

Политика обработки персональных данных АО «ЦВКС «МСК-IX»

1. Общие положения

1.1. Настоящая Политика определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в АО «ЦВКС «МСК-IX» (далее – «Оператор») персональных данных, права и обязанности Оператора при обработке персональных данных, а также права субъектов персональных данных.

1.2. Настоящая Политика разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Трудовым кодексом РФ, Налоговым кодексом РФ, Гражданским кодексом РФ, Федеральным законом от 06.12.2011 № 402-ФЗ «О бухгалтерском учёте», иными нормативными правовыми актами РФ, а также нормативными документами уполномоченных органов государственной власти по вопросам безопасности персональных данных.

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

1.4. Обработка персональных данных – любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.5. Настоящая Политика распространяется на все персональные данные субъектов, обрабатываемые Оператором. Политика является общедоступной и размещается на официальном сайте Оператора в сети Интернет по адресу: <https://www.msk-ix.ru/legal/>.

1.6. Настоящая Политика подлежит пересмотру при изменении законодательства РФ о персональных данных, изменении технологических и организационных процессов обработки персональных данных, а также при выявлении новых рисков безопасности. Внесение изменений производится приказом Генерального директора Оператора. Субъекты персональных данных уведомляются об изменениях путём публикации новой редакции Политики на официальном сайте.

2. Правовые основания обработки персональных данных

2.1. Общие положения

Обработка персональных данных осуществляется Оператором на основании следующих правовых оснований, предусмотренных законодательством РФ:

2.2. Основания для обработки

- Согласие субъекта ПДн (ч. 1 ст. 6 ФЗ-152):
 - Для обработки специальных категорий ПД;

- При трансграничной передаче данных;
- В случаях, не предусмотренных законом.
- Исполнение договора (ч. 1 п. 2 ст. 6 ФЗ-152):
 - Трудовые договоры;
 - Гражданско-правовые договоры;
 - Договоры с контрагентами.
 -
- Исполнение обязанностей по закону (ч. 1 п. 1 ст. 6 ФЗ-152):
 - Ведение кадрового учета;
 - Сдача отчетности в госорганы;
 - Исполнение требований ТК РФ.
- Защита жизненно важных интересов (ч. 1 п. 4 ст. 6 ФЗ-152):
 - В случаях, когда получение согласия невозможно;
 - При угрозе жизни и здоровью субъекта.
- Общественно значимые цели (ч. 1 п. 5 ст. 6 ФЗ-152):
 - При условии соблюдения прав субъектов ПДн;
 - В рамках реализации государственных задач.

2.3. Специальные правовые основания

- Для обработки специальных категорий ПДн (ст. 10 ФЗ-152):
 - Только при наличии отдельного письменного согласия;
 - В случаях, прямо предусмотренных законом;
- Для обработки биометрических ПДн (ст. 11 ФЗ-152):
 - При наличии письменного согласия;
 - В случаях, установленных законом.

2.4. Обязательные требования

- Уведомление Роскомнадзора о начале обработки ПДн;
- Регистрация в реестре операторов персональных данных;
- Соблюдение требований к защите ПДн;
- Локализация баз данных на территории РФ.

2.5. Документальное оформление

- Согласия субъектов оформляются в письменной форме;
- Договоры содержат условия обработки ПДн;
- Локальные акты регламентируют порядок обработки;
- Приказы определяют ответственных лиц.

2.6. Контроль соблюдения

- Регулярный аудит законности обработки;
- Проверка наличия правовых оснований;
- Обновление правовых оснований при изменении законодательства;
- Информирование сотрудников об изменениях.

2.7. Оператор также руководствуется локальными актами:

- Уставом Оператора;
- Локальными актами, регулирующими обработку и защиту персональных данных (Перечень мер по обеспечению безопасности персональных данных, Инструкция для работников, допущенных к обработке ПДн, Положение о порядке доступа к персональным данным и др.).

2.8. Обязанность уведомления Роскомнадзора

Оператор обязан уведомить Роскомнадзор о начале обработки персональных данных и пройти регистрацию в реестре операторов персональных данных в порядке, установленном действующим законодательством. За отсутствие регистрации предусмотрена административная ответственность.

3. Категории субъектов и обрабатываемых персональных данных

3.1. Категории субъектов персональных данных

Оператор обрабатывает персональные данные следующих категорий субъектов:

- работники Оператора и члены их семей (супруги, близкие родственники);
- кандидаты на работу;
- клиенты, партнеры, контрагенты (работники и/или представители юридических лиц);
- посетители Оператора;
- аффилированные лица Оператора;
- физические лица, обратившиеся с запросами;
- иные субъекты в рамках деятельности Оператора.

3.2. Категории персональных данных

В зависимости от содержания и правового режима обработки персональные данные подразделяются на следующие категории:

3.2.1. Общедоступные персональные данные – данные, доступ неограниченного круга лиц к которым предоставлен субъектом либо которые подлежат опубликованию в соответствии с законом (например, сведения о работниках, включаемые в кадровые документы, предоставляемые в ПФР, ФНС, иные госорганы).

3.2.2. Специальные категории персональных данных (обрабатываются только при наличии письменного согласия субъекта либо в случаях, прямо предусмотренных ч. 2 ст. 10 Федерального закона № 152-ФЗ):

- расовая, национальная принадлежность;
- политические взгляды;
- религиозные или философские убеждения;
- состояние здоровья (обрабатывается в объеме, необходимом для решения вопроса о трудоспособности, предоставления льгот и гарантий, связанных с выполнением трудовой функции);
- интимная жизнь (не обрабатывается).

3.2.3. Биометрические персональные данные (обрабатываются только при наличии письменного согласия, за исключением случаев, установленных законом) – сведения,

характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность:

- фотографии (при использовании систем видеонаблюдения, пропускного режима, в корпоративных системах идентификации);
- иные биометрические данные (не обрабатываются).

3.2.4. Иные персональные данные (не отнесённые к специальным или биометрическим):

- фамилия, имя, отчество;
- пол, дата и место рождения;
- адрес места жительства, регистрации;
- паспортные данные (серия, номер, кем и когда выдан);
- СНИЛС, ИНН;
- сведения о семейном положении, детях, родственниках;
- сведения о трудовой деятельности, должности, заработной плате, стаже;
- контактные данные (телефон, адрес электронной почты);
- сведения об образовании, квалификации, профессиональной подготовке;
- иные данные, необходимые для достижения целей обработки.

3.3. Обработка специальных и биометрических данных

Оператор обрабатывает специальные и биометрические персональные данные только при наличии законных оснований. При необходимости обработки таких данных Оператор получает письменное согласие субъекта в порядке, установленном ст. 10 и 11 Федерального закона № 152-ФЗ, с учетом требований к форме согласий, действующих с 01 сентября 2025 года. Согласие оформляется как отдельный документ и не может быть включено в пользовательское соглашение или иную политику конфиденциальности.

4. Сроки хранения персональных данных

4.1. Сроки хранения персональных данных определяются исходя из целей обработки, требований законодательства (в том числе архивного), а также договорных обязательств.

4.2. Конкретные сроки хранения для основных категорий данных:

Категория данных / документов	Срок хранения	Нормативное основание
Личные дела работников (приказы о приёме, переводе, увольнении, личные карточки)	75 лет (для принятых до 2003 г. – 75 лет, после – 50 лет)	ст. 22.1 Закона № 125-ФЗ «Об архивном деле»
Трудовые договоры	75 лет (50 лет)	Перечень типовых архивных документов (утв. Приказом Росархива от 20.12.2019 № 236)
Расчётные листки, сведения о зарплате	75 лет (50 лет)	То же

Категория данных / документов	Срок хранения	Нормативное основание
Налоговые и бухгалтерские документы	5 лет (после окончания налогового периода)	ст. 23 НК РФ
Данные о кандидатах, не принятых на работу	1 год (если иное не предусмотрено согласием)	П. 2 ст. 5, ст. 7 152-ФЗ
Договоры с контрагентами и персональные данные их работников	5 лет после окончания срока действия договора	ГК РФ, требования налогового учёта
Данные посетителей (журнал учёта)	1 год (если не требуется дольше для обеспечения безопасности)	Локальные акты
Данные лиц, обратившихся с запросами	3 года (в зависимости от содержания)	Общий срок исковой давности (ст. 196 ГК РФ)
Видеозаписи с камер наблюдения	30 дней (если иное не предусмотрено законом)	Постановление Правительства РФ № 512 (объекты транспортной инфраструктуры), иное – локальные акты
Согласия на обработку персональных данных	В течение срока обработки данных + 3 года после уничтожения данных (для подтверждения законности обработки)	ст. 17, 19 152-ФЗ

4.3. В отсутствие установленного законом срока данные хранятся не дольше, чем требуется для целей обработки.

4.4. По истечении срока хранения персональные данные подлежат уничтожению или обезличиванию актом комиссии, назначаемой приказом руководителя.

5. Основные принципы, цели и условия обработки персональных данных

5.1. Принципы обработки персональных данных

Обработка персональных данных в Операторе осуществляется на основе следующих принципов:

- обработке подлежат только персональные данные, которые отвечают целям их обработки;

- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки; не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки;
- хранение персональных данных осуществляется 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 либо договором, стороной, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- право доступа для обработки персональных данных имеют работники Оператора в соответствии с возложенными на них функциональными обязанностями;
- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2. Цели обработки персональных данных

Персональные данные обрабатываются в Операторе в следующих целях:

- регулирование трудовых отношений с работниками Оператора (соблюдение требований ТК РФ и иных нормативных правовых актов);
- предоставление работникам Оператора и членам их семей дополнительных гарантий и компенсаций, в том числе негосударственного пенсионного обеспечения, добровольного медицинского страхования, медицинского обслуживания и других видов социального обеспечения;
- подготовка, заключение, исполнение и прекращение гражданско-правовых договоров с контрагентами;
- ведение бухгалтерского и налогового учёта, составление и сдача отчётности в контролирующие органы;
- обеспечение пропускного и внутриобъектового режима на территории Оператора;
- предоставление рекламной информации, проведение маркетинговых мероприятий в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора;
- реализация прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Оператора, или третьих лиц либо достижения общественно значимых целей.

5.3. Условия обработки персональных данных

Обработка персональных данных в Операторе допускается при наличии хотя бы одного из следующих оснований:

- обработка осуществляется с согласия субъекта персональных данных;
- обработка необходима для исполнения договора, стороной, выгодоприобретателем или поручителем по которому является субъект;
- обработка необходима для исполнения судебного акта, акта другого органа или должностного лица;

- обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта, если получение согласия невозможно;
- обработка необходима для осуществления прав и законных интересов Оператора при условии, что не нарушаются права и свободы субъекта;
- иные основания, предусмотренные ст. 6, 10, 11 Федерального закона № 152-ФЗ.

6. Перечень действий с персональными данными и способы их обработки

6.1. Оператор осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

6.2. Обработка персональных данных осуществляется следующими способами:

- неавтоматизированная обработка;
- автоматизированная обработка с передачей по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка.

6.3. **Локализация баз данных.** При сборе персональных данных, в том числе посредством сети «Интернет», Оператор осуществляет запись, систематизацию, накопление, хранение, уточнение, извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории Российской Федерации.

6.4. **Трансграничная передача персональных данных.** До начала осуществления трансграничной передачи Оператор уведомляет Роскомнадзор. Передача осуществляется в соответствии со ст. 12 Федерального закона № 152-ФЗ с учётом требований о локализации.

6.5. Оператор вправе поручить обработку персональных данных другому лицу на основании договора, обеспечивая соблюдение таким лицом принципов и правил обработки, предусмотренных Федеральным законом № 152-ФЗ.

7. Меры по обеспечению безопасности персональных данных

7.1. При обработке персональных данных Оператор принимает необходимые правовые, организационные и технические меры защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

7.2. Обеспечение безопасности персональных данных достигается посредством:

- назначения лица, ответственного за организацию обработки персональных данных;
- принятия локальных нормативных актов и иных документов в области обработки и защиты персональных данных;
- применения организационных и технических мер (включая антивирусную защиту, межсетевое экранирование, контроль доступа, шифрование при необходимости);
- обнаружения фактов несанкционированного доступа и принятия необходимых мер;
- обеспечения записи, систематизации, накопления, хранения, уточнения, извлечения персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ;
- хранения персональных данных и их материальных носителей, обрабатываемых в разных целях и содержащих разные категории, отдельно друг от друга;

- установления правил доступа к персональным данным, обрабатываемым в информационной системе, а также обеспечения регистрации и учета всех действий;
- контроля за принимаемыми мерами и уровнем защищенности информационной системы;
- применения средств защиты информации, прошедших оценку соответствия;
- проведения внутренних проверок соблюдения требований не реже одного раза в год;
- иных мер, предусмотренных законодательством РФ.

8. Уведомление об утечке персональных данных

8.1. В случае выявления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов (инцидента, «утечки»), Оператор обязан:

8.1.1. Уведомить Роскомнадзор об инциденте в срок не позднее 24 часов с момента его обнаружения.

8.1.2. Уведомить Роскомнадзор о результатах расследования инцидента и принятых мерах в срок не позднее 72 часов с момента его обнаружения.

8.1.3. Уведомить субъекта персональных данных об инциденте в случае, если утечка данных создала риск причинения вреда правам и законным интересам субъекта.

8.2. Уведомление должно содержать: описание инцидента, категории и объём утекших персональных данных, перечень субъектов, чьи права могли быть нарушены, информацию о принятых и планируемых мерах, сведения о лице, ответственном за взаимодействие с Роскомнадзором.

9. Порядок реагирования на запросы и обращения субъектов персональных данных, их представителей и уполномоченных органов

9.1. Право субъекта на обращение

Субъект персональных данных или его законный представитель имеет право обратиться к Оператору с запросом (обращением) по следующим вопросам:

- подтверждение факта обработки персональных данных Оператором;
- получение информации о правовых основаниях, целях, способах обработки;
- получение сведений о сроках хранения;
- доступ к своим персональным данным (включая получение копий);
- уточнение (исправление) неточных персональных данных;
- блокирование или уничтожение персональных данных при их неправомерной обработке или утрате необходимости;
- отзыв согласия на обработку персональных данных;
- обжалование действий (бездействия) Оператора.

9.2. Способы и адреса направления запросов

Запрос (обращение) направляется одним из следующих способов:

1. **Почтовым отправлением** по адресу: 127083, г.Москва,
2. ул.8 Марта, д.1, стр.12, пом.XXXV, ком.19 с пометкой на конверте: «**По вопросам персональных данных**».

3. **Электронной почтой** на специальный адрес: info@msk-ix.ru с темой письма: «Запрос о персональных данных».
4. **Лично через секретариат** Оператора по вышеуказанному адресу в рабочие дни с 9:00 до 18:00.

Для ускорения обработки запроса рекомендуется использовать форму, приведённую в Приложении № 1 к настоящей Политике (типовая форма запроса размещена на сайте Оператора). Отсутствие заполнения по форме не является основанием для отказа, если запрос позволяет идентифицировать субъекта и понять суть требования.

9.3. Документы, удостоверяющие личность и полномочия

При направлении запроса в письменной форме (почтой или лично) субъект прилагает копию документа, удостоверяющего личность (паспорт). Представитель дополнительно прилагает документ, подтверждающий полномочия (нотариально заверенную доверенность).

При направлении запроса по электронной почте подписание электронной подписью не требуется, но Оператор вправе запросить скан-копию паспорта для идентификации перед предоставлением ответа.

9.4. Порядок рассмотрения запросов субъектов и их представителей

9.4.1. Запрос подлежит рассмотрению в срок не более 10 рабочих дней со дня его получения Оператором (ч. 1 ст. 20 Федерального закона № 152-ФЗ).

9.4.2. Если запрос направлен в электронной форме и не позволяет однозначно идентифицировать субъекта (отсутствует ФИО, контактные данные, копия документа), Оператор вправе запросить у субъекта дополнительные сведения по электронной почте. Срок приостанавливается до получения необходимых данных, но не более чем на 5 рабочих дней.

9.4.3. По результатам рассмотрения Оператор:

- предоставляет запрашиваемую информацию (в форме ответа на бумажном носителе или в электронном виде по выбору субъекта, если иное не указано в запросе);
- уточняет (исправляет) персональные данные, о чём уведомляет субъекта;
- блокирует или уничтожает персональные данные, если обработка признана неправомерной или отозвано согласие, и направляет уведомление.

9.4.4. При отказе в удовлетворении запроса Оператор направляет мотивированный ответ с указанием правового основания отказа (ст. 14, 20 152-ФЗ).

9.5. Реагирование на запросы уполномоченных органов (Роскомнадзор, прокуратура, суд)

9.5.1. Запросы уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) рассматриваются в сроки, установленные законодательством (обычно 15 рабочих дней, если иной срок не указан в запросе).

9.5.2. При получении запроса от Роскомнадзора о предоставлении информации, связанной с обработкой персональных данных (в том числе в рамках проверки), Оператор обязан направить запрашиваемые сведения в течение 10 рабочих дней с даты получения запроса (ч. 4 ст. 20 152-ФЗ).

9.5.3. Запросы судебных приставов, следственных органов, судов исполняются в порядке, установленном процессуальным законодательством (7–30 дней в зависимости от вида запроса).

9.5.4. Запросы иных государственных органов (ФНС, ПФР, СФР и др.) рассматриваются в рамках действующего законодательства в сроки, предусмотренные для предоставления отчётности или ответов на требования.

10. Обязанности работников Оператора

10.1. Работники Оператора, допущенные к обработке персональных данных, обязаны:

- знать и неукоснительно выполнять требования настоящей Политики, иных локальных нормативных актов по вопросам обработки и защиты персональных данных;
- обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей и в соответствии с целями обработки;
- не разглашать персональные данные, полученные в результате выполнения своих должностных обязанностей, третьим лицам без соответствующего разрешения;
- пресекать действия третьих лиц, которые могут привести к разглашению (уничтожению, искажению) персональных данных;
- выявлять факты разглашения (уничтожения, искажения) персональных данных и информировать об этом непосредственного руководителя и лицо, ответственное за обработку персональных данных;
- хранить тайну о сведениях, содержащих персональные данные, в соответствии с локальными актами Оператора;
- незамедлительно сообщить об утере или недостатке носителей персональных данных, а также о любых инцидентах.

10.2. Работникам запрещается несанкционированное копирование персональных данных на бумажные носители и на любые электронные носители, не предназначенные для хранения персональных данных, а также передача персональных данных по открытым каналам связи без применения средств криптографической защиты.

10.3. Каждый новый работник, непосредственно осуществляющий обработку персональных данных, подлежит ознакомлению с требованиями законодательства РФ, с настоящей Политикой и другими локальными актами под роспись и обязуется их соблюдать.

10.4. Лица, виновные в нарушении требований законодательства РФ в области защиты персональных данных, несут дисциплинарную, материальную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством.

11. Права субъекта персональных данных

11.1. Субъекты персональных данных имеют право на:

- полную информацию об их персональных данных, обрабатываемых в Операторе, включая подтверждение факта обработки, правовые основания и цели обработки, способы обработки, сроки обработки и хранения;
- доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
- уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- отзыв согласия на обработку персональных данных (при этом Оператор вправе продолжить обработку без согласия при наличии оснований, указанных в п. 2–11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Федерального закона № 152-ФЗ);
- принятие предусмотренных законом мер по защите своих прав, включая обжалование действий или бездействия Оператора в Роскомнадзор или в суд;
- требование о прекращении обработки персональных данных, их уничтожении при отсутствии законных оснований для их обработки;
- осуществление иных прав, предусмотренных законодательством РФ.

11.2. Запросы субъектов персональных данных должны быть рассмотрены в срок, не превышающий 10 рабочих дней со дня получения запроса. При наличии оснований для отказа в предоставлении информации Оператор обязан направить мотивированный ответ с указанием причин отказа в тот же срок.

11.3 Процедура отзыва согласия:

Способ отзыва:

- письменное заявление;
- электронный документ с электронной подписью.

Последствия отзыва:

- прекращение обработки (кроме случаев, предусмотренных законом);
- уничтожение данных при отсутствии иных законных оснований.

11.4. Защита прав

Субъект вправе:

- Обжаловать действия оператора:
 - в Роскомнадзор
 - в судебном порядке
- Требовать возмещения причиненного ущерба

11.5. Подтверждение личности

При обращении субъект обязан предоставить:

- Документ, удостоверяющий личность
- Контактные данные для обратной связи
- Подтверждение отношений с оператором (при необходимости)

11.6. Особенности при автоматизированная обработке:

Субъект имеет право на возражение, разъяснение последствий, уведомление о принятых решениях. Срок реагирования на возражения — 30 дней

11.7. Информирование

Оператор обязан:

- Уведомлять субъекта о:

- результатах рассмотрения запроса;
 - принятых мера
 - причинах отказа (при наличии).
- Предоставлять информацию в доступной форме.
 - Соблюдать сроки обработки запросов.

12. Порядок уничтожения, блокирования персональных данных

12.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту, с момента такого обращения.

12.2. В случае выявления неточных персональных данных при обращении субъекта Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту, с момента такого обращения, если блокирование не нарушает права и законные интересы субъекта или третьих лиц.

12.3. В случае подтверждения факта неточности персональных данных на основании сведений, представленных субъектом, или иных необходимых документов, Оператор уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование.

12.4. В случае выявления неправомерной обработки персональных данных Оператор в срок, не превышающий трех рабочих дней с даты выявления, прекращает неправомерную обработку.

12.5. Если обеспечить правомерность обработки невозможно, Оператор в срок, не превышающий десять рабочих дней с даты выявления неправомерной обработки, обязан уничтожить такие персональные данные.

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

12.7. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку и уничтожить данные в срок, не превышающий тридцати дней с даты достижения цели обработки, если иное не предусмотрено трудовым договором или федеральным законом.

12.8. В случае отзыва субъектом согласия на обработку персональных данных Оператор прекращает их обработку и, если сохранение данных более не требуется для целей обработки, уничтожает данные в срок, не превышающий тридцать дней с даты поступления отзыва, если иное не предусмотрено трудовым договором или федеральным законом.

12.9. В случае отсутствия возможности уничтожения персональных данных в течение указанных сроков Оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

12.10. При достижении целей обработки персональных данных либо при утрате необходимости в их достижении Оператор обязан прекратить обработку и уничтожить персональные данные либо обеспечить их обезличивание в порядке, установленном Приказом Роскомнадзора от 19.06.2025 № 140 и Постановлением Правительства РФ от 01.08.2025 № 1154. Обезличивание персональных данных осуществляется с применением следующих методов:

- введение идентификаторов;
- изменение состава данных;
- декомпозиция;
- перемешивание;
- преобразование (агрегирование).

13. Ответственность

13.1. Оператор несёт ответственность за нарушение законодательства в области персональных данных в соответствии с действующим законодательством Российской Федерации.

13.2. Административная ответственность за нарушение правил обработки персональных данных установлена ст. 13.11 КоАП РФ (в редакции, действующей с 30 мая 2025 года) и включает, в частности:

- за обработку персональных данных в случаях, не предусмотренных законом, либо обработку, несовместимую с целями сбора: на юридических лиц – от 150 000 до 300 000 рублей;
- за повторное нарушение: на юридических лиц – от 300 000 до 500 000 рублей;
- за невыполнение обязанности по опубликованию Политики: на юридических лиц – от 30 000 до 60 000 рублей;
- за утечку персональных данных: на юридических лиц – от 100 000 до 200 000 рублей;
- за повторную утечку персональных данных (непринятие мер по обеспечению безопасности): для юридических лиц – штраф от 1% до 3% выручки, но не менее 20 000 000 рублей и не более 500 000 000 рублей;
- за невыполнение обязанности по уведомлению Роскомнадзора об утечке персональных данных: на юридических лиц – от 1 000 000 до 3 000 000 рублей;
- за непредставление уведомления о начале обработки персональных данных (отсутствие регистрации в реестре операторов) — штрафы от 50 000 до 3 000 000 рублей;
- за незаконную передачу биометрических персональных данных: на юридических лиц — от 1 300 000 до 1 500 000 рублей.

13.3. Уголовная ответственность за незаконное использование и передачу персональных данных установлена ст. 137, 272–274 УК РФ (включая создание и распространение вредоносных программ для незаконного получения персональных данных).

14. Управление инцидентами в области защиты персональных данных

14.1. Оператор создаёт и поддерживает систему управления инцидентами, включающую:

- процедуры выявления, фиксации и классификации инцидентов;
- назначение ответственных за реагирование на инциденты;
- порядок оперативного информирования руководства и уполномоченных органов об инцидентах;
- план действий по ликвидации последствий инцидента и минимизации ущерба.

14.2. Все инциденты, связанные с персональными данными, регистрируются в специальном журнале учёта инцидентов. Проводится анализ причин инцидента и разрабатываются меры по предотвращению подобных инцидентов в будущем.

15. Мониторинг и аудит

15.1. Оператор регулярно проводит мониторинг соблюдения требований настоящей Политики и действующего законодательства в области защиты персональных данных.

15.2. Аудит системы защиты персональных данных проводится не реже одного раза в год. При необходимости могут проводиться внеплановые аудиты (при изменении законодательства, после инцидентов, при изменении технологических процессов).

15.3. По результатам аудита составляется отчёт с указанием выявленных недостатков, рекомендаций по их устранению и сроков выполнения мероприятий.

16. Взаимодействие с третьими лицами при обработке персональных данных

16.1. Оператор вправе передавать персональные данные субъектов третьим лицам либо поручать им обработку данных только при наличии законного основания. К таким основаниям относятся: получение явного согласия субъекта; прямая обязанность оператора, установленная федеральным законом; необходимость для исполнения договора, стороной которого является субъект.

16.2. Если передача данных осуществляется в целях, не вытекающих напрямую из закона или договора, оператор обязан получить от субъекта письменное согласие. С 01 сентября 2025 года такое согласие оформляется отдельным документом — включать его в текст договора, оферты или анкеты запрещено. В согласии должны быть чётко указаны: наименование третьего лица, цель передачи, перечень передаваемых данных и разрешённых действий с ними, срок действия согласия и порядок его отзыва. Субъект вправе в любой момент отозвать согласие — оператор обязан прекратить передачу данных в установленный срок.

16.3. Оператор может поручить обработку данных третьему лицу (обработчику) на основании договора. В таком договоре (поручении) необходимо зафиксировать: перечень передаваемых персональных данных; перечень действий, которые обработчик вправе совершать с данными; цели обработки (строго в интересах оператора); обязательство обработчика соблюдать конфиденциальность и обеспечивать безопасность данных в соответствии со статьёй 19 Федерального закона № 152-ФЗ; обязанность обработчика по запросу оператора предоставлять документы и информацию, подтверждающие соблюдение требований закона; условие об уведомлении оператора о случаях неправомерного доступа или утечки данных. При этом ответственность перед субъектом за действия обработчика несёт оператор. Исключение: если поручение дано иностранному лицу (физическому или юридическому), ответственность перед субъектом несут и оператор, и обработчик.

16.4. При передаче данных без поручения (когда третье лицо действует как самостоятельный оператор в собственных целях) ответственность за соблюдение требований 152-ФЗ распределяется между оператором и получателем данных в соответствии с конкретными действиями каждой стороны.

16.5. Перед передачей данных оператор оценивает надёжность третьего лица: проверяет наличие у него политики конфиденциальности, реализованных мер защиты информации, а также соответствие применяемых технических и организационных мер требованиям законодательства.

16.6. При трансграничной передаче персональных данных (в страну, не обеспечивающую адекватную защиту по решению Роскомнадзора) помимо согласия субъекта может потребоваться предварительное уведомление Роскомнадзора.

16.7. Оператор ведёт внутренний учёт фактов передачи данных: фиксирует, кому, какие данные и на каком основании были переданы. Это необходимо для оперативного реагирования на претензии субъектов и для прохождения проверок.

16.8. В случае получения от субъекта обращения (запроса, требования) в связи с передачей его данных третьим лицам оператор рассматривает его в установленном порядке и информирует заявителя о результатах.

17. Заключительные положения

17.1. Настоящая Политика является локальным нормативным актом Оператора. Действующая редакция Политики на бумажном носителе хранится по месту нахождения Оператора и доступна для ознакомления работникам и субъектам персональных данных по их запросу.

17.2. Электронная версия действующей редакции настоящей Политики публикуется в открытом доступе в сети Интернет на официальном сайте Оператора по адресу: <https://www.msk-ix.ru/legal/>.

17.3. Контроль за исполнением требований настоящей Политики возлагается на лицо, ответственное за организацию обработки персональных данных в АО «ЦВКС «МСК-IX», назначаемое приказом Генерального директора.

17.4. Вопросы, не урегулированные настоящей Политикой, разрешаются в соответствии с действующим законодательством Российской Федерации.

Приложение № 1

Рекомендуемая форма запроса субъекта персональных данных

Генеральному директору АО «ЦВКС «МСК-IX»

от _____

(фамилия, имя, отчество полностью)

проживающего(ей) по адресу: _____

паспорт: серия _____ номер _____

контактный телефон: _____

адрес эл. почты (при наличии): _____

ЗАПРОС

о предоставлении информации, касающейся обработки моих персональных данных

Прошу в соответствии со ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» предоставить мне информацию, подтверждающую факт обработки моих персональных данных Оператором, правовые основания и цели обработки, перечень обрабатываемых персональных данных, источники их получения, сроки хранения, сведения о трансграничной передаче (если имеется), а также предоставить возможность ознакомления с моими персональными данными (получить их копии).

(При необходимости – иные требования: об уточнении, блокировании, уничтожении, отзыве согласия и т.д. – указать отдельно.)

Даю согласие на обработку моих персональных данных в целях рассмотрения настоящего запроса.

Дата _____ Подпись _____

Примечание: при направлении запроса об отзыве согласия на обработку персональных данных в тексте запроса указывается: «Я, _____, отзываю ранее данное мной согласие на обработку моих персональных данных, предоставленное (указать когда и в рамках какого договора/действия). Прошу прекратить обработку моих персональных данных и уничтожить их в соответствии с п. 12.8 Политики».