

Приложение № 1
к Приказу № 4-П от «16» июля 2020 г.



Утверждаю
Генеральный директор
ООО «КМУ Рус»

/ Пинский В.В. /
Приказ № 4-П от «16» июля 2020 г.

Политика ООО «КМУ Рус» в отношении обработки персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика Общества с ограниченной ответственностью «КМУ Рус» (далее по тексту – Оператор) в отношении обработки персональных данных (далее - Политика) разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных) в целях обеспечения 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. Политика действует в отношении всех персональных данных, которые обрабатывает Оператор.

1.3. Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных Оператор обеспечил неограниченный доступ к Политике путем ее публикации на интернет-сайте ООО «КМУ Рус» в сети «Интернет» (www.kmu-rus.ru), а также обеспечил неограниченный доступ к материальному носителю Политики в офисе Оператора по адресу: 141281, Московская область, г. Пушкино, г. Ивантеевка, Санаторный проезд, д. 1, Здание Бизнес-Центра, офис 14, этаж 1.

1.5. Основные понятия, используемые в Политике:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (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;

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

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;

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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных 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;

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

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

2. ОСНОВНЫЕ ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Субъект персональных данных имеет право:

2.1.1. получать информацию, касающуюся обработки его персональных данных:

- ✓ подтверждение факта обработки персональных данных оператором;
- ✓ правовые основания и цели обработки персональных данных;
- ✓ цели и применяемые оператором способы обработки персональных данных;
- ✓ наименование и место нахождения оператора, сведения о лицах (за исключением

работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

- ✓ обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- ✓ сроки обработки персональных данных, в том числе сроки их хранения;

- ✓ порядок осуществления субъектом персональных данных прав, предусмотренных

Законом о персональных данных;

- ✓ информацию об осуществленной или о предполагаемой трансграничной передаче данных;

- ✓ наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

- ✓ информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Закона о персональных данных;

- ✓ требовать 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, а также принимать предусмотренные законом меры по защите своих прав;

- ✓ обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Закона о персональных данных или иным образом нарушает его права и свободы;

- ✓ на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;

- ✓ иные сведения, предусмотренные Законом о персональных данных или другими федеральными законами.

2.1.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- ✓ обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- ✓ обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

✓ обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

✓ доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

✓ обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

2.1.3. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Закона о персональных данных или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. ОСНОВНЫЕ ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА

3.1. Оператор имеет право:

✓ самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;

✓ поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;

✓ в случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных.

3.2. Оператор обязан:

✓ предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Закона о персональных данных.

✓ разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку, если в соответствии с федеральным законом предоставление персональных данных и (или) получение Оператором согласия на обработку персональных данных являются обязательными;

✓ предоставить субъекту персональных данных следующую информацию если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных частью 4 ст. 18 Закона о персональных данных, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

✚ наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

✚ цель обработки персональных данных и ее правовое основание;

✚ перечень персональных данных;

✚ предполагаемые пользователи персональных данных;

✚ установленные настоящим Федеральным законом права субъекта персональных данных;

✚ источник получения персональных данных.

Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 ст. 18 Закона о персональных данных, в случаях, если:

- ✓ субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- ✓ персональные данные получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- ✓ обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 настоящего Закона о персональных данных;
- ✓ Оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- ✓ предоставление субъекту персональных данных сведений, предусмотренных частью 3 статьи 18 Закона о персональных данных, нарушает права и законные интересы третьих лиц;
- ✓ разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;
- ✓ Оператор обязан рассмотреть возражение, указанное в части 3 настоящей ст. 16 Закона о персональных данных, в течение 30 (тридцати) дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

3.3. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Закона о персональных данных.

3.4. Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, ответственным за организацию обработки персональных данных у Оператора.

3.5. Ответственность за нарушение требований законодательства Российской Федерации и нормативных актов Оператора в сфере обработки и защиты персональных данных определяется в соответствии с законодательством Российской Федерации.

4. ЦЕЛИ СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.2. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.3. **Обработка Оператором персональных данных осуществляется в следующих целях:**

- ✓ обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;
- ✓ реализации прав и законных интересов Оператора в рамках ведения видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора, или третьих лиц либо достижения общественно значимых целей;
- ✓ оформление трудовых отношений, ведение кадрового делопроизводства;
- ✓ содействие работникам в трудоустройстве, получении образования и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества;

- ✓ привлечение и отбор кандидатов на работу у Оператора;
- ✓ организация постановки на индивидуальный (персонифицированный) учет работников в системе обязательного пенсионного страхования;
- ✓ заполнение и передача в органы исполнительной власти и иные уполномоченные организации требуемых форм отчетности;
- ✓ заключение, исполнение изменение и прекращение гражданско-правовых договоров;
- ✓ ведение бухгалтерского учета, реализация требований законов о налогообложении в вопросах начисления, внесения налоговых платежей с доходов физлиц, ЕСН, пенсионных законов во время формирования, передачи в Пенсионный фонд данных персонификации относительно каждого получателя страховых выплат, внесение данных в первичную статистическую документацию по Трудовому, Налоговому кодексам, а также федеральным законам;
- ✓ исполнения судебных актов, актов других государственных органов или должностных лиц;
- ✓ осуществление пропускного режима;
- ✓ в иных случаях, установленных законодательством Российской Федерации и Уставом Оператора.

4.4. Обработка персональных данных работников может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

5. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Правовым основанием обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, в том числе:

- ✓ Конституция Российской Федерации;
 - ✓ Международных договорах Российской Федерации;
 - ✓ Гражданский кодекс Российской Федерации;
 - ✓ Трудовой кодекс Российской Федерации;
 - ✓ Налоговый кодекс Российской Федерации;
 - ✓ Федеральный закон от 08.02.1998 N 14-ФЗ "Об обществах с ограниченной ответственностью";
 - ✓ Федеральный закон от 06.12.2011 N 402-ФЗ "О бухгалтерском учете";
 - ✓ Федеральный закон от 15.12.2001 N 167-ФЗ "Об обязательном пенсионном страховании в Российской Федерации";
 - ✓ Постановление Правительства Российской Федерации от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
 - ✓ Постановление Правительства Российской Федерации от 15.09.2008 N 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
 - ✓ Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состав 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»;
 - ✓ иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора;
- а также:
- ✓ Устав Оператора;
 - ✓ Положение об обработке персональных данных в ООО «КМУ Рус»;
 - ✓ договоры, заключаемые между Оператором и субъектами персональных данных;
 - ✓ согласие субъектов персональных данных на обработку их персональных данных.

6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

6.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

6.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

6.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

6.5. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных.

6.6. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разд. 4 настоящей Политики. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

7.2. Оператор может обрабатывать персональные данные следующих категорий субъектов персональных данных:

- 7.2.1. Кандидаты на трудоустройство к Оператору;
- 7.2.2. Работники и бывшие работники Оператора;
- 7.2.3. Клиенты и контрагенты Оператора (физические лица);
- 7.2.4. Представители (работники) клиентов и контрагентов Оператора (юридических лиц).

7.3. В отношении категории, указанной в пункте 7.2.1. настоящих Правил, обрабатываются:

- ✓ фамилия, имя, отчество;
- ✓ дата и место рождения;
- ✓ пол;
- ✓ контактные данные;
- ✓ сведения об образовании, опыте работы, квалификации;
- ✓ иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

7.4. В отношении категории, указанной в пункте 7.2.2. настоящих Правил, обрабатываются:

- ✓ фамилия, имя, отчество;
- ✓ пол;
- ✓ гражданство;
- ✓ дата и место рождения;
- ✓ прежние фамилия, имя и отчество, дата, место и причина изменения (в случае изменения);
- ✓ паспортные данные (серия, номер, кем и когда выдан, код подразделения, выдавшего паспорт);
- ✓ адрес и дата регистрации по месту жительства / месту пребывания;
- ✓ адрес фактического проживания;
- ✓ контактные данные (номер телефона, адрес электронной почты);
- ✓ идентификационный номер налогоплательщика;

- ✓ страховой номер индивидуального лицевого счета (СНИЛС);
- ✓ номер расчетного счета, банковской карты;
- ✓ сведения об образовании (когда и какие образовательные учреждения закончил, номер диплома, направление подготовки и специальности по диплому, квалификация по диплому);
- ✓ сведения об ученой степени, ученом звании (дата присвоения, номер диплома, аттестата);
- ✓ информация о владении иностранными языками, степень владения;
- ✓ сведения о трудовой деятельности с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т.п.), в том числе наличие поощрений, наград и (или) дисциплинарных взысканий;
- ✓ отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- ✓ сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения);
- ✓ сведения об инвалидности;
- ✓ сведения об удержании алиментов;
- ✓ сведения о доходах (в том числе с предыдущих мест работы);
- ✓ информация о государственных наградах, иных наградах и знаках отличия (кем и когда награжден);
- ✓ сведения о наличии / отсутствии судимости;
- ✓ сведения о допуске к государственной тайне, оформленном за период работы, службы, учебы (форма, номер и дата);
- ✓ результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;
- ✓ данные об отпусках;
- ✓ трудовая книжка;
- ✓ иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

7.5. В отношении категории, указанной в пункте 7.2.3. настоящих Правил, обрабатываются:

- ✓ фамилия, имя, отчество;
- ✓ дата и место рождения;
- ✓ паспортные данные;
- ✓ адрес регистрации по месту жительства;
- ✓ контактные данные;
- ✓ должность;
- ✓ индивидуальный номер налогоплательщика;
- ✓ номер расчетного счета;
- ✓ иные персональные данные, предоставляемые клиентами и контрагентами (физическими лицами), необходимые для заключения и исполнения договоров.

7.6. В отношении категории, указанной в пункте 7.2.4. настоящих Правил, обрабатываются:

- ✓ фамилия, имя, отчество;
- ✓ паспортные данные;
- ✓ контактные данные;
- ✓ должность;
- ✓ иные персональные данные, предоставляемые представителями (работниками) клиентов и контрагентов, необходимые для заключения и исполнения договоров.

7.7. Обработка Оператором биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) осуществляется в соответствии с законодательством Российской Федерации.

7.8. Оператором не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов,

религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

8. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

8.2. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

8.3. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

✓ 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

✓ 2) фамилию, 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) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

✓ 4) цель обработки персональных данных;

✓ 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

✓ 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

✓ 8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

✓ 9) подпись субъекта персональных данных.

8.4. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

8.5. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

8.6. Обработка персональных данных осуществляется следующими способами:

✓ автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

✓ неавтоматизированная обработка персональных данных - обработка персональных данных, осуществляемая при непосредственном участии человека;

✓ смешанная обработка персональных данных.

8.7. Оператор организует обработку персональных данных в следующем порядке:

✓ 1) назначает ответственного за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным;

✓ 2) издает настоящую Политику, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

✓ 3) применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;

✓ 4) осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;

✓ 5) осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;

✓ 6) знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политики, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

8.8. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

8.9. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 № 18.

8.10. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

8.11. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

✓ определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

✓ применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

✓ применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

✓ оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

✓ учетом машинных носителей персональных данных;

✓ обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

✓ восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

✓ установлением 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;

✓ контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

8.12. Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

8.13. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

8.14. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

8.15. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

8.16. Хранение персональных данных без использования средств автоматизации осуществляется в сейфах или металлических несгораемых шкафах с замками.

9. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

9.1. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии ч. 5 ст. 19 Закона о персональных данных.

9.2. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

9.3. Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах Оператора, осуществляется в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

9.4. Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.

9.5. Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети «Интернет», так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

9.6. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах Оператора, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

9.7. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

10. СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- ✓ идентификация и аутентификация субъектов доступа и объектов доступа;
- ✓ управление доступом субъектов доступа к объектам доступа;
- ✓ ограничение программной среды;
- ✓ защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- ✓ регистрация событий безопасности;
- ✓ антивирусная защита;
- ✓ обнаружение (предотвращение) вторжений;
- ✓ контроль (анализ) защищенности персональных данных;
- ✓ обеспечение целостности информационной системы и персональных данных;
- ✓ обеспечение доступности персональных данных;
- ✓ защита среды виртуализации и технических средств;
- ✓ защита информационной системы, ее средств, систем связи и передачи данных;
- ✓ выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- ✓ управление конфигурацией информационной системы и системы защиты персональных данных.

10.2. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

✓ Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

✓ Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

✓ Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

10.3. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится Оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Закона о персональных данных, и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Закона о персональных данных.

10.4. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

10.5. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

✓ а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

✓ б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

10.6. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- ✓ а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;
- ✓ б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- ✓ в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;
- ✓ г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- ✓ д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- ✓ е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

10.7. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- ✓ а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- ✓ б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- ✓ в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- ✓ г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;
- ✓ д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

10.8. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- ✓ а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;
- ✓ б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

10.9. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- ✓ а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- ✓ б) обеспечение сохранности носителей персональных данных;

✓ в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

✓ г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

10.10. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных п. 10.9. настоящих Правил, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

10.11. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных п. 10.10. настоящих Правил, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

10.12. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных п. 10.11. настоящих правил, необходимо выполнение следующих требований:

✓ а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

✓ б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

10.13. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

11. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ, УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРЕКРАЩЕНИЕ ИХ ОБРАБОТКИ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

11.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Оператором субъекту персональных данных или его представителю в течение 10 рабочих дней с момента обращения либо получения запроса субъекта персональных данных или его представителя. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору следует направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.

11.2. Запрос должен содержать:

✓ номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

✓ сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

✓ подпись субъекта персональных данных или его представителя.

11.3. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

11.4. Оператор предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

11.5. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

11.6. Сведения должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

11.7. Полный перечень информации и порядок ее получения установлен Законом о персональных данных.

11.8. В случае, если сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в ч. 7 ст. 14 Закона о персональных данных, и ознакомления с такими персональными данными не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

11.9. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных ч. 7 ст. 14 Закона о персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в ч. 4 ст. 14 Закона о персональных данных (п. 11.8. настоящих правил), в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в ч. 3 ст. 14 Закона о персональных данных, должен содержать обоснование направления повторного запроса.

11.10. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным ч. 4 и 5 ст. 14 Закона о персональных данных. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

11.11. Оператор обязан сообщить в порядке, предусмотренном ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 10 (десяти) рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.12. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение ч. 8 ст. 14 Закона о персональных данных или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 10 (десяти) рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.13. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня

предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

11.14. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 10 (десяти) рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.15. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

11.16. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение 7 (семи) рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

11.17. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

11.18. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

✓ в течение 24 (двадцати четырех) часов о произошедшем инциденте, о

предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

✓ в течение 72 (семидесяти двух) часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

11.19. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами.

11.20. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами.

11.21. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий 10 (десяти) рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Закона о персональных данных. Указанный срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

11.22. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5.1 статьи 21 Закона о персональных данных (11.18.-11.21. настоящих правил), Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1. Настоящая политика является общедоступным документом.

12.2. Ответственность лиц, имеющих доступ к персональным данным, определяется действующим законодательством Российской Федерации.

Принято в печать
Акт приема-передачи
Специально для
ООО "КМУ Рус"
Директор

