ПОЛИТИКА защиты, обработки и обеспечения безопасности персональных данных в ООО «Профит-Лига»

1. Общие положения

1.1. Политика обработки и обеспечения безопасности персональных данных (ПДн) в ООО «Профит-Лига» (далее Политика) является локальным нормативным актом ООО «Профит-Лига» (далее Общество), разработанным в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и определяет основные принципы, цели и условия обработки ПДн, а также меры защиты ПДн в Обществе.

1.2. Контроль за исполнением требований настоящей Политики осуществляется Ответственным за организацию обработки ПДн.

1.3. Настоящая Политика разработана в целях реализации требований законодательства Российской Федерации в области обработки ПДн и обеспечения Безопасности ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.4. Общество вправе вносить изменения в Политику с соблюдением требований законодательства Российской Федерации и нормативных правовых актов.

2. Термины и определения

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

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 настоящим Федеральным законом;

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

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;

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

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

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

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;

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

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

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

Ответственный за обеспечение безопасности ПДн – лицо, ответственное за обеспечение безопасности ПДн, за реализацию и непрерывность соблюдения установленных мер защиты и осуществляющее контроль функционирования средств защиты информации, применяемых в ИСПДн Общества.

Ответственный за организацию обработки ПДн – лицо, осуществляющее внутренний контроль за соблюдением Обществом и ее работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

Работник Общества – лицо, осуществляющее свою деятельность в Обществе на основании трудового договора, и имеющее возможность получить доступ к обработке ПДн, как с применением автоматизированных средств обработки ПДн, так и без таковых.

Система защиты ПДн (СЗПДн) – комплекс организационных и технических мер, определенных с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

Средства защиты информации (СЗИ) – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

Субъект ПДн – физическое лицо, которое прямо или косвенно определено или определяемо с помощью ПДн.

Уполномоченный орган по защите прав субъектов ПДн – федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн.

ФЗ «О персональных данных» – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Иные термины, значение которых не определено в настоящей Политике, используются в значении, которое придается им законодательством Российской Федерации и нормативными правовыми актами.

3. Принципы обработки ПДн

3.1. Обработка ПДн Обществом осуществляется на основе принципов:

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Цели и правовые основания обработки ПДн

4.1. Целью настоящего Положения является:

– обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

– защиты жизни, здоровья или иных важных интересов субъектов ПДн;

– заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных законодательством и Уставом Общества;

– организации кадрового учета, обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам;

– ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и кадровом перемещении в рамках штатного расписания, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым и Налоговым кодексами Российской Федерации, федеральными законами;

– организации и проведения практики, студентов по программам высшего профессионального обучения и среднего профессионального обучения;

– реализации контрольно-пропускного режима в Общества, обеспечения сохранности имущества;

– раскрытия информации об органах управления, ведение необходимой корпоративной и иной документации в соответствии с законодательством Российской Федерации;

– формирования справочных материалов для внутреннего информационного обеспечения деятельности Общества, ее обособленных подразделений, входящих в корпоративную структуру Общества;

– исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации;

– выдачи доверенностей представителям Общества, организаций, привлекаемых для реализации проектов деятельности Общества;

– совершения иных действий, не противоречащих законодательству Российской Федерации;

– контроля и повышения качества обслуживания клиентов, обучения работников, урегулирования претензий и спорных ситуаций, а также защиты прав и законных интересов Общества путем записи, хранения и анализа телефонных переговоров работников Общества с клиентами, представителями контрагентов и иными лицами при использовании служебных средств связи.

4.2. Основаниями для обработки ПДн Субъектов ПДн Общества, в том числе, являются:

– Гражданский кодекс Российской Федерации;

– Налоговый кодекс Российской Федерации;

– Трудовой кодекс Российской Федерации;

– Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон от 01.04.1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

– Федеральный закон от 29.12.2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

– Федеральный закон от 06.12.2011 г. № 402-ФЗ «О бухгалтерском учете»;

– Федеральный закон от 07.08.2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

– Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление Правительства РФ № 1119);

– Устав Общества.

4.3. В Обществе осуществляется Автоматизированная обработка ПДн и Обработка ПДн без использования средств автоматизации путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления, предоставления, доступа), блокирования, удаления, уничтожения ПДн.

4.4. Общество в своей деятельности исходит из того, что при взаимодействии с Обществом Субъект ПДн предоставляет точную и достоверную информацию, о своих ПДн, а также своевременно извещает Общество об изменении своих ПДн.

5. Категории ПДн и категории Субъектов ПДн

5.1. Общество обрабатывает ПДн следующих категорий Субъектов ПДн:

– работники;

– кандидаты на трудоустройство;

– контрагенты (физические лица, работники контрагентов);

– практиканты;

– работники сторонних организаций (в рамках договорных отношений);

– посетители Общества;

– зарегистрированных пользователей сайта ООО «Профит-Лига» – www.pr-lg.ru;

– учредители Общества.

5.2. В соответствии с положениями Постановления Правительства РФ № 1119 в Общества обрабатываются следующие категории ПДн без использования средств автоматизации и с использованием средств автоматизации:

– иные категории ПДн – ПДн, не отнесенные к категориям: специальные, биометрические и общедоступные ПДн;

– биометрические категории ПДн – сведения, которые характеризуют физиологические и биологические особенности человека.

5.3. Полный перечень ПДн и категории субъектов ПДн утверждается Перечнем обрабатываемых персональных данных.

6. Условия обработки ПДн Субъектов ПДн и условия передачи ПДн третьим лицам

6.1. Общество обрабатывает ПДн Субъектов ПДн в соответствии с локальными нормативными актами Общества, разработанными в соответствии с требованиями законодательства Российской Федерации в области ПДн.

6.2. Обработка ПДн в Обществе допускается в следующих случаях:

– обработка ПДн осуществляется с согласия Субъекта ПДн на обработку его ПДн;

– обработка ПДн, разрешенных субъектом ПДн для распространения, осуществляется с согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, представляемого субъектом персональных данных отдельно от других согласий субъекта персональных данных на обработку его ПДн;

– обработка ПДн необходима в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах; для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации;

– обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, является Субъект ПДн, а также для заключения договора по инициативе Субъекта ПДн;

– обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением случаев, установленных в ст. 15 ФЗ «О персональных данных», при условии обязательного обезличивания ПДн;

– осуществляется обработка ПДн, полученных из открытых источников, размещенных в них Субъектом ПДн либо по его просьбе;

– обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6.3. Если иное не предусмотрено федеральным законом, Общество вправе поручить обработку ПДн другому лицу, на основании заключаемого с этим лицом договора, при условии наличия согласия Субъекта ПДн. Лицо, осуществляющее обработку ПДн по поручению Общества, обязано соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ «О персональных данных».

6.4. В поручении третьему лицу указываются цели обработки и перечень действий (операций) с ПДн, которые могут быть совершены данным лицом, устанавливается его обязанности по обеспечению Конфиденциальности ПДн и Безопасности ПДн при их обработке, а также требования к защите обрабатываемых

ПДн в соответствии с ФЗ «О персональных данных».

6.5. Общество не осуществляет трансграничную передачу ПДн (передачу на территорию стран, обеспечивающих адекватную защиту ПДн с согласия субъекта ПДн).

6.6. Общество не принимаются решения, порождающие юридические последствия в отношении Субъектов ПДн или иным образом затрагивающие их права и законные интересы, на основании исключительно Автоматизированной обработки ПДн, за исключением случая наличия согласия в письменной форме Субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов Субъекта ПДн.

6.7. Общество прекращает обработку ПДн в следующих случаях:

– при выявлении неправомерной обработки ПДн, осуществляемой Обществом или лицом, действующим по поручению Общества. Общество в срок, не превышающий трех рабочих дней с даты такого выявления, прекращает неправомерную обработку ПДн или обеспечивает прекращение неправомерной обработки ПДн лицом, действующим по поручению Общества, и устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Общества в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Общество уведомляет Субъекта ПДн или его представителя, а в случае, если обращение или запрос были направлены в уполномоченный орган по защите прав Субъектов ПДн, также этот орган;

– при достижении цели обработки ПДн Общество прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Общества) и уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Общества) 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 Обществом и Субъектом ПДн либо если Общество не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных ФЗ «О персональных данных» или другими федеральными законами.

– при отзыве Субъектом ПДн согласия на обработку своих ПДн Общество прекращает обработку ПДн или обеспечивает ее прекращение (если Обработка ПДн осуществляется другим лицом, действующим по поручению Общества) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Общества) 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 Обществом и Субъектом ПДн либо если

Общество не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных ФЗ «О персональных данных» или другими федеральными законами.

6.8. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в настоящем разделе, Общество осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Общества) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.1. Обработка аудиозаписей телефонных переговоров

6.1.1. В целях исполнения договорных обязательств, повышения качества обслуживания, а также обеспечения защиты прав и законных интересов Общества, в Обществе может осуществляться запись телефонных переговоров с контрагентами, их представителями, работниками и иными лицами, взаимодействующими с Обществом.

6.1.2. Аудиозаписи телефонных переговоров могут содержать персональные данные субъектов персональных данных, включая, но не ограничиваясь: голосом, номером телефона, сведениями о должности, фамилии, имени, отчестве, а также иной информацией, сообщаемой в рамках делового взаимодействия.

6.1.3. Обработка аудиозаписей осуществляется Обществом на следующих правовых основаниях:

– исполнение договоров, стороной которых либо выгодоприобретателем или поручителем является субъект персональных данных;

– осуществление прав и законных интересов Общества, включая обеспечение качества обслуживания, предотвращение спорных ситуаций и защиту имущественных интересов;

– иные основания, предусмотренные законодательством Российской Федерации.

6.1.4. Обработка аудиозаписей осуществляется исключительно в целях:

– фиксации и подтверждения договорных договорённостей;

– контроля качества взаимодействия с контрагентами;

– обучения и оценки работников Общества;

– рассмотрения обращений, претензий и спорных ситуаций;

– защиты прав и законных интересов Общества.

6.1.5. Общество исходит из того, что взаимодействие с контрагентами и их представителями осуществляется в рамках деловых отношений, и персональные данные, сообщаемые в ходе телефонных переговоров, предоставляются субъектами персональных данных добровольно в рамках исполнения договорных обязательств.

Общество не осуществляет целенаправленный сбор избыточных персональных данных в рамках телефонных переговоров. Работникам запрещается запрашивать у субъектов персональных данных сведения, не относящиеся к целям обработки, за исключением случаев, прямо предусмотренных законодательством Российской Федерации.

6.1.6. Аудиозаписи телефонных переговоров хранятся в течение срока,

необходимого для достижения целей обработки, но не более 2 (двух) месяцев с даты записи, если иное не требуется, для:

– рассмотрения претензий и споров;

– исполнения требований законодательства Российской Федерации;

– защиты прав и законных интересов Общества.

По истечении срока хранения аудиозаписи подлежат уничтожению либо обезличиванию в установленном порядке.

6.1.7. Доступ к записям телефонных переговоров предоставляется только уполномоченным работникам Общества в пределах их должностных обязанностей, в том числе работникам Департамента правовых вопросов/Юридического отдела, Службы безопасности, Департамента персонала и Отдела кадров, исключительно для достижения целей обработки персональных данных, предусмотренных настоящей Политикой.

6.1.8. Общество принимает необходимые организационные и технические меры для защиты аудиозаписей от неправомерного доступа, изменения, удаления, копирования и распространения в соответствии с требованиями законодательства Российской Федерации и локальных нормативных актов Общества.

7. Согласие на обработку ПДн

7.1. Получение и обработка ПДн в случаях, предусмотренных ФЗ «О персональных данных», осуществляется Обществом с согласия Субъекта ПДн. Согласие на обработку ПДн может быть дано Субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя Субъекта ПДн полномочия данного представителя на дачу согласия от имени Субъекта ПДн проверяются Обществом.

7.2. В случаях, предусмотренных ФЗ «О персональных данных», обработка ПДн осуществляется Обществом только с согласия в письменной форме Субъекта ПДн. Равнозначным содержащему собственноручную подпись Субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в соответствии с Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

7.3. Письменное согласие Субъекта ПДн должно включать:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

7.4. Субъект ПДн дает Обществу согласие на обработку ПДн свободно, по своей воле и в своем интересе. Согласие на обработку ПДн может быть отозвано Субъектом ПДн путем направления в Общество письменного заявления в свободной форме. В этом случае Общество обязуется прекратить обработку, а также уничтожить все имеющиеся в Обществе ПДн в сроки, установленные ФЗ «О персональных данных». Передача ПДн третьим лицам осуществляется Обществом с согласия Субъекта

7.5. ПДн в соответствии с требованиями законодательства Российской Федерации.

7.6. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, оформляется отдельно от иных согласий субъекта ПДн на обработку его ПДн. Требования к содержанию согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

8. Права Субъектов ПДн

8.1. Для обеспечения соблюдения установленных законодательством прав Субъектов ПДн, в Обществе разработан и введен порядок работы с обращениями и запросами Субъектов ПДн, а также порядок предоставления Субъектам ПДн информации, установленной законодательством Российской Федерации в области ПДн.

8.2. Субъект ПДн или его законный представитель имеет право на получение информации, касающейся обработки ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Обществом;
- правовые основания и цели обработки ПДн;
- цели и применяемые Обществом способы обработки ПДн;
- наименование и местонахождение Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Обществом или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему Субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления Субъектом ПДн прав, предусмотренных ФЗ «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Общества, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами в области ПДн.

8.3. Общество предоставляет указанную информацию при обращении или на основании соответствующего письменного запроса Субъекта ПДн или его представителя, содержащего: номер основного документа, удостоверяющего личность Субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие Субъекта ПДн в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Обществом, подпись Субъекта ПДн или его представителя.

8.4. Субъект ПДн вправе требовать от Общества уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки ПДн, а также принимать предусмотренные законодательством Российской Федерации в области ПДн меры по защите своих прав.

8.5. Для реализации и защиты своих прав и законных интересов в части обеспечения правомерности обработки ПДн и обеспечения Безопасности ПДн Субъект ПДн имеет право обратиться к Обществу.

8.6. Если Субъект ПДн считает, что Общество осуществляет обработку ПДн с нарушением требований ФЗ «О персональных данных» или иным образом нарушаетего права и свободы, Субъект ПДн вправе обжаловать действия или бездействие Общества в Уполномоченный орган по защите прав Субъектов ПДн или в судебном порядке.

8.7. Право Субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе, если доступ Субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

9. Права и обязанности Общества

9.1. Общество вправе:

– отстаивать свои интересы в судебных органах;

– предоставлять ПДн Субъектов третьим лицам, если это предусмотрено законодательством Российской Федерации (правоохранительные, налоговые органы и др.);

– отказывать в предоставлении ПДн в случаях, предусмотренных

законодательством Российской Федерации;

– использовать ПДн Субъекта ПДн без его согласия, в случаях, предусмотренных законодательством Российской Федерации.

9.2. Обязанности Общества:

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

2. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

2.1) перечень персональных данных;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

9.3. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

3) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 настоящего Федерального закона;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.

9.4. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона.

10. Обеспечение безопасности ПДн

10.1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам, в частности, относятся:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения

настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

10.2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети «Интернет», с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

10.3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

10.4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

10.5. Для обеспечения Безопасности ПДн Общество принимает необходимые и достаточные организационные и технические меры для защиты ПДн Субъектов ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий, включающие, в том числе:

- определение угроз безопасности ПДн при их обработке в ИСПДн;
- применение организационных и технических мер по обеспечению Безопасности ПДн при обработке ПДн в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Постановлением Правительства РФ № 1119 уровни защищенности ПДн;
- применение прошедших в установленном порядке процедуру оценки соответствия СЗИ;
- оценка эффективности принимаемых мер по обеспечению безопасности

ПДн до ввода в эксплуатацию ИСПДн;

- учет Работников Общества, допущенных к обработке ПДн;
- учет материальных Носителей ПДн;
- обнаружение фактов НСД к ПДн и принятием мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контроль за принимаемыми мерами по обеспечению Безопасности ПДн и уровня защищенности ИСПДн.

10.6. Комплекс мероприятий, предусмотренных Постановлением Правительства РФ № 1119 и приказами о составе и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, по обеспечению Безопасности ПДн в Обществе определяется в локальных нормативных актах Общества, с учетом результатов оценки возможного вреда Субъекту ПДн, который может быть нанесен в случае нарушения Безопасности его ПДн, актуальности угроз Безопасности ПДн, а также установления уровня защищенности ПДн.

10.7. Работники Общества, имеющие доступ к ПДн не вправе их использовать в личных целях, размещать в сети интернет и иных ресурсах.

11. Порядок рассмотрения обращений и запросов субъектов персональных данных

11.1. Субъект персональных данных или его представитель вправе направить в Общество обращение или запрос, связанный с обработкой персональных данных, в целях получения информации, уточнения персональных данных, блокирования или уничтожения персональных данных, прекращения обработки персональных данных, а также в целях реализации иных прав, предусмотренных законодательством Российской Федерации.

11.2. Обращение или запрос направляется субъектом персональных данных в письменной форме одним из следующих способов:
– почтовым отправлением по адресу местонахождения Общества;
– посредством направления электронного документа, подписанного усиленной квалифицированной электронной подписью субъекта персональных данных;
– иными способами, предусмотренными законодательством Российской Федерации.

11.3. Обращение или запрос должен содержать:

1. фамилию, имя, отчество субъекта персональных данных или его представителя;
2. сведения об основном документе, удостоверяющем личность;
3. сведения, подтверждающие участие субъекта персональных данных в отношениях с Обществом (номер договора, дата, иные идентификаторы), либо сведения, подтверждающие факт обработки оператором персональных данных субъекта;
4. Суть обращения или запроса;

5. подпись субъекта персональных данных или его представителя.

11.4. Общество рассматривает обращение или запрос и предоставляет ответ в срок, не превышающий **30 календарных дней** с даты его получения, если иной срок не установлен законодательством Российской Федерации.

11.5. В случае необходимости продления срока рассмотрения обращения или запроса (например, получения дополнительных данных или документов) Общество направляет субъекту персональных данных уведомление с указанием причин продления и нового срока предоставления ответа. Указанный срок не может превышать 45 календарных дней.

11.6. В случае подтверждения факта неточности, неполноты, незаконности или избыточности персональных данных Общество обязано в срок, не превышающий **7 рабочих дней**, уточнить, заблокировать или уничтожить персональные данные и уведомить об этом субъекта персональных данных.

11.7. Общество прекращает обработку персональных данных субъекта и уничтожает их в случаях и сроки, установленные Федеральным законом № 152-ФЗ и настоящей Политикой, в том числе при отзыве субъектом согласия на обработку персональных данных, при достижении целей обработки или при выявлении неправомерной обработки.

11.8. Субъект персональных данных вправе обжаловать действия или бездействие Общества, связанные с обработкой персональных данных, в уполномоченный орган по защите прав субъектов персональных данных либо в судебном порядке.

12. Конфиденциальность персональных данных и порядок доступа работников Общества к персональным данным

12.1. Общество обеспечивает соблюдение конфиденциальности персональных данных и недопущение их раскрытия третьим лицам без правовых оснований либо согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации.

12.2. Доступ к персональным данным предоставляется только тем работникам Общества, которым такой доступ необходим в связи с исполнением ими трудовых обязанностей.

12.3. Уровни и категории доступа работников к персональным данным определяются внутренними локальными актами Общества, исходя из принципа минимально необходимого доступа.

12.4. Ответственный за организацию обработки персональных данных обеспечивает ведение перечня работников, имеющих доступ к персональным данным, а также учет всех случаев предоставления доступа.

12.5. Работники, получающие доступ к персональным данным, обязаны:

1. соблюдать режим конфиденциальности;
2. использовать персональные данные исключительно в целях исполнения своих должностных обязанностей;
3. не допускать копирования, передачи, распространения, уничтожения или изменения персональных данных, если такие действия не предусмотрены их должностными обязанностями;
4. соблюдать требования внутренних локальных актов Общества, регулирующих

порядок обработки персональных данных.

12.6. Работники Общества, имеющие доступ к персональным данным, проходят обязательное ознакомление с положениями настоящей Политики, нормативными актами Общества в области защиты и обработки персональных данных, а также обучение требованиям законодательства Российской Федерации.

12.7. Все действия по обработке персональных данных (доступ, изменение, уничтожение и иные операции) подлежат регистрации и учету в информационных системах персональных данных в соответствии с внутренними регламентами Общества.

12.8. Нарушение работником требований конфиденциальности либо порядка доступа к персональным данным влечет меры ответственности, предусмотренные трудовым законодательством, локальными актами Общества и Федеральным законом № 152-ФЗ.

13. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Общества в области ПДн

13.1. Внутренний контроль за соблюдением в Обществе требований законодательства Российской Федерации и внутренних нормативных документов Общества в области ПДн осуществляется Ответственным за организацию обработки ПДн на постоянной основе с привлечением Ответственного за обеспечение безопасности ПДн.

13.2. Ответственный за организацию обработки ПДн, в частности, обязан:

– осуществлять внутренний контроль за соблюдением Обществом и Работниками Общества законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

– доводить до сведения работников Общества положения законодательства Российской Федерации о ПДн, внутренних нормативных документов Общества по вопросам обработки ПДн, требований к защите ПДн;

– организовывать прием и обработку обращений и запросов Субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

14. Ответственность за реализацию положений Политики

14.1. Работники Общества, осуществляющие обработку ПДн, а также Ответственный за организацию обработки ПДн, Ответственный за обеспечение безопасности ПДн несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации за нарушение требований настоящей Политики, иных локальных нормативных актов Общества в области ПДн и законодательства Российской Федерации в области ПДн.

14.2. Любые нарушения настоящей Политики и иных локальных актов Общества по вопросам обработки и обеспечению безопасности персональных данных будут расследоваться в соответствии с действующими в Обществе процедурами.

14.3. Лица, признанные виновными в нарушении установленных порядка и процедур обработки и обеспечения безопасности персональных данных, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством Российской Федерации.

15. Заключительные положения

15.1. Настоящая Политика является общедоступным документом и подлежит размещению на официальном сайте Общества.

15.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.