## Департамент государственного имущества и земельных отношений Забайкальского края

Краевое государственное бюджетное учреждение по архивно-информационному и геопространственному обеспечению «Забайкальский архивно-геоинформационный центр» (КГБУ «ЗабГеоИнформЦентр»)

### положение

# об обработке и защите персональных данных заказчиков-физических лиц

в Краевом государственном бюджетном учреждении по архивно-информационному и геопространственному обеспечению «Забайкальский архивно-геоинформационный центр»

Департамент государственного имущества и земельных отношений Забайкальского края

Краевое государственное бюджетное учреждение по архивно-информационному и геопространственному обеспечению «Забайкальский архивно-геоинформационный центр» (КГБУ «ЗабГеоИнформЦентр»)

«УТВЕРЖДАЮ»

Приказ №<u>54-Ли</u>от «<u>Об</u>» \_\_\_\_\_

2017 г.

Руководитель Б.Д. Жамбалов

м.п.

Положение

об обработке и защите персональных данных заказчиков-физических лиц

в Краевом государственном бюджетном учреждений по архивно-информационному и геопространственному обеспечению «Забайкальский архивно-геоинформационный центр» (КГБУ «ЗабГеоИнформЦентр»)

Настоящее Положение разработано на основании и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», Федерального закона от 27.06.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иных нормативно-правовых актов.

### 1. Общие положения

- 1.1. Настоящее Положение об обработке и защите персональных данных заказчиков-физических лиц в Краевом государственном бюджетном учреждении по архивно-информационному и геопространственному обеспечению «Забайкальский архивно-геоинформационный центр» (далее Положение) устанавливает порядок обработки и защиты персональных данных заказчиков-физических лиц в связи с оказанием КГБУ «ЗабГеоИнформЦентр» (далее Учреждение) платных услуг (работ) и выполнением государственного задания.
- 1.2. Положение содержит правила обработки и защиты персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.
- 1.3. Действие настоящего Положения не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской

Федерации, а также при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

- 1.4. Персональные данные обрабатываются с согласия субъекта персональных данных, если иное не определено федеральным законом. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме.
- 1.5. Специальные категории персональных данных, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья обрабатываются в случаях, предусмотренных ст. 10 Федерального закона от 26.07.2006 г. № 152-ФЗ «О персональных данных», только при наличии письменного согласия субъекта персональных данных.
- 1.6. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.
- 1.7. Обработка персональных данных в Учреждении ограничивается достижением конкретных, заранее определенных и законных целей. Содержание и объём обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки. Обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается.
- 1.8. Целью Положения является защита персональных данных от несанкционированного доступа, неправомерного их использования или утраты.
- 1.9. Положение утверждается, вводится в действие и изменяется приказом руководителя Учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.
- 1.10. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

#### 2. Основные понятия

2.1. Для целей настоящего Положения используются следующие основные понятия: персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (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;

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;

<u>автоматизированная обработка персональных данных</u> — обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

<u>предоставление персональных данных</u> – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

<u>уничтожение</u> 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;

<u>обезличивание</u> персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

<u>информационная система персональных данных</u> — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

- 2.2. В состав персональных данных субъекта персональных данных входят:
- реквизиты документа, удостоверяющего личность;
- анкетные и биографические данные (фамилия, имя, отчество. Дата рождения и т.п.);
- сведения о составе семьи;
- сведения о социальных льготах;
- адрес места жительства;
- номера телефонов (домашнего, мобильного и др.);
- адрес личной электронной почты;
- адрес фактического места проживания;
- номера СНИЛС, ИНН.

### 3. Меры по защите персональных данных

- В Учреждении разработаны и внедрены следующие меры для обеспечения выполнения предусмотренных действующим законодательством обязанностей по предотвращению несанкционированного доступа или неправомерного использования, утраты информации, содержащей персональные данные заказчиков-физических лиц:
- назначен ответственный за организацию обработки персональных данных;
- - определены Перечни категорий персональных данных, обрабатываемых в Учреждении;
- определен Перечень должностей, имеющих доступ к различным группам (базам) персональных данных;
- определен тип угроз безопасности персональных данных, актуальных для информационной системы, установлен уровень защищенности персональных данных в соответствии с требованиями постановления правительства Российской Федерации от 01.11.2012 г. № 1119;
- пР назначен ответственный за обеспечение безопасности персональных данных в информационной системе;
- определены места хранения и ведётся учёт материальных носителей персональных данных;
  - пр организован ограниченный доступ в помещения, где обрабатываются персональные данные;
  - определен порядок передачи помещений, в которых обрабатываются персональные данные, под охрану в нерабочее время; ведётся учёт электронных носителей информации (flash-карты, внешние НЖМД);
  - реализованы требования по парольной защите доступа к информационным ресурсам (длина не менее шести знаков, регулярная смена паролей);
  - определен порядок размещения мониторов на рабочих местах пользователей, исключающий просмотр визуальной информации посторонними лицами;
  - обеспечивается защита от воздействия вредоносных программ и программноматематических воздействий (антивирусная защита, администрирование);

TPHA .

реализована передача обрабатываемых персональных данных по общедоступной сертифицированных использованием (Интернет) C телекоммуникационной сети программных средств защиты информации;

- организован контроль выполнения условий, обеспечивающих сохранность персональных

данных и исключающих несанкционированный доступ к ним.

# 4. Защита персональных данных заказчиков-физических лиц Учреждения

4.1. Оператор обрабатывает персональные данных заказчиков-физических лиц в случаях,

предусмотренных законодательством и Уставом Учреждения.

4.2. При заключении договора субъект персональных данных дает согласие на обработку своих персональных данных. Согласие на обработку персональных данных прикрепляется к договору.

4.3. Персональные данные, полученные оператором в связи с заключением договора, стороной которого является субъект персональных данных, не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных.

5. Порядок хранения и использования персональных данных

Обработка персональных данных заказчиков-физических лиц в осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, исполнения оператором договорных обязательств.

хранящимся на электронных носителях Доступ к персональным данным, и в информационных системах регламентирован инструкцией по применению парольной

защиты. 5.3. Документы, содержащие персональные данные, хранятся в шкафах или тумбочках закрытых на ключ у работников, ответственных за ведение и хранение таких документов.

5.4. Помещения, в которых хранятся документы, содержащие персональные данные заказчиков-физических лиц, оборудуются замками.

5.5. Хранение персональных данных субъектов персональных данных может осуществляться

на электронных носителях, а также в бумажном варианте.

5.6. Допуск к персональным данным разрешен работникам, чья должность включена в Перечень должностей, имеющих доступ к персональным данным, которым персональные данные необходимы для выполнения конкретных трудовых функций.

5.7. К персональным данным, обрабатываемым в Учреждении, могут допускаться работники контрольно-ревизионных органов при наличии документов, являющихся обоснованием к работе с персональными данными.

5.8. Работники, в ведение которых входит работа с персональными данными, обеспечивают защиту персональных данных от несанкционированного доступа и копирования.

5.9. Работники, допущенные к обработке персональных данных, обязаны:

- осуществлять передачу персональных данных субъектов персональных данных в пределах Учреждения в соответствии с Перечнем должностей;

- предупредить лиц, получающих персональные данные субъекта персональных данных, 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;

- разрешать доступ к персональным данным субъекта персональных данных только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов персональных данных, которые необходимы для выполнения конкретных функций;

- передавать персональные данные субъекта персональных данных представителям работников в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными субъектов персональных данных, которые необходимы для выполнения указанными представителями их функций.
- 5.10. Работникам, допущенным к обработке персональных данных, запрещается:
- сообщать персональные данные субъекта персональных данных третьей стороне без письменного согласия заказчика-физического лица, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью заказчика-физического лица, а также в других случаях, предусмотренных законодательством Российской Федерации;
- сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия.
- 5.11. Защита персональных данных субъекта персональных данных от их неправомерного использования или утраты обеспечивается оператором за счет его средств в порядке, установленном законодательством Российской Федерации.

### 6. Порядок обеспечения защиты персональных данных

- 6.1. Под угрозой и опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних и внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.
- 6.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.
- 6.3. Защита персональных данных представляет собой жестко регламентированный процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.
- 6.4. Внутренняя защита.
- 6.4.1. Для обеспечения внутренней защиты персональных данных субъекта персональных данных необходимо соблюдать следующие меры:
- определение и утверждение Перечня работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-правовых актов и методических документов по защите информации и сохранению тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами;
- определение и утверждение Перечня работников, имеющих право доступа в помещения, в которых находится вычислительная техника с доступом к информационным системам;
- организация процесса уничтожения информации;
- своевременное выявление нарушения требований доступа к разрешительной системы работниками структурных подразделений (отделов) Учреждения;

- воспитательная и разъяснительная работа с работниками структурных подразделений (отделов), цель которой — предупредить утрату ценных сведений при работе с конфиденциальными документами.

6.4.2. Выдача документов на бумажном носителе, содержащих персональные данные субъекта персональных данных, на рабочие места руководителям структурных

подразделений (отделов) Учреждения запрещена.

6.4.3. Все файлы, содержащие персональные данные субъекта персональных данных в электронном виде, должны быть защищены паролем, который сообщается инженерупрограммисту 1 категории.

6.5. Внешняя защита.

6.5.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладеть персональными данными. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение сведениями и их использование, но и видоизменение, уничтожение, внесение вируса, подмена и др.

6.5.2. Распределение функций, рабочие процессы, оформление, ведение и хранение документов, содержащих персональные данные, является закрытой от посторонних лиц

информацией.

6.5.3. Для обеспечения внешней защиты персональных данных помещения Учреждения должны быть оборудованы техническими средствами охраны и сигнализации;

6.5.4. Кроме мер защиты персональных данных, установленных законодательством, оператор вправе использовать иные меры защиты персональных данных.

### 7. Уничтожение персональных данных

- 7.1. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.
- 7.2. Персональные данные субъекта персональных данных подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении таких целей.
- 7.3. Уничтожение документов, содержащих персональные данные, производится комиссионно. Комиссия назначается приказом руководителя Учреждения. По результатам работы комиссии оформляются акты об уничтожении.

# 8. Права субъектов по обеспечению защиты своих персональных данных.

Субъекты персональных данных имеют право на:

- полную информацию о своих персональных данных и обработке этих данных;

- свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта персональных данных, за исключением случаев, предусмотренных федеральным законодательством;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства Российской Федерации;

- требование об извещении оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

# 9. Ответственность за нарушение требований по защите персональных данных

- 9.1. Работники Учреждения при приеме на работу проходят инструктаж относительно принятых в Учреждении мер по защите персональных данных и порядке их обработки, после чего дают Обязательство о неразглашении персональных данных и иной конфиденциальной информации.
- 9.2. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных субъекта персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.
- 9.3. За разглашение персональных данных, утрату документов и иных носителей, содержащих персональные данные заказчика-физического лица; иные нарушения обязанностей по их защите, обработке и хранению влекут наложение дисциплинарного взыскания выговора, увольнения. В случае причинения Учреждению ущерба, связанного с нарушением правил обработки и защиты персональных данных работник несет полную материальную ответственность в соответствии с п. 7 ч. 1 ст. 243 Трудового кодекса РФ.
- 9.4. Нарушение неприкосновенности частной жизни, в том числе незаконного собирания или распространения сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространения этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации работник несет уголовную ответственность на основании ст. 137 Уголовного кодекса РФ.

Положение обязательно для всех работников Учреждения. В соответствие с требованиями п. 8 ст. 86 Трудового кодекса Российской Федерации, работники должны быть ознакомлены под подпись с документами работодателя, устанавливающими порядок обработки персональных данных субъектов персональных данных, а также об их правах и обязанностях в этой области.