

Регламент в отношении обработки персональных данных и реализуемых требований к защите персональных данных

Введение

Настоящий Регламент Акционерного общества «Пивобезалкогольный комбинат «Крым» 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 Акционерном обществе «Пивобезалкогольный комбинат «Крым» (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. Цель

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.

2. Область применения

2.1. 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.

2.2. 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.

2.3. Настоящий Регламент является неотъемлемой частью документации Компании наряду с Положением о персональных данных.

2.4. Политика по общему правилу имеет преимущественную юридическую силу перед локальными нормативными правовыми актами Компании, однако в случае, если настоящим Регламентом предусмотрены иные положения, чем Политикой, применению подлежат положения настоящего Регламента как документа, учитывающего особенности законодательства Российской Федерации в области персональных данных.

2.5. В случае возникновения противоречия положений документации Компании законодательству Российской Федерации в области персональных данных Компания обязуется внести соответствующие изменения в документацию, регламентирующую обеспечение безопасности персональных данных.

3. Нормативные ссылки

3.1. 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».

4. Термины, определения и сокращения 4.1. Перечень сокращений:

ИС - Информационная система

ИСПД - ИС персональных данных

ПД - Персональные данные

СЗИ - Средства защиты информации

СКЗИ - Средства криптографической защиты информации

4.2. Перечень определений:

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

Субъект персональных данных - физическое лицо, обладающее персональными данными прямо или косвенно его определяющими

Автоматизированная обработка персональных данных - обработка

персональных данных с помощью средств вычислительной техники

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

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

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

5. Общие положения

5.1. Безопасность ПД достигается путем исключения несанкционированного, в том числе случайного, доступа к ПД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иных несанкционированных действий.

5.2. При обработке ПД Компания придерживается следующих принципов:

5.2.1. соблюдение законности обработки ПД;

5.2.2. обработка ПД исключительно в целях, перечисленных в п.7 настоящего Регламента;

5.2.3. хранение ПД, обработка которых осуществляется с несвязанными между собой целями, в различных базах данных;

5.2.4. сбор только тех ПД, которые минимально необходимы для достижения заявленных целей обработки;

5.2.5. выполнение мер по обеспечению безопасности ПД, их точности, достаточности и других характеристик при обработке;

5.2.6. соблюдение прав субъекта ПД на доступ к его ПД;

5.2.7. соблюдение требований по уничтожению либо обезличиванию ПД по достижении целей их обработки или в случае утраты необходимости в достижении этих целей.

5.3. Компания не осуществляет принятие решений на основании исключительно автоматизированной обработки ПД.

6. Обрабатываемые персональные данные

6.1. ИСПД, принадлежащие Компании, предназначены для обработки ПД следующих лиц:

- работников, в том числе бывших работников;
- иных лиц (родственников работников и т.д.), чьи данные необходимо обрабатывать в соответствии с трудовым, налоговым и иным законодательством (для выплаты алиментов по решению суда, в целях заполнения формы No Т-2 в соответствии с трудовым законодательством и т.д.);
- контрагентов, в том числе потенциальных, с которыми заключены /могут быть заключены договоры гражданско-правового характера (представителей организаций, физических лиц, индивидуальных предпринимателей);
- лиц, осуществляющих разовый доступ на территорию Компании;
- физических лиц, являющихся потребителями продукции Компании, а также лиц, участвующих в маркетинговых мероприятиях и акциях.

6.2. В Компании не допускается 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

7. Цели сбора и обработки персональных данных

7.1. Компания производит обработку ПД работников, в том числе бывших работников, иных лиц, чьи данные необходимо обрабатывать в соответствии с трудовым, налоговым и иным законодательством (для выплаты алиментов по решению суда, в целях заполнения формы No Т-2 в соответствии с трудовым

законодательством и т.д.) в целях выполнения требований трудового, налогового и иного законодательства РФ, а также выполнения возложенных обязательств перед работниками по заключенным трудовым договорам и в иных интересах работников.

7.2. Компания производит обработку ПД контрагентов, в том числе потенциальных, в целях заключения договоров, а также исполнения заключенных договоров.

7.3. Компания производит обработку ПД работников, лиц, фактически выполняющих свои трудовые функции на территории Компании и являющихся работниками организаций, с которыми у Компании заключены договоры по предоставлению труда работников (персонала), а также лиц, осуществляющих разовый доступ на территорию Компании, в целях организации процесса доступа работников и посетителей на территорию Компании в соответствии с законом Российской Федерации N2487-1 от 11 марта 1992 года «О частной детективной и охранной деятельности в Российской Федерации».

7.4. Компания производит обработку ПД потребителей продукции, посетителей сайтов Компании, участников маркетинговых акций и мероприятий в целях исполнения договорных обязательств, повышения качества обслуживания, обработки претензий, совершенствования продукции, индивидуального общения с потребителями и их информирования о деятельности Компании, информирования участников маркетинговых акций и мероприятий о выигрышах, проведения маркетингового анализа.

8. Условия обработки персональных данных и их передача третьим лицам

8.1. Обработка персональных данных в Компании осуществляется с согласия субъекта на обработку его персональных данных, если иное не предусмотрено законодательством РФ.

8.2. Компания вправе осуществлять трансграничную передачу ПД в порядке и на условиях, предусмотренными федеральными законами.

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

8.4. К обработке ПД в Компании допускаются только работники, прошедшие определенную процедуру допуска, которая включает в себя:

- ознакомление работника под роспись с локальными нормативными актами Компании (положения, инструкции и т.д.), строго регламентирующими порядок и

процедуру работы с ПД;

- взятие с работника подписки о соблюдении конфиденциальности в отношении ПД

при работе с ними;

- получение работником и использование в работе индивидуальных атрибутов доступа к информационным системам Компании, содержащим в себе ПД. При этом каждому работнику выдаются минимально необходимые для исполнения трудовых обязанностей права на доступ в ИСПД.

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

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

8.7. 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.

8.8. Для достижения целей обработки персональных данных Компания может передавать ПД исключительно своим работникам и третьим лицам, подписавшим обязательство по обеспечению конфиденциальности и безопасности полученных сведений.

8.9. Передача персональных данных третьим лицам возможна в исключительных случаях только с согласия субъекта ПД и только с целью исполнения обязанностей перед субъектом ПД в рамках договора, либо когда такая обязанность у Компании наступает в результате требований законодательства или при поступлении запроса от уполномоченных государственных и муниципальных органов. В последнем случае Компания ограничивает передачу ПД запрошенным объемом.

8.10. Компания может поручить обработку персональных данных 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».

8.11. Лицо, осуществляющее обработку ПД по поручению Компании, несет ответственность за соблюдение принципов и правил обработки персональных данных, предусмотренных законодательством, перед Компанией.

8.12. Компания несет ответственность перед субъектом персональных данных за действия уполномоченного лица, которому Компания поручила обработку ПД.

9. Защита и обеспечение безопасности персональных данных

9.1. 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.

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

- назначением работника, ответственного за организацию обработки ПД;
- назначением комиссии по защите ПД;
- проведением аудита ИСПД Компании, проведением их классификации;
- разработкой частной модели угроз безопасности 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, разработкой для пользователей и ответственных лиц рабочих (методических) инструкций;
- 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.

10. Права субъектов персональных данных

10.1. 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.

10.2. 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. No 152-ФЗ «О персональных данных» или другими федеральными законами.

10.3. Получить информацию, указанную в пункте 10.2, 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.

10.4. Обработка запросов субъектов ПД производится в Компании согласно утвержденному внутреннему документу, разработанному в соответствии с действующим законодательством в области защиты ПД, и подконтрольна работнику, ответственному за организацию обработки ПД в Компании.

11. Обязанности Компании

11.1. Компания обязуется осуществлять обработку ПД только с согласия субъектов ПД, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. No 152-ФЗ «О персональных данных».

11.2. При сборе ПД Компания обязуется по запросу субъекта ПД предоставлять информацию, касающуюся обработки его ПД, перечисленную в разделе 10 настоящего Регламента. В случае если предоставление ПД является обязательным в соответствии с законодательством, Компания обязуется разъяснять субъекту ПД юридические последствия отказа предоставить его ПД.

11.3. Если ПД получены не от субъекта ПД, Компания до начала обработки таких ПД обязуется предоставить субъекту ПД сведения, касающиеся обработки его ПД, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. No 152-ФЗ «О персональных данных».

11.4. Компания при обработке ПД обязуется принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения,

изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПД. Описание принимаемых мер приведено в п.9 настоящего Регламента.

11.5. Компания обязуется не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами.

11.6. Компания обязуется отвечать на запросы субъектов ПД, их представителей, а также уполномоченного органа по защите прав субъектов ПД, касающиеся обрабатываемых ПД в соответствии с требованиями законодательства.

11.7. В случае предоставления субъектом ПД, либо его представителем сведений, подтверждающих факты каких-либо нарушений в процессе обработки ПД, Компания обязуется устранить данные нарушения в сроки, предусмотренные Федеральным законом

№ 152-ФЗ «О персональных данных», и уведомить субъекта ПД о внесенных изменениях и предпринятых мерах.

11.8. В случае достижения целей обработки ПД Компания обязуется прекратить обработку ПД и уничтожить ПД в течение 30 дней с даты достижения целей обработки ПД, если иное не предусмотрено условиями договора, заключенного с субъектом ПД, либо федеральными законами.

12. Ответственность

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

13. Изменение Регламента

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

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

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