПДн достигается, частности:
      1. определением угроз безопасности ПДн при их обработке в ИСПДн;
      2. применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
      3. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
      4. учетом машинных носителей ПДн;
      5. обнаружением фактов несанкционированного доступа к ПДн и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;
      6. восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
      7. установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

9.2.8. контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

1. Ответственность за разглашение информации, связанной с ПДн
   1. Лица, виновные в нарушении требований настоящего Федерального законодательства, несут ответственность, предусмотренную законодательством Российской Федерации.
   2. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, установленных настоящим Федеральным законом, а также требований к защите ПДн, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.