

ПРАВИЛА обработки персональных данных в ООО «РАКС»

1. Основные понятия

Правила обработки персональных данных (далее - Правила) в ООО «РАКС» (далее - Учреждение) для описания своих целей использует следующие основные понятия:

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

Безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных;

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

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

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам;

Обработка персональных данных – любое действие (операция) или совокупность действий, 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 (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

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

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

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

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети,

средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации;

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

2. Общие положения

2.1. Цель разработки настоящих Правил – обеспечение защиты прав и свобод человека и гражданина, при обработке его персональных данных, в том числе права на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.2. Положения разработаны в соответствии со следующими нормативными правовыми документами Российской Федерации:

Конституция Российской Федерации;

Федеральный закон "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" от 19.12.2005 № 160-ФЗ;

Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ;

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ;

Указ Президента РФ от 06.03.1997 № 188 "Об утверждении перечня сведений конфиденциального характера";

Постановление Правительства РФ "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" от 15.09.2008 № 687;

Гражданский кодекс РФ (ГК РФ) Часть 1 от 30.11.1994 № 51-ФЗ;

Кодекс об Административных Правонарушениях РФ (КоАП РФ) от 30.12.2001 № 195-ФЗ;

Уголовный кодекс РФ (УК РФ) от 13.06.1996 № 63-ФЗ.

2.3. Правила устанавливают порядок обработки персональных данных в Учреждении.

Под обработкой персональных данных понимаются действия (операции) с персональными данными, включающие:

сбор, хранение, уточнение (обновление, изменение);

систематизацию, накопление;

использование;

обезличивание, блокирование, уничтожение.

2.4. Правила определяют необходимый минимальный объем мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

2.5. Учреждение не поручает обработку персональных данных другим лицам, ни на каких условиях, включая основания договора.

2.6. Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством.

2.7. Настоящие Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами.

2.9. Все изменения в Правила вносятся приказом директора Учреждения.

3. Цель и содержание обработки персональных данных

3.1. Цель обработки персональных данных – организация социального обслуживания Учреждением.

3.2. Предоставление государственных услуг и осуществление государственных функций Учреждения, предусматривает обработку следующих персональных данных граждан, обратившихся Учреждение:

-
- фамилия,
- имя,
- отчество,
- дата рождения,
- место рождения,
- адрес проживания,
- адрес места регистрации,
- номер телефона,
- серия и номер документа, удостоверяющего личность, кем и когда он выдан,

4. Порядок обработки персональных данных

4.1. Все персональные данные субъектов Учреждение получает от них самих либо от их представителей.

4.2. Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных.

4.3. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе.

4.4. Учреждение оставляет за собой право отказать в предоставлении услуг субъекту персональных данных в случае предоставления неполных или недостоверных персональных данных, а также в случае отказа дать письменное согласие на обработку персональных данных.

4.5. При установлении договорных отношений с субъектом персональных данных получение письменного согласия на обработку его персональных данных не требуется.

4.6. Получение персональных данных субъекта у третьих лиц, возможно только при уведомлении субъекта об этом заранее и с его письменного согласия.

4.7. Персональные данные обрабатываются в структурных подразделениях Учреждения в соответствии с исполняемыми функциями.

4.8. Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии с утвержденным списком.

4.9. Доступ к персональным данным, обрабатываемым в **информационных системах персональных данных** (далее - **ИСПДн**), осуществляется в соответствии с утвержденным списком.

4.10. Уполномоченные лица, допущенные к персональным данным субъектов Учреждения имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностными регламентами указанных лиц.

4.11. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями "Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" утвержденным постановлением Правительства РФ от 15.09.2008 № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

4.12. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

4.13. Персональные данные подлежат уничтожению либо обезличиванию в случаях достижения целей обработки или в случае утраты необходимости в их достижении;

Персональные данные подлежат уничтожению в случаях:

отзыва согласия субъекта персональных данных;

представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

выявления неправомерной обработки персональных данных.

4.14. Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются в соответствии с утвержденным списком.

4.15. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения, а также уведомляет субъекта о внесенных изменениях.

4.16. Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, если иное не предусмотрено Федеральными законами.

4.17. Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента отзыва согласия субъекта персональных данных.

4.18. Уничтожение персональных данных осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

4.19. Уничтожение персональных данных осуществляется в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных. Учреждение уведомляет об этом субъекта или его законного представителя.

4.20. Уничтожение осуществляет комиссия в составе сотрудников структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

4.21. Уничтожение достигается путем измельчения на бумагорезательной машине или сожжения (при наличии соответствующего оборудования и помещения). При этом составляется акт, утверждаемый руководителем структурного подразделения, проводившего уничтожение документов. При необходимости уничтожения большого количества документов Учреждение может воспользоваться услугами специализированных организаций по уничтожению или переработке бумаги. В этом случае к акту уничтожения необходимо приложить накладную на передачу документов, подлежащих уничтожению, в специализированную организацию, а так же комиссия, проводящая уничтожение, должна присутствовать при уничтожении документов в специализированной организации.

4.22. Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, выполняется в случаях, установленных в пункте 4.13 по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

4.23. Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за техническое обслуживание автоматизированных систем, которым принадлежат базы данных.

4.24. Уничтожение достигается путем затирания информации на носителях информации (в том числе и резервных копиях). При этом составляется акт, утверждаемый лицом, ответственным за техническое обслуживание автоматизированных систем, которому принадлежат базы данных.

4.25. Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами.

4.26. При невозможности осуществления затирания информации на носителях допускается проведение обезличивания путем перезаписи полей баз данных, которые позволяют определить субъекта данными, исключающими дальнейшее определение субъекта.

4.27. Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.

4.28. Срок хранения персональных данных 3-лет после снятия субъекта персональных данных с обслуживания.

4.29. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

4.30. Сотрудники должны быть ознакомлены под роспись с настоящими Правилами и другими документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности этой области.

5. Передача персональных данных третьим лицам

5.1. При обработке персональных данных субъекта должны соблюдаться следующие требования:

не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта;

предупреждать лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

6. Права субъектов персональных данных

6.1. В целях обеспечения своих интересов субъекты имеют право:

получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом;

требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона. Субъект при отказе Учреждения исключить или исправить персональные данные субъекта имеет право заявлять в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

обжаловать в суд любые неправомерные действия или бездействие Учреждения при обработке и защите персональных данных субъекта.

7. Порядок действий в случае запросов надзорных органов

7.1. В соответствии с частью 4 статьи 20 Федерального закона "О персональных данных" Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

7.2. Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением Учреждения.

7.3. В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

8. Защита персональных данных субъекта

8.1. Защиту персональных данных субъектов от неправомерного их использования или утраты Учреждение обеспечивает за счет собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

РД ФСТЭК России - "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Утверждены приказом ФСТЭК России №21 от 18 февраля 2013 г.;

специальными требованиями и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30 августа 2002 г. № 282;

внутренними документами Учреждения, действующими в сфере обеспечения информационной безопасности.

8.2. Защита персональных данных предусматривает ограничение к ним доступа.

8.3. Порядок доступа к персональным данным определен законодательством РФ.

8.4. Ответственные за организацию обработки персональных данных, администрирование средств и механизмов защиты, техническое обслуживание информационных систем персональных данных назначаются приказом директора Учреждения.

8.5. Руководитель структурного подразделения Учреждения, осуществляющего обработку персональных данных:

несет ответственность за организацию защиты персональных данных в структурном подразделении;

закрепляет за сотрудниками, уполномоченными обрабатывать персональные данные, конкретные носители с персональными данными, которые необходимы для выполнения возложенных на них функций;

организовывает изучение уполномоченными сотрудниками нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении;

организовывает контроль доступа к персональным данным в соответствии с функциональными обязанностями сотрудников подразделения.

8.6. Сотрудники, допущенные к персональным данным дают письменное обязательство о неразглашении таких данных в установленном порядке.

9. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с персональными данными, обязаны:

знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Учреждения по защите персональных данных;

сохранять конфиденциальность персональных данных;

обеспечивать сохранность закрепленных за ними носителей персональных данных;

контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

докладывать своему непосредственному руководителю отдела (структурного подразделения) обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

10. Ответственность сотрудника за нарушение норм, регулирующих обработку и защиту персональных данных субъектов

10.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности.

10.2. К данным лицам могут быть применены следующие дисциплинарные взыскания:

- замечание;
- выговор;
- увольнение.

10.3. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

10.4. Копия приказа о применении к сотруднику дисциплинарного взыскания с указанием оснований его применения вручается сотруднику под расписку в течение пяти дней со дня издания приказа.

10.5. Если в течение года со дня применения дисциплинарного взыскания сотрудник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Директор Учреждения, до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с сотрудника по собственной инициативе, по письменному заявлению сотрудника или по ходатайству его непосредственного руководителя.