Общество с ограниченной ответственностью
«Центр современных технологий безопасности информации»

УТВЕРЖДАЮ
Генеральный директор ООО «ЦСТБИ»

_____ С.В. Штейнбок
«02» сентября 2026 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников (иных лиц)

1. Общие положения

1.1. Настоящее Положение является локальным нормативным актом ООО «Центр современных технологий безопасности информации» (далее - Общество), принятым с учётом требований, в частности, гл. 14 Трудового кодекса РФ, Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных).
1.2. В Положении устанавливаются:

- цель, порядок и условия обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются, категории (перечни) обрабатываемых персональных данных, способы, сроки их обработки и хранения, порядок уничтожения таких данных при достижении целей обработки или при наступлении иных законных оснований;
- положения, касающиеся защиты персональных данных, процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в области персональных данных, на устранение последствий таких нарушений.

1.3. В Положении используются термины и определения в соответствии с их значениями, определенными в Законе о персональных данных.
1.4. Положение вступает в силу с момента его утверждения генеральным директором и действует до его отмены приказом генерального директора или до введения нового Положения.
1.5. Внесение изменений в Положение производится приказом генерального директора. Изменения вступают в силу с момента подписания соответствующего приказа.

2. Категории субъектов персональных данных

2.1. К субъектам, персональные данные которых обрабатываются в Обществе в соответствии с Положением, относятся:

- кандидаты для приёма на работу в Общество;
- работники Общества;
- бывшие работники Общества;
- члены семей работников Общества - в случаях, когда согласно законодательству сведения о них предоставляются работником.

3. Цели обработки персональных данных, категории (перечни) обрабатываемых персональных данных

3.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
3.2. Содержание и объем обрабатываемых персональных данных должны соответствовать

заявленной цели обработки, предусмотренной в настоящем разделе. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленной цели их обработки.

Персональные данные обрабатываются Оператором с целью применения и исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ними отношений, в том числе:

• при содействии в трудоустройстве;
• ведении кадрового и бухгалтерского учёта;
• содействии работникам в получении образования;
• оформлении награждений и поощрений;
• предоставлении со стороны Общества установленных законодательством условий труда, гарантий и компенсаций;
• заполнении и передаче в уполномоченные органы требуемых форм отчётности;
• обеспечении личной безопасности работников и сохранности имущества;
• осуществлении контроля за количеством и качеством выполняемой работы;
• оценке профессиональных качеств кандидатов и работников, в том числе при проведении аттестации.

3.3. Обработка персональных данных в целях обеспечения соблюдения трудового законодательства РФ.

В соответствии с настоящим разделом Положения Оператор определяет категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении цели их обработки или при наступлении иных законных оснований применительно к такой цели, как «обеспечение соблюдения трудового законодательства РФ (в т.ч. содействие работникам в трудоустройстве, получении образования и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы и обеспечение сохранности имущества, обеспечение соблюдения законов и иных нормативных правовых актов)».

3.4. Категории субъектов персональных данных, цели и объем обрабатываемых данных.

3.4.1. Работники Оператора

- Цель обработки: Обеспечение соблюдения трудового законодательства РФ, ведение кадрового и бухгалтерского учета, исполнение трудового договора, обеспечение личной безопасности работников и сохранности имущества.
- Перечень данных: ФИО, пол, дата и место рождения, паспортные данные, СНИЛС, ИНН, адрес регистрации и проживания, контактные данные, сведения о семейном положении, образовании, воинском учете, трудовой деятельности, доходах, номера банковских счетов.
- Порядок и сроки: Обработка осуществляется смешанным способом с передачей по внутренней сети. Срок хранения — в течение действия трудового договора, а после его прекращения — в течение сроков, установленных архивным законодательством (личные дела — 50 лет, бухгалтерская документация — не менее 5 лет).

3.4.2. Кандидаты для приема на работу

• Цель обработки: оценка профессиональных качеств кандидата и принятие кадровых решений.

• Перечень данных: ФИО, контактные данные, сведения об образовании, квалификации, опыте работы, профессиональные навыки и деловые качества, а также результаты профессиональных тестирований, оценочные листы, необходимые для оценки его деловых и профессиональных качеств.

• Порядок и сроки: данные обрабатываются с согласия кандидата. При отказе в трудоустройстве данные подлежат уничтожению в срок, не превышающий 30 дней, если кандидат не дал согласие на их хранение для рассмотрения на другие вакансии. Согласие на хранение данных в кадровом резерве даётся на срок не более 1 года с возможностью продления по письменному заявлению кандидата. По истечении срока действия согласия (либо при отсутствии продления) данные подлежат уничтожению в течение 30 дней.

• Порядок удаления персональных данных, обрабатываемых в целях оценки профессиональных качеств:

- для кандидатов, не принятых на работу: персональные данные, полученные в ходе оценки (результаты тестов, оценочные листы, резюме), подлежат уничтожению в течение 30 дней с момента принятия решения об отказе в трудоустройстве, если иное не предусмотрено письменным согласием кандидата. Уничтожение оформляется в порядке, предусмотренном пп. 6.5–6.6 настоящего Положения;
- для работников, прошедших оценку: результаты оценки включаются в состав личного дела работника и хранятся в течение 50 лет.

3.4.3. Бывшие работники

- Цель обработки: Исполнение требований законодательства РФ (налоговый и бухгалтерский учет, архивное дело), защита прав и законных интересов Оператора.
- Перечень данных: Данные, необходимые для расчета и перечисления налогов, пенсионных отчислений, подтверждения трудового стажа.
- Порядок и сроки: Обработка осуществляется в сроки, установленные законодательством об архивном деле (50 лет для личных дел), после чего данные подлежат уничтожению.

3.4.4. Члены семей работников

- Цель обработки: Предоставление гарантий и компенсаций, предусмотренных трудовым законодательством, ведение воинского учета (при необходимости).
- Перечень данных: ФИО, степень родства, дата и место рождения (в объеме, предоставленном самим работником).
- Порядок и сроки хранения: Персональные данные членов семей работников хранятся в форме, позволяющей определить субъекта данных, не дольше, чем этого требуют цели их обработки. Базовый срок хранения: если данные были предоставлены в связи с трудовой деятельностью работника (например, для получения льгот или оформления пропуска), они хранятся в течение срока действия трудового договора работника. Срок хранения после прекращения трудового договора: В случае, если обработка данных членов семьи была необходима для исполнения договора или законодательства, но не была завершена к моменту увольнения работника, их данные хранятся в течение срока, установленного законодательством для соответствующих документов (например, если данные включены в личное дело работника, хранящееся 50 лет).
- Порядок уничтожения: Уничтожение персональных данных членов семьи производится в следующих случаях:
    - Достижение цели обработки;
    - Истечение срока хранения, установленного Политикой или законодательством;
    - Отзыв согласия субъектом (если обработка основывалась исключительно на согласии и отсутствуют законные основания для продолжения обработки).
    - Срок уничтожения: Данные подлежат уничтожению в срок, не превышающий 30 дней с момента наступления основания для уничтожения (достижение цели, отзыв согласия и т.п.), если иной срок не предусмотрен договором или законодательством.

- Порядок уничтожения: Уничтожение производится комиссией, создаваемой приказом Генерального директора, с составлением Акта об уничтожении персональных данных. В акте указывается перечень уничтоженных данных членов семей, способ уничтожения (шредер, гарантированное удаление файлов) и дата.

4. Порядок и условия обработки персональных данных

4.1. Общество уведомляет Роскомнадзор в порядке, установленном законодательством, до начала обработки персональных данных, если такое уведомление требуется.
4.2. Правовым основанием обработки персональных данных являются Трудовой кодекс РФ, иные нормативные правовые акты, содержащие нормы трудового права, Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных", Федеральный закон от 06.12.2011 N 402-ФЗ "О бухгалтерском учете", Постановление Правительства РФ от 27.11.2006 N 719 "Об утверждении Положения о воинском учёте".
4.3. Обработка персональных данных осуществляется с соблюдением принципов и условий, предусмотренных законодательством в области персональных данных и настоящим Положением.
4.4. Обработка персональных данных в Обществе выполняется следующими способами:

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

4.5. Обработка персональных данных в Обществе осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством в области персональных данных.
4.5.1. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 Закона о персональных данных.
Согласие на обработку таких персональных данных оформляется отдельно от других согласий на обработку персональных данных. Согласие предоставляется субъектом персональных данных лично либо в форме электронного документа, подписанного электронной подписью, с использованием информационной системы Роскомнадзора.
4.6. Общество не осуществляет трансграничную передачу персональных данных.
4.7. Обработка персональных данных осуществляется путём сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, предоставление, использования, блокирования, удаления, уничтожения персональных данных, в том числе с помощью средств вычислительной техники.
4.7.1. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных в Обществе осуществляются посредством:

- получения оригиналов документов либо их копий;
- копирования оригиналов документов;
- внесения сведений в учётные формы на бумажных и электронных носителях;
- создания документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесения персональных данных в информационные системы персональных данных.

4.8. Распространение, предоставление, доступ персональных данных субъектов персональных данных осуществляется в случаях и в порядке, предусмотренных законодательством в области персональных данных и Положением.

5. Сроки обработки и хранения персональных данных

5.1. Обработка персональных данных в Обществе прекращается в следующих случаях:

- при выявлении факта неправомерной обработки персональных данных. Срок прекращения обработки - в течение трех рабочих дней с даты выявления такого факта;
- при достижении целей их обработки (за некоторыми исключениями);
- по истечении срока действия или при отзыве субъектом персональных данных согласия на обработку его персональных данных (за некоторыми исключениями), если в соответствии с Законом о персональных данных их обработка допускается только с согласия;
- при обращении субъекта персональных данных к Обществу с требованием о прекращении обработки персональных данных (за исключением случаев, предусмотренных ч. 5.1 ст. 21 Закона о персональных данных). Срок прекращения обработки - не более 10 рабочих дней с даты получения требования (с возможностью продления не более чем на пять рабочих дней, если направлено уведомление о причинах продления).

5.2. Персональные данные хранятся в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Исключение - случаи, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных.

5.3. Персональные данные на бумажных носителях хранятся в Обществе в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации", Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утв. Приказом Росархива от 20.12.2019 N 236)).

5.4. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

6. Порядок блокирования и уничтожения персональных данных

6.1. Общество блокирует персональные данные в порядке и на условиях, предусмотренных законодательством в области персональных данных.

6.2. Персональные данные подлежат уничтожению Оператором в случаях:

- достижения цели обработки персональных данных;
- отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- выявления неправомерных действий с персональными данными, а также в иных случаях, предусмотренных действующим законодательством Российской Федерации.

6.3. В случае достижения цели обработки персональных данных Оператор обязуется 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 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.

6.4. В случае, если субъект персональных данных отозвал свое согласие на обработку персональных данных Оператор обязуется 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 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.

6.5. Уничтожение персональных данных осуществляет комиссия, созданная приказом генерального директора.

6.5.1. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

6.5.2. Персональные данные на бумажных носителях уничтожаются с использованием шредера. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путём удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

6.5.3. Комиссия подтверждает уничтожение персональных данных, указанных в пп. 6.2, 6.3, 6.4 настоящего Положения, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденным Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

• актом об уничтожении персональных данных — если данные обрабатываются без использования средств автоматизации;

• актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных — если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учётом сведений, которые должны содержаться в указанных документах, утверждаются приказом генерального директора.

6.6. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

6.7. Уничтожение персональных данных, не указанных в пп. 6.3–6.5 настоящего Положения, подтверждается актом, который оформляется непосредственно после уничтожения таких данных. Форма акта утверждается приказом генерального директора.

6.8. Порядок удаления персональных данных, обрабатываемых в целях оценки профессиональных качеств:

• для кандидатов, не принятых на работу: персональные данные, полученные в ходе оценки (результаты тестов, оценочные листы, резюме), подлежат уничтожению в течение 30 дней с момента принятия решения об отказе в трудоустройстве, если иное не предусмотрено письменным согласием кандидата;

• для работников, прошедших оценку: результаты оценки включаются в состав личного дела работника и хранятся в течение 50 лет.

Уничтожение персональных данных, указанных в настоящем пункте, оформляется в порядке, предусмотренном пп. 6.5–6.6 настоящего Положения.

7. Защита персональных данных. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений

7.1. Без письменного согласия субъекта персональных данных Общество не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

7.1.1. Запрещено раскрывать и распространять персональные данные субъектов персональных данных по телефону.
7.2. С целью защиты персональных данных в Обществе приказами генерального директора назначаются (утверждаются):

- работник, ответственный за организацию обработки персональных данных;
- перечень должностей, при замещении которых обрабатываются персональные данные;
- перечень персональных данных, к которым имеют доступ работники, занимающие должности, предусматривающие обработку персональных данных;
- порядок доступа в помещения, в которых ведется обработка персональных данных;
- порядок передачи персональных данных в пределах Общества;
- форма согласия на обработку персональных данных, форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
- порядок защиты персональных данных при их обработке в информационных системах персональных данных;
- порядок проведения внутренних расследований, проверок;
- иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области персональных данных.

7.3. Работники, которые занимают должности, предусматривающие обработку персональных данных, допускаются к ней после подписания обязательства об их неразглашении.
7.4. Материальные носители персональных данных хранятся в шкафах, запирающихся на ключ. Помещения Общества, в которых они размещаются, оборудуются запирающими устройствами. Выдача ключей от шкафов и помещений осуществляется под подпись.
7.5. Доступ к персональной информации, содержащейся в информационных системах Общества, осуществляется по индивидуальным паролям.
7.6. В Обществе используется сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.
7.7. Работники Общества, обрабатывающие персональные данные, периодически проходят обучение требованиям законодательства в области персональных данных.
7.8. В должностные инструкции работников Общества, обрабатывающих персональные данные, включаются, в частности, положения о необходимости сообщать о любых случаях несанкционированного доступа к персональным данным.
7.9. В Обществе проводятся внутренние расследования в следующих ситуациях:
• при неправомерной или случайной передаче (предоставлении, распространении, доступе) персональных данных, повлекшей нарушение прав субъектов персональных данных;
• в иных случаях, предусмотренных законодательством в области персональных данных.
7.10. Работник, ответственный за организацию обработки персональных данных, осуществляет внутренний контроль:

- за соблюдением работниками, уполномоченными на обработку персональных данных, требований законодательства в области персональных данных, локальных нормативных актов;
- соответствием указанных актов требованиям законодательства в области персональных данных.

Внутренний контроль проходит в виде внутренних проверок.
7.10.1. Внутренние плановые проверки осуществляются на основании ежегодного плана, который утверждается генеральным директором.
7.10.2. Внутренние внеплановые проверки осуществляются по решению работника, ответственного за организацию обработки персональных данных. Основанием для них служит информация о нарушении законодательства в области персональных данных, поступившая в устном или письменном виде.
7.10.3. По итогам внутренней проверки оформляется докладная записка на имя генерального директора. Если выявлены нарушения, в документе приводится перечень мероприятий по их устранению и соответствующие сроки.

7.11. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (далее - инцидент).
7.11.1. В случае инцидента Общество в течение 24 часов уведомляет Роскомнадзор:

- об инциденте;
- его предполагаемых причинах и вреде, причиненном правам субъекта (нескольким субъектам) персональных данных;
- принятых мерах по устранению последствий инцидента;
- представителе Общества, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

При направлении уведомления нужно руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными Приказом Роскомнадзора от 14.11.2022 N 187.
7.11.2. В течение 72 часов Общество обязано сделать следующее:

- уведомить Роскомнадзор о результатах внутреннего расследования;
- предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

При направлении уведомления также необходимо руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учёта инцидентов в области персональных данных, утвержденными Приказом Роскомнадзора от 14.11.2022 N 187.
7.12. В случае предоставления субъектом персональных данных (его представителем) подтвержденной информации о том, что персональные данные являются неполными, неточными или неактуальными, в них вносятся изменения в течение семи рабочих дней. Общество уведомляет в письменном виде субъекта персональных данных (его представителя) о внесенных изменениях и сообщает (по электронной почте) о них третьим лицам, которым были переданы персональные данные.
7.13. Общество уведомляет субъекта персональных данных (его представителя) об устранении нарушений в части неправомерной обработки персональных данных. Уведомляется также Роскомнадзор, если он направил обращение субъекта персональных данных (его представителя) либо сам сделал запрос.
7.14. В случае уничтожения персональных данных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки, Общество уведомляет в течении семи рабочих дней субъекта персональных данных (его представителя) о принятых мерах в письменном виде. Общество уведомляет по электронной почте также третьих лиц, которым были переданы такие персональные данные.

8. Ответственность за нарушение норм, регулирующих обработку персональных данных

8.1. Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами. Кроме того, они привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.
8.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к их защите, установленных Законом о персональных данных, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.