Приложение 3
к приказу государственного
бюджетного учреждения социального
обслуживания Краснодарского края
«Брюховецкий комплексный центр
социального обслуживания населения»
от 29.12.2023 № 250

ПОЛИТИКА
обработки персональных данных государственного бюджетного учреждения социального обслуживания Краснодарского края «Брюховецкий комплексный центр социального обслуживания населения»

1 Общие положения

1.1. Назначение политики

Политика обработки персональных данных (далее – Политика) определяет цели и общие принципы обработки персональных данных, а также реализуемые меры защиты персональных данных в Государственном бюджетном учреждении социального обслуживания Краснодарского края «Брюховецкий комплексный центр социального обслуживания населения» (далее – Оператор). Политика является общедоступным документом Оператора и предусматривает возможность ознакомления с ней любых лиц.

Политика в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" на основании:

Приказа ФСТЭК России от 18.02.2013г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказа ФСБ от 10 июля 2014 года N 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2. Основные понятия

автоматизированная обработка персональных данных — обработка

персональных данных с помощью средств вычислительной техники;

аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному;

безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных 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);

биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию;

вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных;

доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

доступ к информации – возможность получения информации и ее использования;

закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации);

защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых

документов или требованиями, устанавливаемыми собственником информации;

идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных;

информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;

контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

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

межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы;

нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;

неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается

осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;

носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

оператор персональных данных (Оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

сбор;
запись;
систематизацию;
накопление;
хранение;
уточнение(обновление, изменение);
извлечение;
использование;
передачу(распространение, предоставление, доступ);
обезличивание;
блокирование;
удаление;
уничтожение.

обезличивание персональных данных — действия, в результате которых

становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

персональные данные – любая информация, относящаяся к прямо или косвенно 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;

субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

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;

уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации;

целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1.3. Основные права Оператора

Оператор оставляет за собой право проверить полноту и точность предоставленных персональных данных, В случае выявления ошибочных или неполных персональных данных, Оператор имеет право прекратить все отношения с субъектом персональных данных.

1.4. Основные обязанности оператора

Оператор не собирает персональные данные, не обрабатывает и не передает персональные данные субъектов персональных данных третьим лицам, без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.5. Основные права субъекта

Субъект персональных данных имеет право:

1) получить сведения, касающиеся обработки его персональных данных Оператором;

2) потребовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

3) отозвать согласие на обработку персональных данных в предусмотренных законом случаях.

2 Общие требования по защите персональных данных

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Оператора.

Целью Политики является обеспечение безопасности объектов защиты Оператора от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения 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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

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.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

«Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

ограничение и регламентация состава 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 – методических документов по защите информации и сохранении тайны;

наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

организация порядка уничтожения информации;

своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

воспитательная и разъяснительная работа с сотрудниками Учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

не допускается выдача личных дел сотрудников. Личные дела могут выдаваться на рабочие места только директору, работникам отдела кадров и в исключительных случаях, по письменному разрешению директора другим сотрудникам Учреждения.

Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем.

«Внешняя защита».

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение,

внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

порядок приема, учета и контроля деятельности посетителей;

пропускной режим организации;

учет и порядок выдачи удостоверений;

технические средства охраны, сигнализации;

порядок охраны территории, зданий, помещений, транспортных средств;

требования к защите информации при интервьюировании и собеседованиях.

Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

По возможности персональные данные обезличиваются.

Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

Требования настоящего Политики распространяются на всех сотрудников Оператора (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3 Цели сбора персональных данных

1) Цель обработки персональных данных физических лиц (субъектов персональных данных):

осуществление деятельности по оказанию услуг в области социального обслуживания;

внесение персональных данных в регистр получателей социальных услуг;

передача персональных данных по запросу третьих лиц в установленных законодательством случаях;

передача персональных данных (фамилия, имя, отчество) в средства массовой информации;

размещение фотографий на информационных стендах, в средствах массовой информации, на сайте министерства труда и социального развития Краснодарского края, а так же на иных сайтах в информационно-телекоммуникационных сетях «Интернет».

2) Цель обработки персональных данных сотрудников ГБУ СО КК «Брюховецкий КЦСОН»:

использование персональных данных для формирования кадровых документов и для выполнения Учреждением всех требований трудового законодательства, в том числе с правом передачи персональных данных в министерство труда и социального развития Краснодарского края и в другие структурные подразделения в соответствии с законодательством;

использование персональных данных для осуществления расчетов с работником, в том числе с правом передачи персональных данных в кредитные организации, с которыми учреждение состоит в договорных отношениях;

передача персональных данных в налоговую инспекцию по форме 2-НДФЛ;

передача персональных данных в пенсионный фонд социального страхования (индивидуальные сведения о начисленных страховых взносах, данные о трудовом стаже и иные сведения, содержащие персональные данные в соответствии с действующим законодательством);

передача персональных данных в страховые компании, с которыми учреждение состоит в договорных отношениях, для формирования полиса добровольного обязательного) медицинского страхования;

передача (получение) персональных данных в военные комиссариаты для сверки учетных сведений личной карточки формы Т-2 с учетными данными военного комиссариата по месту регистрации при приеме и увольнении с работы, при изменении учетных данных (фамилии, образования, должности, семейного положения и состава семьи, домашнего адреса) и т.д.;

размещение фотографий сотрудников на информационных стендах, в средствах массовой информации, на сайте министерства труда и социального развития Краснодарского края, а так же на иных сайтах в информационно-телекоммуникационных сетях «Интернет», создавать и размножать визитные карточки с фамилией, именем, отчеством сотрудника для осуществления трудовых функций;

размещение на официальном сайте учреждения персональных данных (Ф.И.О., образование, квалификация, опыт работы) для соблюдения требований приказа министерства труда и социальной защиты Российской федерации от 17 ноября 2014 г. № 886н «Об утверждении порядка размещения на официальном сайте поставщика социальных услуг в информационно-телекоммуникационной сети «Интернет» и обновления информации об этом поставщике»;

передача персональных данных по запросу третьих лиц в установленных законодательством случаях.

4 Правовые основания обработки персональных данных

1) устав учреждения;

2) ст. ст. 85-90 Трудового кодекса РФ;

3) Федеральным законом от 27.07.2006 г, № 152-ФЗ "О персональных данных".

5 Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

Оператор осуществляет на законной и справедливой основе обработку персональных данных следующих физических лиц (субъектов ПДн):

Цель "регистрация сведений физических лиц (субъектов персональных данных), необходимых для осуществления деятельности (оказания услуг в области социального обслуживания)" достигается посредством обработки персональных данных следующих категорий для следующих субъектов;

1) физические лица:

Иные категории: фамилия, имя, отчество, год рождения, дата рождения, место рождения, адрес, семейное положение, трудоспособность, СНИЛС, контактные сведения, паспортные данные, состав семьи.

Объем; менее чем 100 000 субъектов персональных данных

Цель "обработка в соответствии с трудовым законодательством" достигается посредством обработки персональных данных, следующих категорий для следующих субъектов:

1) сотрудники:

Специальные категории: судимость.

Иные категории: место рождения, состав семьи, трудоспособность, семейное положение, профессия, фамилия, имя, отчество, образование, дата рождения, сведения. о воинском учёте, контактные сведения, информация о трудовой деятельности, гражданство, паспортные данные, адрес, год рождения, ИНН, СНИЛС.

Объем: менее чем 100 000 субъектов персональных данных

6 Порядок и условия обработки персональных данных

6.1. Перечень действий с персональными данными, осуществляемых: Оператором осуществляются следующие действия с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, удаление, уничтожение, извлечение, передача (распространение, предоставление, доступ).

6.2. Способы обработки персональных данных

Оператором применяются следующие способы обработки персональных данных: смешанная обработка персональных данных с передачей по внутренней сети и сети интернет.

6.3. Передача персональных данных третьим лицам:

Министерство труда и социального развития Краснодарского края.

Условия передачи персональных данных: поручение Оператора. Местонахождение третьего лица: 350000, Краснодарский край, г. Краснодар, ул. Чапаева, 58.

Управление Социального фонда России Брюховецкого района.

Условия передачи персональных данных: поручение Оператора. Местонахождение третьего лица: 352750, Краснодарский край, Брюховецкий район, станица Брюховецкая, Красная улица, 209.

Государственное казенное учреждение Краснодарского края «Брюховецкая централизованная бухгалтерия учреждений социального обслуживания»

Условия передачи персональных данных: поручение Оператора. Местонахождение третьего лица: 352750, Краснодарский край, Брюховецкий район, станица Брюховецкая, Красная ул., д.201.

Государственное казенное учреждение Краснодарского края "Управление социальной защиты населения в Брюховецком районе"

Условия передачи персональных данных: поручение Оператора. Местонахождение третьего лица: 352750, Краснодарский край, Брюховецкий район, станица Брюховецкая, ул. Красная, д.199.

Трансграничная передача персональных данных не осуществляется.

Цели передачи персональных данных: начисление заработной платы в рамках банковского зарплатного проекта, аутсорсинг обработки информации в системе.

Объем передаваемых данных; менее чем 100 000 субъектов персональных данных.

Перечень действий, разрешенных третьему лицу: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Способы обработки ПДн третьим лицом: автоматизированная обработка персональных данных с передачей по внутренней сети и сети интернет.

В случае поручения обработки персональных данных третьему лицу, ему предъявляются требования принимать необходимые организационные, технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, в том числе: определение угроз безопасности персональных данных при их обработке в информационных системах; учёт машинных носителей персональных данных; обнаружение фактов несанкционированного доступа к персональным данным и принятием мер; контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищённости информационных систем персональных данных.

При передаче персональных данных на основе федерального закона условия передачи персональных данных устанавливаются соответствующим федеральным законом.

6.4. Обеспечение безопасности персональных данных Оператором достигается, в частности следующими мерами:

1) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения закона "О персональных данных", соотношение

указанного вреда и принимаемых защитных мер;

2) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных закону "О персональных данных" и внутренним документам учреждения по вопросам обработки персональных данных;

3) ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, политикой учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

4) назначение Ответственного за организацию обработки персональных данных;

5) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

6) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

7) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

8) издание политики учреждения в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных;

9) учет машинных носителей персональных данных;

10) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

11) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных,

6.5. Базы персональных данных Оператора находятся полностью в пределах территории Российской Федерации.

6.6. Сроки обработки персональных данных

Персональные данные субъектов, обрабатываемые Оператором подлежат уничтожению либо обезличиванию в случае:

1) достижения целей обработки персональных данных или утраты необходимости в достижении этих целей;

2) прекращения деятельности Оператора.

6.7. Условия обработки персональных данных без использования средств автоматизации.

При обработке персональных данных, осуществляемой без использования средств автоматизации, Оператор выполняет требования, установленные постановлением Правительства Российской Федерации, от 15 сентября 2008 года № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

7 Регламент реагирования на запросы обращения субъектов персональных данных и их представителей.

При обращении, запросе в письменной или электронной форме субъекта персональных данных или его законного представителя, на доступ к своим персональным данным Учреждение руководствуется требованиями статей 14, 18 и 20 Федерального закона № 152-ФЗ.

Субъект или его законный представитель может воспользоваться формами запросов, указанными в приложениях 1-2 к данной Политике.

Доступ субъекта персональных данных или его законного представителя к своим персональным данным Оператор предоставляет только под контролем ответственного за организацию обработки персональных Оператора,

Обращение субъекта персональных данных или его законного представителя фиксируются в журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных.

Запрос в письменной или электронной форме субъекта персональных данных или его законного представителя фиксируются в журнале регистрации письменных запросов граждан на доступ к своим персональным данным.

Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекта к персональным данным.

В случае, если данных предоставленных субъектом недостаточно для установления его личности или предоставление персональных данных нарушает конституционные права и свободы других лиц ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает сотрудника (сотрудников) структурного подразделения, обрабатывающего персональные данные субъекта по согласованию с руководителем этого структурного .подразделения.

Сведения о наличии персональных данных Оператор предоставляет субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

Сведения о наличии персональных данных предоставляются субъекту при

ответе на запрос в течение тридцати дней от даты получения запроса субъекта персональных данных или его законного представителя.

8 Регламент реагирования на запросы обращения уполномоченных органов

В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ Оператор 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.

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

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

Заместитель директора А.А. Пручай

Приложение 4
к приказу государственного
бюджетного учреждения социального
обслуживания Краснодарского края
«Брюховецкий комплексный центр
социального обслуживания населения»
от 29.12.2023 № 250

Форма запроса субъекта персональных данных, в случае выявления недостоверных персональных данных

Директору ГБУ СО КК «Брюховецкий КЦСОН» Е.Б. Туржан
от _____
(Ф.И.О., номер основного документа, удостоверяющего личность
_____
субъекта или его законного представителя, сведения о дате
_____
выдачи указанного документа и выдавшем органе,
_____
адрес, контактные данные)

З А П Р О С
на уточнение/блокирование/уничтожение персональных данных, в связи с выявлением недостоверных персональных данных

Прошу:
мои персональные данные, обрабатываемые в ГБУ СО КК «Брюховецкий КЦСОН», в связи с выявлением следующих недостоверных сведений:

_____
_____
_____
_____
_____
_____
(перечислить)

_____ _____ _____
(дата) (подпись) (расшифровка)

Заместитель директора А.А. Пручай

Приложение 5
к приказу государственного
бюджетного учреждения социального
обслуживания Краснодарского края
«Брюховецкий комплексный центр
социального обслуживания населения»
от 29.12.2023 № 250

Форма запроса субъекта персональных данных на предоставление доступа к своим персональным данным

Директору ГБУ СО КК «Брюховецкий КЦСОН» Е.Б. Туржан
от _____
(Ф.И.О., номер основного документа, удостоверяющего личность

_____
субъекта или его законного представителя, сведения о дате

_____
выдачи указанного документа и выдавшем органе,

_____
адрес, контактные данные)

ЗАПРОС
на получение доступа к персональным данным

Прошу предоставить мне для ознакомления следующую информацию (в том числе документы), составляющую мои персональные данные:

_____
_____
_____
_____
_____
_____
_____
_____
_____
(перечислить)

_____ _____ _____
(дата) (подпись) (расшифровка)

Заместитель директора А.А. Пручай