

УТВЕРЖДАЮ

Председатель Комитета


Гойкина Н.В.
« 25 » 12 2016г.

ПОЛИТИКА

обработки и защиты персональных данных в Комитете по делам архивов при Правительстве Удмуртской Республики

1. Общие положения

1.1. Настоящая политика в отношении обработки и защиты персональных данных (далее — Политика) разработана в соответствии с ч. 2 ст. 18.1 Федерального закона РФ «О персональных данных» №152-ФЗ от 27 июля 2006 года в (в ред. № 261-ФЗ от 25.07.2011) и действует в отношении всех персональных данных (далее — ПДн), которые Комитет по делам архивов при Правительстве Удмуртской Республики (далее - Комитет) получает в ходе основной производственной деятельности от субъектов персональных данных (далее — субъект ПДн), являющихся сотрудниками Комитета, близкими родственниками сотрудников Комитета и третьими лицами, как сторона гражданско-правового договора, заявителями на предоставление государственной услуги по организации исполнения запросов.

1.2. Комитет обеспечивает защиту обрабатываемых ПДн от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями следующих законодательных и нормативных документов:

- Трудовой кодекс Российской Федерации (гл. 14) от 30.12.2001 г.
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 01.11.2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденный приказом Гостехкомиссии России от 30.08.2002 № 282;

- Руководящий документ ФСБ России от 21.02.2008 № 149/5-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;
- Руководящий документ ФСТЭК России от 15.02.2008 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Руководящий документ ФСТЭК России от 14.02.2008 «Методика определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»;
- ГОСТ 34.603-92 «Виды испытаний автоматизированных систем»;
- РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов».
- Приказ ФСБ РФ от 10.07.2014г. №378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности».

1.3. Изменение настоящей политики.

1.3.1. Комитет имеет право вносить изменения в настоящую политику, указывая в заголовке документа о внесенных изменениях и дате последнего обновления редакции.

1.3.2. Новая редакция настоящей политики вступает в силу с момента ее размещения на сайте Комитета в сети Интернет, если иное не предусмотрено новой редакцией настоящей политики.

1.3.3. Оригинал действующей редакции настоящей политики хранится по адресу нахождения Комитета: 426004, г.Ижевск, ул.Ломоносова, д.5.

2. Термины и определения

- Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).
- Обработка персональных данных — 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.
- Автоматизированная обработка персональных данных — обработка ПДн с помощью средств вычислительной техники.
- Информационная система персональных данных (ИСПД) — совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
- Общедоступные персональные данные — ПДн, доступ к которым предоставлен для неограниченного круга лиц по согласию субъекта ПДн в соответствии с Федеральным законом ФЗ-152 «О персональных данных».

- Блокирование персональных данных — временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).
- Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

3. Обработка персональных данных

3.1. Обработка ПДн в Комитете осуществляется в соответствии с утвержденными положениями об обработке и защите ПДн.

3.2. Получение ПДн в Комитете от субъекта ПДн.

3.2.1. Все ПДн Комитета получает от самого субъекта ПДн в рамках трудовых, гражданско-правовых отношений. Если ПДн субъекта ПДн получены третьей стороны, то субъект ПДн письменно уведомляется Комитет об этом.

3.2.2. Комитет сообщает субъекту ПДн о составе обрабатываемых ПДн, источнике их получения, целях, способах и сроках обработки данных ПДн, а также о возможных последствиях отказа субъекта ПДн от обработки его ПДн Комитетом.

3.2.3. Комитет получает ПДн в ходе следующих процедур обработки ПДн:

- передача субъектом ПДн необходимых документов (трудовая книжка, справка о доходах и др.) в рамках трудовых отношений;
- копирование оригиналов документов, предоставленных субъектом ПДн (паспорт, свидетельство ИНН, документ об образовании и др.) в рамках гражданско-правовых отношений, в случаях исполнения договора по инициативе субъекта ПДн.

3.3. Цели обработки ПДн в Комитете:

- осуществление трудовых отношений
- осуществление гражданско-правовых отношений;

3.4. Категории субъектов ПДн, обрабатываемых в Комитете:

- физические лица, состоящие с Комитетом в трудовых отношениях;
- физические лица, являющие близкими родственниками сотрудников Комитета;
- физические лица, уволившиеся из Комитета;
- физические лица, состоящие с Комитетом в гражданско-правовых отношениях

3.5. Состав ПДн обрабатываемых в Комитете, состав документов, содержащих ПДн, цели и правовые основания обработки по категориям субъектов ПДн, сроки хранения документов представлены в утвержденном Председателем Комитета перечне ПДн, в том числе:

- сведения, полученные при осуществлении трудовых отношений с субъектом ПДн (Ф.И.О., паспортные данные, место жительства, ИНН, сведения о воинском учете, образовании, сведения о близких родственниках и др.);
- сведения, полученные при осуществлении гражданско-правовых отношений (Ф.И.О., паспортные данные, место жительства, свидетельство ОГРН и др.);

3.6. Обработка ПДн в Комитете ведется с использованием средств автоматизации (электронные носители ПДн) и без использования средств автоматизации (бумажные носители ПДн).

3.7. Хранение ПДн в Комитете осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем того требуют цели обработки ПДн, за исключением случаев, когда срок хранения ПДн установлен Федеральными законами или договором, стороной которого является субъект ПДн.

3.8. ПДн, полученные Комитетом от субъекта ПДн, хранятся как на бумажных носителях, так и в электронном виде.

3.9. ПДн на бумажных носителях хранятся в запираемых шкафах и сейфах в защищаемых помещениях.

3.10. ПДн в электронном виде хранятся на жестких дисках компьютеров сотрудников Комитета и файловом сервере.

3.11. В Комитете запрещено размещать электронные документы, содержащие ПДн, в открытых электронных каталогах (файлообменниках).

3.12. Уничтожение ПДн осуществляется Комитетом в случае достижения целей обработки ПДн в срок, не превышающий 30 (тридцати) дней с даты достижения целей обработки ПДн и производится в соответствии с утвержденной Председателем Комитета инструкцией о порядке уничтожения носителей ПДн.

3.13. Уничтожение носителей ПДн на бумажных носителях в Комитете производится путем дробления (измельчения), с составлением соответствующего акта об уничтожении носителей ПДн.

3.14. ПДн на электронных носителях уничтожаются путем форматирования носителя, без возможности последующего восстановления информации.

3.15. Передача ПДн осуществляется Комитетом в следующих случаях если:

- субъект ПДн выразил свое согласие передачу своих ПДн;
- передача ПДн предусмотрена законодательством Российской Федерации.

3.16. Перечень организаций, которым передаются ПДн Комитета:

- Пенсионный фонд Российской Федерации для учета (на законных основаниях);
- Федеральная налоговая служба Российской Федерации (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- иные государственные и муниципальные органы и организации на законном основании или с согласия субъекта ПДн или уведомления субъекта о передаче его ПДн, если это не нарушает права и законные интересы субъекта ПДн.

4. Защита персональных данных

4.1. В соответствии с требованиями нормативных документов в Комитете создана система защиты ПДн, состоящая из подсистем правовой, организационной и технической защиты:

- подсистема правовой защиты представляет собой комплекс организационно-распорядительных и нормативных документов, обеспечивающих создание и функционирование системы защиты ПДн (далее — СЗПД);
- подсистема организационной защиты включает в себя организацию структуры управления СЗПД, контрольно-пропускного и внутриобъектового режимов, разрешительной системы, защиты информации при работе с персоналом, партнерами и сторонними лицами, аналитической работы;
- подсистема технической защиты включает в себя комплекс программных и программно-аппаратных средств, обеспечивающих защиту ПДн, при их обработке.

4.2. Основные организационные и технические меры по защите ПДн, используемые в Комитете:

4.2.1. Контрольно-пропускной пост расположен при входе в здание Комитета. Установлено преграждающее устройство - турникет. Пост состоит из одного сотрудника ФГУП «Охрана» МВД России по УР. На посту расположена контрольная панель охранной сигнализации. Проход посетителей до поста охраны свободный. Посетитель может самостоятельно пройти в здание после того как назовет фамилию имя и отчество или должность сотрудника Комитета, к которому он пришел..

4.2.2. Внутриобъектовый режим предусматривает допуск сотрудников в помещения Комитета на основании правил внутреннего трудового распорядка и допуск посетителей под контролем сотрудников Комитета на местах. Доступ в помещения где находятся средства обработки ПДн, а так же ПДн на бумажном носителе ограничен.

4.2.3. Разрешительная (разграничительная) система представляет собой совокупность организационно-правовых норм и требований, устанавливаемых Председателем Комитета, с целью обеспечения правомерного ознакомления и использования сотрудниками Комитета ПДн, необходимых для исполнения своих должностных обязанностей.

4.2.4. Разрешительная система включает в себя две ограничительные процедуры: допуск сотрудника к обработке ПДн и непосредственный доступ к носителям ПДн. Разграничен доступ в помещения, где ведется обработка ПДн.

4.2.5. Организационные мероприятия:

- назначение ответственного за организацию обработки ПДн, в том числе защиту;
- утверждение состава постоянно действующей экспертной комиссии по защите ПДн;
- утверждение перечня сотрудников Комитета, допущенных к обработке ПДн, права их доступа к конкретным носителям ПДн и перечень разрешенных действий;
- проведение инструктажа о порядке и принципах обработки и защиты ПДн сотрудникам Комитета, участвующим в обработке ПДн, в соответствии с требованиями нормативных документов, утвержденных Председателем Комитета;
- проведение периодического внутреннего контроля и аудита безопасности ПДн;
- осуществление плановых проверок наличия носителей и соблюдения сотрудниками Комитета требований по обработке и защите ПДн;
- организация приема и обработки обращений и запросов физических и юридических лиц;
- проведение экспертизы материалов, предназначенных для открытого опубликования, содержащие ПДн, на наличие в таких материалах только общедоступных ПДн;
- взятие согласий на обработку с субъектов ПДн, при заключении трудовых и гражданско-правовых договоров.

5. Программно-технические меры защиты:

- Для хранения бумажных носителей ПДн предусмотрены запираемые шкафы и сейфы;
- По периметру Комитета установлены камеры видеонаблюдения. Монитор видеонаблюдения и модуль видеозаписи находится на посту охраны;
- При входе в помещения в которых ведется обработка ПДн или в которых установлены средства обработки и хранения ПДн, вывешен список сотрудников имеющих право доступа в данное помещение;
- Установлены индивидуальные пароли доступа сотрудников в информационную систему в соответствии с их должностными обязанностями;
- Для защиты от внедрения вредоносных программ используется лицензионное антивирусное средство защиты с регулярно обновляемыми антивирусными базами;
- Передача ПДн в государственные органы (на законном основании) и банк осуществляется в защищенном виде, с применением средств криптографической защиты;
- Предусмотрена возможность восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним или неумышленных действий (резервное копирование).

6. Основные права и обязанности субъекта ПДн и Комитета

6.1. Права субъекта ПДн при обработке его ПДн.

6.1.1. Субъект ПДн имеет право неограниченного доступа к своим ПДн.

6.1.2. Субъект ПДн имеет право получить от Комитета следующие сведения:

- подтверждение факта обработки ПДн Комитетом;
- правовые основания и цели обработки ПДн;
- цели и применяемые Комитетом способы обработки ПДн;
- наименование и место нахождения Комитета, сведения о лицах (за исключением сотрудников Комитета), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Комитетом или на основании положений Федерального закона;
- сроки обработки и хранения ПДн;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом;
- порядок обращения в Комитет и направление ей запросов;
- порядок обжалования действий или бездействия Комитета по вопросам обработки и ПДн.

6.2. Обязанности субъекта ПДн при обработке его ПДн.

6.2.1. Субъект ПДн обязан предоставить Комитету для обработки полные и достоверные сведения, необходимые для обработки Комитетом.

6.3. Права Комитета при обработке ПДн:

- проверка достоверности обрабатываемых ПДн субъектов ПДн законными способами;
- требование от сотрудников Комитета выполнения требований нормативных документов по обработке и защите ПДн;
- осуществление контроля выполнения требований по обработке ПДн;
- привлечение к ответственности сотрудников Комитета, нарушающих требования законодательства по обработке ПДн.

6.4. Обязанности Комитета при обработке ПДн:

- предоставление субъекту ПДн информации о целях, способах, сроках и перечне действий по обработке его ПДн;
- уведомление субъекта ПДн, в случае если его ПДн были получены не от субъекта ПДн;
- принятие необходимых правовых, организационных и технических мер по защите ПДн от несанкционированного или случайного доступа к ним;
- предоставление письменных ответов на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн;

7. Ответственность

7.1. Ответственность за обработку и защиты ПДн субъектов ПДн несет Комитет.

7.2. За разглашение ПДн и нарушение порядка обработки ПДн вне зависимости от формы их представления, работники Комитета могут быть привлечены к дисциплинарной, административной, гражданской, уголовной и иной, предусмотренной законодательством ответственности.

7.3. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, установленных Федеральным законом, а также требований к защите ПДн, установленных в соответствии с Федеральным законом,

подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.