

Приложение № 1
к приказу АО «КБ «Навигатор»
от 01 июня г. № 08-30/25

**ПОЛИТИКА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
АКЦИОНЕРНОЕ ОБЩЕСТВО
«КОНСТРУКТОРСКОЕ БЮРО «НАВИГАТОР»**

Общие положения

Настоящая Политика обработки персональных данных (далее – Политика):

- является основополагающим внутренним документом Акционерного общества «Конструкторское бюро «Навигатор» (далее – Организация), регулирующим вопросы обработки персональных данных;
- разработана в целях обеспечения соответствия законодательству Российской Федерации обработки, хранения и защиты персональных данных (далее – ПДн) работников Организации, а также субъектов ПДн, не являющихся работниками Организации;
- раскрывает основные категории ПДн, обрабатываемых Организацией, цели, способы и принципы обработки ПДн, права и обязанности Организации при обработке ПДн, права субъектов ПДн, а также перечень мер, применяемых Организацией в целях обеспечения безопасности ПДн при их обработке;
- предназначена для работников Организации, осуществляющих обработку ПДн в целях непосредственной реализации ими закрепленных в Политике принципов, а также является информационным ресурсом для субъектов ПДн, позволяющим определить концептуальные основы деятельности Организации при обработке ПДн.

Источники нормативного правового регулирования вопросов обработки ПДн

Политика Организации в отношении обработки персональных данных определяется на основании следующих нормативных правовых актов Российской Федерации:

- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждено постановлением Правительства Российской Федерации от 15.09.2008 г. № 687;
- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства Российской Федерации от 01.11.2012 г. №1119;
- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Уголовный кодекс Российской Федерации.

Основные термины и понятия, используемые в локальных документах Организации, принимаемых по вопросу обработки ПДн

Автоматизированная обработка персональных данных – обработка ПДн с помощью средств вычислительной техники;

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Оператором для установления личности субъекта ПДн;

Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

Доступ к персональным данным – ознакомление определенных лиц (в том числе работников) с ПДн субъектов, обрабатываемыми Оператором, при условии сохранения конфиденциальности этих сведений;

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

Использование персональных данных – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц;

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем;

Конфиденциальность персональных данных – обязанность лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному 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;

Общедоступные персональные данные – ПДн, доступ неограниченного круга лиц к которым предоставлен на основании федерального закона, субъектом ПДн либо по его просьбе, в том числе данные, которые в соответствии с законодательством подлежат обязательному раскрытию или опубликованию;

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

Распространение – действия, направленные на раскрытие ПДн неопределенному кругу лиц;

Субъект персональных данных – физическое лицо, к которому относятся ПДн;

Трансграничная передача персональных данных – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители с ПДн.

Принципы и общие условия обработки

Обработка ПДн в Организации осуществляется на основе следующих принципов:

- Законность и справедливость целей и способов обработки ПДн.
- Законность и добросовестность целей и способов обработки ПДн.
- Соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Организации.
- Соответствие содержания и объема обрабатываемых ПДн целям обработки ПДн.
- Достоверность ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн.
- Недопустимость объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.
- Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.
- 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 от 27.07.2006 г. № 152-ФЗ «О персональных данных».
- Комплекс мер по защите ПДн направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности ПДн и обеспечивает безопасность ПДн в процессе деятельности Организации.
- Организация, при осуществлении обработки ПДн, обязано принимать необходимые организационные и технические меры, в том числе использовать криптографические средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн.
- Мероприятия по защите ПДн определяются Положением об организации обработки и защиты в Организации, а также приказами, инструкциями и другими внутренними документами Организации.

Обеспечение безопасности ПДн

Для обеспечения безопасности ПДн в Организации применяется необходимый и достаточный комплекс организационных и технических мер, направленных на предотвращение несанкционированных действий, включая:

- несанкционированный доступ,
- уничтожение,
- модификацию,
- блокирование доступа.

Состав комплекса организационных и технических мер строится в соответствии с положениями нормативных и методических документов ФСТЭК России и ФСБ России и обеспечивает реализацию следующих основных правил обеспечения безопасности ПДн:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн;
- распределение персональной ответственности между работниками, участвующими в обработке ПДн, за выполнение требований по обеспечению безопасности ПДн;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- размещение технических средств обработки ПДн, исключающее бесконтрольный доступ к защищаемой информации, включая ПДн;

- ограничение допуска посторонних лиц в помещения Организации, недопущение их бесконтрольного нахождения в помещениях, где ведется работа с ПДн и размещаются технические средства их обработки;
- регулярная проверка знаний работниками, непосредственно осуществляющих обработку ПДн, в части требований действующего законодательства Российской Федерации, а также нормативно-методических документов по защите ПДн (включая положения Политики);
- определение и регулярная актуализация угроз безопасности ПДн при их обработке в информационных системах ПДн;
- организация порядка уничтожения ПДн;
- своевременное выявление нарушений требований разрешительной системы доступа;
- воспитательная и разъяснительная работа с работниками Организации по предупреждению утраты ПДн;
- регулярное обучение работников Организации по вопросам, связанным с обеспечением безопасности ПДн.

Цели обработки персональных данных

Целями обработки ПДн в Организации являются:

- обеспечение требований трудового законодательства Российской Федерации в отношении работников Организации, включая, в том числе.
 - организацию и ведение кадрового учета и делопроизводства,
 - организацию и проведение обучения работников,
 - организацию исчисления и уплаты налога на доходы физических лиц, а также единого социального налога,
- ведение хозяйственной деятельности и предоставление услуг, включая:
 - заключение, исполнение и прекращение гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством и Уставом Организации.

При определении объема и характера обрабатываемых ПДн Организация руководствуется указанными выше целями обработки ПДн.

Сроки обработки

Сроки обработки ПДн определяются в соответствии со сроком действия договора с субъектом ПДн, Приказом Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», Постановлением ФКЦБ России от 16.07.2003 № 03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ», сроком исковой давности, а также иными требованиями законодательства Российской Федерации.

В Организации создаются и хранятся документы, содержащие сведения о субъектах ПДн. Требования к использованию в Организации данных типовых форм документов установлены Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Права и обязанности

Организация как оператор персональных данных, вправе:

- отстаивать свои интересы в суде;

- предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении ПДн в случаях, предусмотренных законодательством;
- поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее – поручение оператора);
- использовать ПДн субъекта без его согласия, в случаях, предусмотренных законодательством.

Организация как оператор персональных данных, обязано:

- принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, связанных с обработкой ПДн, предусмотренных законодательством Российской Федерации, включая:
 - назначение ответственного за организацию обработки ПДн;
 - назначение ответственного за организацию защиты ПДн;
 - издание документов, определяющих политику обработки ПДн, локальных правовых актов по вопросам обработки ПДн, а также локальных правовых актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
 - применение правовых, организационных и технических мер по обеспечению безопасности ПДн;
 - осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн действующему законодательству Российской Федерации и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам оператора;
 - оценка вреда, который может быть причинен субъектам ПДн в случае нарушения законодательства Российской Федерации, соотношение указанного вреда и принимаемых в Организации мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации;
 - ознакомление работников Организации, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику в отношении обработки ПДн, локальными правовыми актами по вопросам обработки ПДн.
- разрабатывать, утверждать и обеспечивать неограниченный доступ к документу (опубликовать в информационно-телекоммуникационной сети), определяющему политику обработки ПДн;
- осуществлять обработку ПДн субъектов с соблюдением принципов и правил, предусмотренных законодательством Российской Федерации.

Субъект персональных данных имеет право:

- требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать перечень своих ПДн, обрабатываемых Организацией и источник их получения;

- получать информацию о сроках обработки своих ПДн, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке неправомерные действия или бездействия при обработке его ПДн;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Заключительные положения

С учетом обязанности оператора ПДн по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки ПДн.

Политика является внутренним документом Организации, общедоступной и подлежит размещению на официальном сайте Организации.

Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите ПДн, но не реже одного раза в три года

Контроль исполнения требований Политики осуществляется ответственным за организацию обработки и защиты ПДн Организации.

Ответственность должностных лиц Организации, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту ПДн, определяется в соответствии с законодательством Российской Федерации и внутренними документами Организации.