

Приложение

УТВЕРЖДЕНА
приказом КГКУ «УЗИ»
от «20» мая 2022 г.
№ 415 /2022

Политика обработки персональных данных краевого государственного казенного учреждения «Управление землями и имуществом на территории Приморского края»

1. Общие положения

1.1. Политика обработки персональных данных (далее – «Политика») разработана в соответствии с Федеральным законом от 27.07.2006. №152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, определяет порядок и условия обработки персональных данных работников Учреждения и иных лиц, меры по обеспечению безопасности персональных данных в краевом государственном казенном учреждении «Управление землями и имуществом на территории Приморского края» (далее – «Учреждение», «Оператор», КГКУ «УЗИ») с целью 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.

1.2 Учреждение при обработке персональных данных руководствуется следующими нормативными правовыми актами:

- Конституцией Российской Федерации от 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования от 1 июля 2020 г.;
- Гражданским кодексом Российской Федерации от 30 ноября 1994 г № 51-ФЗ;
- Трудовым кодексом Российской Федерации от 30 декабря 2001 г. № 197-ФЗ;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

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

– приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

– иными нормативными правовыми актами Российской Федерации и нормативными документами уполномоченных органов государственной власти в сфере обработке и защиты персональных данных.

1.2 Обеспечение конфиденциальности и безопасности обработки персональных данных является одной из приоритетных задач Учреждения.

1.3. В целях реализации положений Политики в Учреждения введен в действие комплект организационно-распорядительной документации, обязательной к исполнению всеми сотрудниками Учреждения, допущенными к обработке персональных данных.

1.4. Все сотрудники Учреждения перед допуском к обработке персональных данных обязаны ознакомиться под роспись со следующими документами:

– Инструкция пользователей информационных систем КГКУ «УЗИ»;

– Политика информационной безопасности в информационных системах КГКУ «УЗИ»;

– Положение о разграничении доступа к информационным системам КГКУ «УЗИ» и их ресурсам;

1.5. Обработка, хранение и обеспечение конфиденциальности и безопасности обработки персональных данных осуществляется в соответствии с

действующим законодательством РФ в сфере защиты персональных данных, и в соответствии с локальными актами Учреждения.

1.6. Настоящая Политика распространяется на все действия Учреждения, 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.

1.7. Настоящая Политика вступает в силу с момента её утверждения директором КГКУ «УЗИ» либо лицом, замещающим директора Учреждения в установленном порядке, и действует бессрочно до замены её новой политикой обработки персональных данных.

1.8. Учреждение проводит пересмотр настоящей Политики и её актуализацию по мере необходимости, в частности:

- при изменении порядка обработки персональных данных в Учреждении;
- по результатам проверок органа по защите прав субъектов персональных данных, выявившим несоответствия требованиям законодательства РФ по обеспечению безопасности персональных данных;
- при изменении требований законодательства РФ в области персональных данных к порядку обработки и обеспечению безопасности персональных данных;
- в случае выявления существенных нарушений по результатам внутренних проверок систем защиты персональных данных.

2. Понятие и состав персональных данных

2.1. В настоящей Политике используются следующие основные понятия:

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

– неавтоматизированная обработка персональных данных – обработка содержащихся в информационной системе персональных данных либо извлеченных из такой системы при непосредственном участии человека;

– оператор персональных данных (далее – 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.

– 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 или на ознакомление с персональными данными неограниченного круга 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 невозможно восстановить содержание персональных данных в информационной системе персональных данных заявителей 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;

– документированная информация – зафиксированная на материальном носителе (бумажном или электронном) путем документирования информация с

реквизитами, позволяющими определить такую информацию или ее материальный носитель;

– информационная система персональных данных – совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных;

– конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

– субъект персональных данных – физическое лицо, к которому прямо или косвенно относятся персональные данные, обрабатываемые Оператором.

2.2. Перечень персональных данных, подлежащих защите в Учреждении определяется приложением к настоящей Политике, в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ «О защите персональных данных», Трудовым кодексом Российской Федерации и другими нормативно-правовыми актами Российской Федерации.

2.3. Сведениями, составляющими персональные данные, в Учреждении является любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

2.4. В Учреждении обрабатываются персональные данные сотрудников Учреждения и физических лиц, обратившихся в Учреждение, в рамках осуществления полномочий Учреждения (состав персональных данных перечислены в Приложении к настоящей Политике).

2.5. Персональные данные, перечисленные в Приложении к настоящей Политике, являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случае обезличивания персональных данных.

3. Цели обработки персональных данных

3.1. Учреждение осуществляет обработку персональных данных в следующих целях:

– заключение государственных контрактов с поставщиками (подрядчиками, исполнителями) в рамках действия Федерального закона от 05.04.2013 № 44-ФЗ

«О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

– предоставление копий технических паспортов, оценочной и иной учетно-технической документации об объектах государственного технического учета и технической инвентаризации и содержащихся в них сведений, хранившихся по состоянию на 1 января 2013 г. в филиале федерального государственного унитарного предприятия «Ростехинвентаризация – Федеральное БТИ» по Приморскому краю;

– обеспечение реализации полномочий министерства имущественных и земельных отношений Приморского края по управлению и распоряжению земельными участками, находящимися в собственности Приморского края, а также по предоставлению земельных участков, находящихся в ведении Приморского края;

– обеспечение реализации полномочий министерства имущественных и земельных отношений Приморского края по управлению и содержанию имущества Приморского края;

– образование земельных участков из земель, находящихся в ведении Приморского края, выявление земельных участков, свободных от прав третьих лиц, потенциально возможных к использованию в целях вовлечения в гражданско-правовой оборот;

– осуществление полномочий наймодателя жилых помещений, составляющих казну Приморского края;

– выполнение кадастровых работ на территории Приморского края;

– организация кадрового учета Учреждения, обеспечение соблюдения трудового законодательства и иных нормативно-правовых актов; ведение кадрового делопроизводства, исполнение требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также с исчислением и уплатой страховых взносов на обязательное медицинское страхование, на обязательное социальное страхование на случай временной нетрудоспособности и в связи с материнством, пенсионного законодательства при формировании и представлении персонифицированных

данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнение первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности, «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных» и других нормативно-правовых актов, обработка и передача персональных данных работников кредитной организации в целях реализации зарплатного проекта (оформления дебетовых карт сотрудников Учреждения);

– обработка персональных данных практикантов в рамках заключения договора по прохождению производственной практики в Учреждении;

– обработка персональных данных иных субъектов персональных данных осуществляется в целях обеспечения выполнения работ и предоставления услуг, определенных Уставом Учреждения;

– обработка персональных данных в иных законных целях.

4. Требования к срокам обработки, хранения и уничтожения персональных данных

4.1. Требования к срокам обработки персональных данных субъектов персональных данных, обрабатываемых в Учреждении, определяются локальными нормативными актами Учреждения, нормативными правовыми актами Российской Федерации и Приморского края в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.2. Сроки обработки персональных данных устанавливаются в согласии на обработку персональных данных субъекта персональных данных.

4.3. Обработка персональных данных без согласия субъекта возможна только в установленных законом случаях.

4.4. Обработка персональных данных начинается не ранее возникновения правовых оснований обработки персональных данных.

4.5. Обработка персональных данных прекращается при достижении целей обработки, утрате правовых оснований обработки, установленных

законодательством Российской Федерации, отзыве согласия на обработку персональных данных субъектом персональных данных.

4.6. По истечении срока обработки персональные данные уничтожаются или обезличиваются.

5. Права и обязанности субъектов персональных данных и Оператора

5.1. При сборе и обработке персональных данных Оператор должен исполнять следующие обязанности:

– предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

– разъяснять субъекту персональных данных юридические последствия отказа предоставить его персональные данные;

– отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством Российской Федерации;

5.2. При сборе и обработке персональных данных Оператор имеет следующие права:

– использовать и распространять персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством Российской Федерации;

– защищать свои права и законные интересы в суде.

5.3. Субъект персональных данных имеет право:

– получать информацию от оператора персональных данных, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных оператором;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые оператором способы обработки персональных данных;

г) сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона.

д) сроки обработки персональных данных, в том числе сроки их хранения;

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

– требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

– требовать перечень своих персональных данных, обрабатываемых Учреждением;

– требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

6. Принципы и условия обработки персональных данных

6.1. Обработка персональных данных Учреждением производится на основе соблюдения принципов:

– законности и справедливости целей и способов обработки персональных данных;

– соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

– соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

– недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

– хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

– уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

7. Обязанности Учреждения по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных

Учреждение обязано:

7.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных с момента такого обращения на период проверки.

7.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных Оператор обязан осуществить блокирование персональных данных с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

7.3. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных обязан уточнить персональные данные в течении 7 (семи) рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.4. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором, Оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных.

7.5. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с

даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

7.6. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных.

7.7. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий 30 (тридцати) дней с даты поступления указанного отзыва.

7.8. В случае отсутствия возможности уничтожения персональных данных в течение требуемого срока оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев.

8. Ответственность Учреждения

8.1. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается на должностных лиц Учреждения, имеющих доступ к персональным данным и работников Учреждения, обрабатывающих персональные данные в рамках их должностных обязанностей.

9. Особенности организации обработки и хранения персональных данных, осуществляемых на материальных носителях, без использования средств автоматизации

9.1. При обработке и хранении документированной информации Учреждение обязано соблюдать условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

9.2. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

9.3. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в

отношении каждой категории персональных данных можно было определить перечень мест хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

9.4. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в разных целях.

9.5. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливается Учреждением.

10. Особенности организации обработки и хранения персональных данных, осуществляемых с использованием средств автоматизации

10.1. Безопасность персональных данных при их обработке в информационных системах Учреждения обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационных системах информационные технологии.

10.2. Допуск работников Учреждения к обработке персональных данных в информационных системах осуществляется на основании ключей (паролей) доступа.

10.3. Учреждение обеспечивает размещение информационных систем, специальное оборудование и организует работу с персональными данными таким образом, чтобы обеспечить сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

10.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа. Работа на компьютерах персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, не допускается.

10.5. Обмен персональными данными субъекта персональных данных в рамках информационного обмена системы межведомственного электронного

взаимодействия осуществляется исключительно по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и применения технических средств.

10.6. При обработке персональных данных в информационных системах пользователями (работниками Учреждения) обеспечивается:

- использование специальных компьютерных программ обработки информации, содержащей сведения о персональных данных субъектов персональных данных;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

10.7. При обработке персональных данных в информационных системах Учреждения обеспечивается:

- учет работников Учреждения, допущенных к работе с персональными данными в информационных системах, прав и паролей доступа;
- регистрация действий и контроль действий работников Учреждения, обрабатывающих персональные данные в рамках их должностных обязанностей, контроль действий участников информационного обмена системы межведомственного электронного взаимодействия, участвующих в предоставлении услуг;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

10.8. Хранение персональных данных в информационных системах Учреждения осуществляется средствами системы хранения данных с использованием специализированного программного обеспечения, отвечающего требованиям информационной безопасности.

10.9. Передача и копирование резервных и технологических копий баз данных допустима только для прямого использования с целью технологической поддержки информационных систем.

10.10. Хранение резервных и технологических копий баз данных информационных систем, содержащих информацию персонального характера, осуществляется на носителях, доступ к которым ограничен.

10.11. При работе с программными средствами информационных систем, реализующими функции просмотра и редактирования персональных данных, не допускается демонстрация экранных форм, содержащих такие данные, работникам, не имеющим соответствующих должностных полномочий.

11. Порядок уничтожения персональных данных

11.1. Уничтожению подлежат персональные данные в случаях и в сроки, предусмотренные разделом 7 настоящей Политики.

11.2. Учреждение составляет сводные описи персональных данных, подлежащих уничтожению за соответствующий период.

11.3. Результат отбора документов, содержащих персональные данные к уничтожению, оформляются актом о выделении к уничтожению документов, не подлежащих хранению.

11.4. Акт о выделении к уничтожению документов, не подлежащих хранению, составляется и утверждается директором Учреждения.

11.5. После утверждения актов о выделении к уничтожению документов, содержащих персональные данные, не подлежащих хранению, дела передаются на переработку (утилизацию) по акту об уничтожении персональных данных, в котором указываются дата передачи, количество сдаваемых дел, способ уничтожения документов, дата уничтожения, подписи лиц, уничтоживших документы.

11.6. Персональные данные на бумажном носителе уничтожаются путем shreddирования.

11.7. Персональные данные на электронном носителе уничтожаются с помощью программных средств для уничтожения информации на магнитных носителях (программный шреддинг).

11.8. После уничтожения документов в номенклатуре дел Учреждения проставляется отметка «Уничтожено. См. акт в Учреждении от _____ № ____» с указанием должности, фамилии, подписи работника Учреждения, ответственного за передачу дел на уничтожение, и даты.

12. Передача персональных данных

12.1. При передаче персональных данных Учреждение должно соблюдать следующие требования:

- передавать персональные данные только тем организациям, с которыми заключены соглашения (договоры) с указанием обязанности обеспечивать защиту информации, являющейся государственным информационным ресурсом в соответствии с действующим законодательством Российской Федерации;
- разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- передавать персональные данные в порядке, установленном действующим законодательством Российской Федерации, и ограничивать передаваемую информацию только теми персональными данными, которые необходимы для выполнения конкретных функций;
- запрещается передавать персональные данные третьей стороне без письменного согласия субъекта персональных данных, кроме случаев, установленных действующим законодательством Российской Федерации.

13. Доступ к персональным данным

13.1. Список сотрудников, допущенных к работе с персональными данными, утверждается приказом директором КГКУ «УЗИ».

14. Обеспечение безопасности персональных данных

14.1. Оператор предпринимает необходимые технические и организационные меры обеспечения информационной безопасности для защиты персональных данных от несанкционированного доступа, изменения, раскрытия или уничтожения, путём внутренних проверок процессов сбора, хранения и обработки данных, и мер безопасности, а также осуществления мер по обеспечению физической безопасности данных для предотвращения несанкционированного доступа к персональным данным.

14.2. Разработку и организацию мероприятий по защите (обеспечению безопасности) персональных данных у Оператора, осуществляют работники отдела информационного обеспечения и защиты информации.

14.3. В целях обеспечения безопасности обрабатываемых персональных данных Оператор применяет следующие меры, включая, но не ограничиваясь:

- назначает лиц, ответственных за обработку персональных данных и/или за обеспечение безопасности персональных данных;
- ограничивает доступ работников к персональным данным в соответствии с должностными обязанностями;
- разрабатывает положения, регламенты, инструкции и иные локальные нормативные акты по направлениям, связанным с обработкой и защитой персональных данных;
- обеспечивает ознакомление работников Оператора с порядком обработки и обеспечения безопасности персональных данных любых субъектов, а также степени ответственности за нарушение такого порядка, проводятся методические работы с персоналом, осуществляющим обработку персональных данных;
- определяет состав и объем организационных мероприятий по защите персональных данных в соответствии с требованиями законодательства РФ;
- определяет состав технических средств защиты информации для системы защиты персональных данных в соответствии с нормативными правовыми актами, принятыми Федеральной службой по техническому и экспортному контролю;

– определяет состав криптографических средств защиты информации для системы защиты персональных данных в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации;

– осуществляет сопровождение и контроль внедрения и эксплуатации средств защиты информации в информационных системах Оператора;

– осуществляет контроль за соблюдением у Оператора норм и требований законодательства Российской Федерации по направлениям, связанным с обработкой и защитой персональных данных.

15. Заключительные положения

15.1. Настоящая Политика является общедоступной и подлежит размещению на общих ресурсах в сети Интернет.

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

15.3. Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных Учреждения.

15.4. Ответственность должностных лиц Учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации (статья 13.11 КоАП РФ – административная ответственность, статья 137 УК РФ – уголовная ответственность) и локальными актами Учреждения.

15.5. В случае если отдельные положения настоящей Политики войдут в противоречие с действующим законодательством Российской Федерации или иными документами Оператора, регулирующими обязательства по обработке персональных данных, применяются положения действующего законодательства Российской Федерации.

Приложение
к Политике обработки
персональных данных краевого
государственного казенного
учреждения «Управление
землями и имуществом на
территории Приморского края»

**Состав персональных данных казенного учреждения «Управления
землями и имуществом на территории Приморского края»**

1. Состав персональных данных сотрудников Учреждения:

- Фамилия, имя, отчество;
- Дата и место рождения;
- Адрес регистрации и адрес места фактического проживания;
- Почтовый адрес;
- Адрес электронной почты;
- Контактные данные (номер домашнего телефона, номер мобильного телефона);
- Сведения о документе, удостоверяющем личность (вид документа, серия, номер, дата выдачи, гражданство);
- Данные об идентификационном номере налогоплательщика (ИНН);
- Данные о страховом свидетельстве обязательного пенсионного страхования (СНИЛС);
- Сведения об образовании, сведения о профессиональной деятельности, сведения о составе семьи, сведения о воинском учете, сведения об отпусках, сведения о доходах;
- Лицевой счёт в банке;
- Заключение медицинской комиссии о состоянии здоровья сотрудников (в случае, если заключение медицинской комиссии требуется сотруднику Учреждения для выполнения возложенных на него трудовых обязанностей).

2. Состав персональных данных иных лиц (субъектов), обрабатываемых Учреждением:

- Фамилия, имя, отчество;
- Дата и место рождения;

- Адрес регистрации и адрес места фактического проживания;
- Почтовый адрес;
- Адрес электронной почты;
- Контактные данные (номера телефонов, электронная почта);
- Сведения о документе, удостоверяющем личность (вид документа, серия, номер, дата выдачи, гражданство);
- Данные об идентификационном номере налогоплательщика (ИНН);
- Данные о страховом свидетельстве обязательного пенсионного страхования (СНИЛС);
- Фамилия, 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. Состав персональных данных, обрабатываемых Учреждением через официальный сайт Учреждения в-сети «Интернет»:

- Фамилия, имя, отчество;
 - Адрес электронной почты;
 - Номер телефона;
 - Почтовый адрес;
 - Другие анкетные данные, размещенные на сайте и/или получаемые;
 - Учреждением в процессе взаимодействия субъекта персональных данных с сайтом Учреждения;
 - Сведения об используемом браузере (или иной программе, с помощью которой осуществляется доступ к сайту Учреждения);
 - IP-адрес;
 - Данные файлов cookie.
-