

Регламент обработки персональных данных и реализуемых требований к защите персональных данных

Введение

Настоящий Регламент ООО «ПИВОВАРЕННАЯ КОМПАНИЯ «БАЛТИКА» в отношении обработки персональных данных (далее по тексту – Регламент) является официальным документом. Настоящий Регламент является открытым документом и предназначен для ознакомления неограниченного круга лиц.

Регламент разработан в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных в ООО «ПИВОВАРЕННАЯ КОМПАНИЯ «БАЛТИКА» (далее – Компании).

Регламент разработан в соответствии с пп.2 п.1 статьи 18.1 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» и определяет политику Компании в отношении обработки информации о субъектах персональных данных, которую Компания может обрабатывать при осуществлении своей деятельности.

1. Общие положения

1.1. Цель и область применения

1.1.1. Целью настоящего Регламента является обеспечение безопасности персональных данных в Компании в соответствии с требованиями действующего законодательства в сфере защиты персональных данных, обеспечение безопасности персональных данных, обрабатываемых в Компании, от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.1.2. В Регламенте определены перечень субъектов, персональные данные которых обрабатываются в Компании, цели сбора и обработки персональных данных, условия обработки персональных данных и их передачи третьим лицам, методы защиты персональных данных, реализуемые в Компании, права субъектов персональных данных и ответственность Компании, а также перечень мер, применяемых в Компании в целях обеспечения безопасности персональных данных при их обработке.

1.1.3. Действие настоящего Регламента распространяется на все подразделения и всех сотрудников Компании, на все процессы деятельности Компании, в рамках которых осуществляется обработка персональных данных, как с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, так и без использования таких средств.

1.2. Термины, определения и сокращения

- персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- оператор персональных данных (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) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:
 - сбор;
 - запись;
 - систематизация;
 - накопление;
 - хранение;

- уточнение (обновление, изменение);
- извлечение;
- использование;
- передача (распространение, предоставление, доступ);
- обезличивание (в случаях, разрешенных законодательством РФ);
- блокирование;
- удаление;
- уничтожение.
- 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 (ИСПД) – 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;
- СЗИ – средства защиты информации;
- СКЗИ- средства криптографической защиты информации.

1.3. Нормативные ссылки

Регламент разработан в соответствии с требованиями Федерального закона от 27 июля 2006 года № 149 «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.4. Основные права и обязанности Оператора и субъекта персональных данных

1.4.1. Основные права субъекта персональных данных.

1.4.1.1. Субъект персональных данных имеет право на доступ к его персональным данным и следующим сведениям:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и местонахождение Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему Субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

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

1.4.1.3. Субъект персональных данных вправе получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения.

1.4.1.4. Субъект персональных данных вправе требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях и дополнениях.

1.4.1.5. Субъект персональных данных вправе реализовать иные права, предусмотренные действующим законодательством РФ о персональных данных.

1.4.1.6. Для реализации вышеуказанных прав субъект персональных данных, может в порядке установленном статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», обратиться в Общество с соответствующим запросом. Для выполнения таких запросов представителю Общества может потребоваться установить личность субъекта персональных данных и запросить дополнительную информацию.

1.4.1.7. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в порядке, предусмотренном законодательством Российской Федерации.

1.4.2. Основные обязанности субъекта персональных данных.

1.4.2.1. Субъект персональных данных обязан предоставить Оператору достоверные персональные данные.

1.4.2.2. Субъект персональных данных обязан своевременно информировать Оператора об изменении персональных данных. Невнесение Оператором изменений, дополнений, исключений в персональные данные, связанное с непредставлением субъектом персональных данных уточняющей, изменяющей информации, освобождает Оператора от ответственности.

1.4.3. Основные права Оператора.

1.4.3.1. Оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных в случаях, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.4.3.2. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные федеральным законодательством.

1.4.4. Основные обязанности Оператора.

1.4.4.1. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную п. 1.4.1.1.

1.4.4.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

1.4.4.3. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных федеральным законодательством, 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;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные законодательством права субъекта персональных данных;
- 5) источник получения персональных данных.

1.4.4.4. Сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

1.4.4.5. Опубликовать или иным образом обеспечить неограниченный доступ к Политике.

1.4.4.6. Принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

1.4.4.7. Оператор несет иные обязанности, предусмотренные действующим законодательством о персональных данных.

2. 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 приведены в приложении №1 к настоящему Регламенту.

3. Правовые основания обработки персональных данных

Компания вправе осуществлять обработку персональных данных только при наличии оснований, предусмотренных пунктом 1 статьи 6 Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

4. Содержание и объем подлежащих обработке персональных данных

4.1. 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.

4.2. Объем обрабатываемых персональных данных определяется в соответствии с применимым правовым основанием обработки персональных данных, указанным в разделе 3 настоящего Регламента.

4.3. В Компании не допускается (за исключением случаев, предусмотренных законодательством Российской Федерации) обработка следующих категорий ПД:

- расовая принадлежность;
- политические взгляды;
- философские убеждения;
- состояние интимной жизни;
- национальная принадлежность;
- религиозные убеждения;
- состояние здоровья, за исключением случаев, предусмотренных законодательством Российской Федерации;
- биометрические персональные данные.

5. Порядок и условия обработки персональных данных

5.1. Все персональные данные могут быть получены от самого субъекта персональных данных. Если персональные данные субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено соответствующее согласие.

5.2. Компания вправе осуществлять трансграничную передачу ПД в порядке и на условиях, предусмотренных федеральными законами.

5.3. Обработка ПД в Компании происходит как неавтоматизированным, так и автоматизированным способом.

5.4. Работники Компании получают доступ только к тем ПД, которые необходимы им для выполнения конкретных трудовых функций.

5.5. ПД хранятся в бумажном и электронном виде. В электронном виде ПД хранятся в ИСПД Компании, а также в архивных копиях баз данных этих ИСПД.

5.6. Обработка ПД может осуществляться Компанией только при наличии правовых оснований, а именно: когда получено согласие субъекта персональных данных, либо когда обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем, либо же на иных основаниях, предусмотренных федеральными законами.

5.7. При хранении ПД соблюдаются предусмотренные законодательством организационные и технические меры, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним. К ним, в частности, относятся:

- назначение работника, ответственного за организацию обработки ПД в Компании;
- ограничение физического доступа к местам хранения и носителям;
- учет всех информационных систем и электронных носителей, а также архивных копий;
- применение сертифицированных СЗИ и СКЗИ.

5.8. Компания и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.9. Условием прекращения обработки ПД является достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

5.10. Компания осуществляет хранение ПД в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.11. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", Компания обязана 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 части 5 статьи 18 Федерального закона "О персональных данных".

5.12. Обработка ПД может осуществляться Компанией путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения.

5.13. Компания передаёт персональные данные третьим лицам исключительно в случаях и на основаниях, предусмотренных федеральными законами.

5.14. Компания может поручить обработку ПД другому лицу на основании заключаемого с этим лицом договора, разработанного с учетом требований Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных». В случае поручения обработки персональных данных другому лицу наличие такого договора является обязательным условием передачи персональных данных такому лицу. Лицо, осуществляющее обработку ПД по поручению Компании, несет ответственность за соблюдение принципов и правил обработки персональных данных, предусмотренных законодательством, перед Компанией. Компания несет ответственность перед субъектом персональных данных за действия уполномоченного лица, которому Компания поручила обработку ПД.

5.15. Компания вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

6.1. В случае подтверждения факта неточности ПД или неправомерности их обработки, Компания обязана осуществить актуализацию ПД либо прекратить их обработку, соответственно.

6.2. При достижении целей обработки ПД, а также в случае отзыва субъектом персональных данных согласия на их обработку ПД подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- Компания не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом "О персональных данных" или иными федеральными законами;
- иное не предусмотрено иным соглашением между Компанией и субъектом персональных данных.

6.3. Субъект персональных данных имеет право на получение информации, касающейся обработки его ПД, за исключением случаев, когда право субъекта ПД на доступ к его ПД может быть ограничено в соответствии с федеральными законами.

6.4. В частности, субъект ПД имеет право на получение следующей информации, касающейся обработки его ПД:

- подтверждение факта обработки ПД;
- правовые основания и цели обработки ПД;
- цели и применяемые способы обработки ПД;
- сведения о лицах (за исключением работников Компании), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с Компанией или на основании федерального закона;
- обрабатываемые ПД, относящиеся к соответствующему субъекту ПД, источник их получения;
- сроки обработки ПД, в том числе сроки их хранения;
- порядок осуществления субъектом ПД своих прав;
- наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Компании, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

6.5. Получить информацию, указанную в пункте 6.4 настоящего Регламента, субъект ПД может, обратившись с письменным запросом в Компанию. Ответ, содержащий запрашиваемую информацию, либо мотивированный отказ в ее предоставлении направляется по адресу, указанному в запросе, в течение 30 дней с момента получения письменного запроса субъекта ПД.

6.6. Обработка запросов субъектов ПД производится в Компании в соответствии с Приложением 2 к настоящему Регламенту.

7. Защита и обеспечение безопасности персональных данных

7.1. Компания принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных субъектов от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий третьих лиц.

7.2. Обеспечение безопасности персональных данных в Компании достигается следующими мерами:

- назначением работника, ответственного за организацию обработки ПД;

- определением типа угроз безопасности персональных данных;
- определением уровня защищенности персональных данных и принятием организационно-технических мер по обеспечению безопасности персональных данных;
- назначением для ИСПД ответственных лиц (администратор ИСПД, администратор безопасности, ответственный пользователь СЗИ и СКЗИ);
- определением списка лиц, допущенных к работе с ПД;
- разработкой и утверждением локальных нормативных актов Компании, регламентирующих порядок обработки ПД;
- проведением периодического обучения и повышением осведомленности работников в области защиты ПД;
- реализацией технических мер, снижающих вероятность реализаций угроз безопасности ПД, при помощи сертифицированных СЗИ и СКЗИ;
- учетом машинных носителей персональных данных;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в ИСПД, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПД;
- проведением периодических проверок состояния защищенности ИСПД Компании;
- раздельным хранением персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- обеспечением в отношении каждой категории ПД возможности определения места хранения ПД (материальных носителей) и установления перечня лиц, осуществляющих обработку ПД либо имеющих к ним доступ;
- соблюдением условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ.

7.3. В Компании установлены, в том числе, следующие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений:

- назначение лица, ответственного за организацию обработки персональных данных;
- издание документов, определяющих политику Компании в отношении обработки персональных данных, нормативных правовых актов по вопросам обработки персональных данных, а также нормативных правовых актов, устанавливающих процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных, предусмотренных пунктом 7.2 настоящего регламента;
- ознакомление работников Компании, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, а также с документами, определяющими политику Компании в отношении обработки персональных данных, нормативными правовыми актами Компании по вопросам обработки персональных данных;
- проведение соответствующего обучения работников Компании, непосредственно осуществляющих обработку персональных данных;
- принятие мер по обнаружению, предотвращению и ликвидации последствий случаев нарушения безопасности персональных данных, то есть фактов неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных;
- создание в Компании команды реагирования на инциденты, ответственной за урегулирование нарушений безопасности персональных данных и их последствий.

8. Ответственность

Компания несет ответственность за разработку, введение и соответствие требованиям законодательства локальных актов Компания по вопросам обработки и защиты ПД.

9. Изменение Регламента

9.1. В целях обеспечения пригодности, адекватности и эффективности, настоящий Регламент подлежит пересмотру не реже одного раза в два года с момента его утверждения.

9.2. Регламент подлежит внеплановому пересмотру в случае существенных изменений в деятельности Компании, изменений в законодательстве в области защиты ПД.

9.3. Ответственность за соблюдение требований настоящего Регламента и поддержание его в актуальном состоянии возлагается на должностное лицо, ответственное за организацию обработки персональных данных.