СВОДКА И ПЛАН ДЕЙСТВИЙ ПО 152-ФЗ

Общество с ограниченной ответственностью «Пример»

Процессов обработки: 2. Требований проверено: 10; требуется выполнить: 7; проверить: 0; выполнено: 3.

Требование	Норма	Что сделать	Риск
Уведомление о намерении осуществлять обработку ПДн	ст. 22 152-ФЗ	Подать уведомление на pd.rkn.gov.ru (сведения — в документе «Уведомление в РКН (сведения)»)	штраф для юрлиц ориентировочно 100–300 тыс. ₽ (ст. 13.11 КоАП)
Политика в отношении обработки ПДн, опубликованная на сайте	ч. 1, 2 ст. 18.1 152-ФЗ	Утвердить приказом политику (готовый проект в пакете) и разместить на сайте	штраф по ст. 13.11 КоАП; предписание РКН
Локальные акты по обработке ПДн и ознакомление работников	п. 2, 6 ч. 1 ст. 18.1 152-ФЗ	Утвердить положение (проект в пакете), ознакомить работников под подпись	
Согласие субъекта, оформленное отдельно от иных документов	ст. 9 152-ФЗ	Использовать формы согласий из пакета: Обработка обращений клиентов с сайта	штраф для юрлиц ориентировочно 300–700 тыс. ₽, повторно — 1–1,5 млн ₽ (ст. 13.11 КоАП)
Меры защиты для ИС «1С:Зарплата и управление персоналом» — уровень защищённости УЗ-4	ст. 19 152-ФЗ; ПП РФ № 1119; приказ ФСТЭК № 21	Утвердить акт определения УЗ (проект в пакете) и выполнить меры для УЗ-4	при утечке — от 3 до 20 млн ₽ в зависимости от объёма и категорий (1 тыс.+ субъектов — 3–5 млн, 10 тыс.+ — 5–10 млн, 100 тыс. + — 10–15 млн, спецкатегории — 10–15 млн, биометрия — 15–

			20 млн); при повторной утечке — оборотный штраф 1–3% выручки (не менее 20 млн ₽, для спецкатегорий и биометрии — 25 млн ₽, не более 500 млн ₽)
Меры защиты для ИС «Сайт и CRM» — уровень защищённости УЗ-4	ст. 19 152-ФЗ; ПП РФ № 1119; приказ ФСТЭК № 21	Утвердить акт определения УЗ (проект в пакете) и выполнить меры для УЗ-4	при утечке — от 3 до 20 млн ₽ в зависимости от объёма и категорий (1 тыс.+ субъектов — 3–5 млн, 10 тыс.+ — 5–10 млн, 100 тыс. + — 10–15 млн, спецкатегории — 10–15 млн, биометрия — 15–20 млн); при повторной утечке — оборотный штраф 1–3% выручки (не менее 20 млн ₽, для спецкатегорий и биометрии — 25 млн ₽, не более 500 млн ₽)
Порядок уведомления РКН об утечке (24 часа / 72 часа)	ч. 3.1 ст. 21 152-ФЗ	Закрепить в положении порядок реагирования на инциденты и взаимодействия с ГосСОПКА	штраф для юрлиц ориентировочно 1–3 млн ₽ за неуведомление РКН об утечке

Документы в пакете являются проектами и вступают в силу после утверждения руководителем Оператора. Суммы штрафов приведены ориентировочно; рекомендуется сверка с действующей редакцией ст. 13.11 КоАП РФ.

УТВЕРЖДЕНО
приказом ООО «Пример»
от «___» _____ 20__ г. № ____

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общество с ограниченной ответственностью «Пример»

1. Общие положения

1.1. Настоящая Политика определяет порядок и условия обработки персональных данных оператором — Общество с ограниченной ответственностью «Пример» (ИНН 7700000000, ОГРН 1027700000000, адрес: 123456, г. Москва, ул. Примерная, д. 1) (далее — Оператор) и меры по обеспечению их безопасности. Политика разработана во исполнение ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон).

1.2. Политика публикуется в свободном доступе, в том числе на сайте Оператора (https://example.ru), и применяется ко всем персональным данным, которые обрабатывает Оператор.

1.3. Основные понятия используются в значениях, определённых ст. 3 Закона.

2. Принципы обработки

2.1. Обработка осуществляется на законной и справедливой основе, ограничивается достижением конкретных, заранее определённых и законных целей; обрабатываются только персональные данные, отвечающие целям обработки, в объёме, не избыточном по отношению к ним; обеспечиваются точность и актуальность данных; персональные данные хранятся не дольше, чем этого требуют цели обработки, и уничтожаются по достижении целей.

3. Цели, категории и перечень персональных данных, категории субъектов, сроки

3.1. Цель: Исполнение трудового договора и требований трудового законодательства (процесс «Кадровый учёт»). Категории субъектов: работники; бывшие работники; кандидаты. Перечень данных: ФИО; дата рождения; паспортные данные; адрес; телефон; СНИЛС; ИНН; сведения о трудовой деятельности. Категория: иные. Правовое основание: трудовой договор; закон. Действия: сбор, запись, систематизация, накопление, хранение, уточнение, использование, передача, удаление, уничтожение. Способ обработки: смешанная. Срок обработки и хранения: 50 лет для кадровых документов по Закону об

архивном деле; иное — до достижения цели. Порядок уничтожения: удаление из ИС, уничтожение бумажных носителей шредером с составлением акта.

3.2. Цель: Обработка заявок и обращений, заключение и исполнение договоров (процесс «Обработка обращений клиентов с сайта»). Категории субъектов: клиенты; посетители сайта. Перечень данных: ФИО; телефон; адрес эл. почты; файлы cookie. Категория: иные. Правовое основание: согласие; договор. Действия: сбор, запись, хранение, использование, удаление, уничтожение. Способ обработки: автоматизированная. Срок обработки и хранения: 3 года после последнего обращения или до отзыва согласия. Порядок уничтожения: удаление из CRM и с сайта с составлением акта.

4. Условия обработки и передачи

4.1. Обработка осуществляется с согласия субъекта, за исключением случаев, предусмотренных Законом (в том числе для исполнения договора, стороной которого является субъект, и для выполнения обязанностей, возложенных на Оператора законодательством). Согласие оформляется отдельно от иных документов.

4.2. Оператор передаёт персональные данные третьим лицам только при наличии оснований, предусмотренных Законом: СФР, ФНС, банк для зарплатного проекта.

4.3. Трансграничная передача персональных данных не осуществляется.

4.4. Запись, систематизация, накопление, хранение, уточнение и извлечение персональных данных граждан Российской Федерации осуществляются с использованием баз данных, находящихся на территории Российской Федерации (Российская Федерация, г. Москва, ЦОД провайдера).

5. Права субъектов

5.1. Субъект вправе получать сведения об обработке своих персональных данных, требовать их уточнения, блокирования или уничтожения, если данные неполные, устаревшие, неточные, незаконно получены или не являются необходимыми для заявленной цели, отозвать согласие, обжаловать действия Оператора в уполномоченный орган или в суд.

5.2. Запросы направляются по адресу 123456, г. Москва, ул. Примерная, д. 1 или по эл. почте pd@example.ru. Оператор отвечает в течение 10 рабочих дней с даты получения запроса; срок может быть продлён не более чем на 5 рабочих дней с направлением мотивированного уведомления.

6. Меры обеспечения безопасности

6.1. Оператор назначил ответственного за организацию обработки персональных данных (Юрисконсульт Петров Пётр Петрович), издал локальные акты, определил уровни защищённости персональных данных в информационных системах, применяет правовые, организационные и технические меры защиты: антивирус, межсетевой экран, разграничение доступа, резервное копирование.

6.2. При выявлении неправомерной или случайной передачи персональных данных, повлёкшей нарушение прав субъектов, Оператор уведомляет уполномоченный орган в течение 24 часов о произошедшем инциденте и в течение 72 часов о результатах внутреннего расследования (ч. 3.1 ст. 21 Закона).

7. Заключительные положения

7.1. Политика пересматривается при изменении законодательства и процессов обработки. Действующая редакция размещается на сайте Оператора. Дата редакции: 27.11.2026.

УТВЕРЖДЕНО
приказом ООО «Пример»
от «___» _____ 20__ г. № ____

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общество с ограниченной ответственностью «Пример»

1. Назначение

Положение устанавливает порядок обработки персональных данных работниками Оператора, доступа к ним, их хранения, передачи, уничтожения и реагирования на инциденты.

2. Доступ

Доступ к персональным данным имеют только работники, которым он необходим для выполнения трудовых обязанностей, по перечню, утверждаемому руководителем. Работники знакомятся с Политикой и настоящим Положением под подпись и подписывают обязательство о неразглашении.

3. Обработка без средств автоматизации

Материальные носители хранятся раздельно по целям обработки в запираемых шкафах; доступ к помещениям ограничен.

4. Обработка в информационных системах

В информационных системах применяются меры, соответствующие установленным уровням защищённости: «1С:Зарплата и управление персоналом» — УЗ-4; «Сайт и CRM» — УЗ-4. Учётные записи персональные, пароли не передаются, права доступа пересматриваются при смене обязанностей.

5. Запросы субъектов

Запросы субъектов регистрируются в журнале и рассматриваются ответственным (Петров Пётр Петрович) в течение 10 рабочих дней.

6. Уничтожение

По достижении целей или при отзыве согласия персональные данные уничтожаются в сроки, установленные ст. 21 Закона; уничтожение подтверждается актом (и выгрузкой из журнала событий ИС — при автоматизированной обработке).

7. Инциденты

Работник, обнаруживший утечку или неправомерный доступ, немедленно сообщает ответственному. Ответственный обеспечивает уведомление Роскомнадзора в течение 24 часов о факте инцидента и в течение 72 часов о результатах расследования, а также взаимодействие с ГосСОПКА.

8. Контроль

Ответственный не реже одного раза в год проводит внутренний контроль соответствия обработки требованиям Закона и оценку вреда, который может быть причинён субъектам.

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ПРИМЕР»

ПРИКАЗ

г. Москва «___» _____ 20__ г. № ____

Об организации обработки персональных данных

В целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных Юрисконсульт Петров Пётр Петрович.

2. Утвердить Политику в отношении обработки персональных данных и Положение об обработке и защите персональных данных; разместить Политику на сайте Оператора.

3. Утвердить уровни защищённости персональных данных в информационных системах согласно Акту.

4. Ответственному ознакомить работников с настоящим приказом и документами под подпись в течение 10 дней.

5. Контроль исполнения приказа оставляю за собой.

Генеральный директор _____ / Иванов Иван Иванович /

С приказом ознакомлен(а): _____ / Петров Пётр Петрович / «___» _____ 20__ г.

УТВЕРЖДЕНО
приказом ООО «Пример»
от «___» _____ 20__ г. № ____

АКТ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общество с ограниченной ответственностью «Пример»

Комиссия в составе: председатель — _____; члены — _____, _____ провела оценку информационных систем персональных данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах, утверждёнными постановлением Правительства РФ от 01.11.2012 № 1119.

Информационная система	Уровень защищённости	Обоснование
1С:Зарплата и управление персоналом	УЗ-4	угрозы 3-го типа; категория ПДн — иные; только сотрудники; не более 100 000 субъектов (процесс «Кадровый учёт»)
Сайт и CRM	УЗ-4	угрозы 3-го типа; категория ПДн — иные; не только сотрудники; не более 100 000 субъектов (процесс «Обработка обращений клиентов с сайта»)

Тип актуальных угроз определён: 3-й (на основании модели угроз Оператора).

Председатель комиссии _____ / _____ /
Члены комиссии _____ / _____ /

СВЕДЕНИЯ ДЛЯ УВЕДОМЛЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

для заполнения формы на pd.rkn.gov.ru (ч. 3 ст. 22 152-ФЗ)

Наименование (ФИО) оператора	Общество с ограниченной ответственностью «Пример»
ИНН / ОГРН	7700000000 / 1027700000000
Адрес оператора	123456, г. Москва, ул. Примерная, д. 1
Цели обработки	Кадровый учёт: Исполнение трудового договора и требований трудового законодательства | Обработка обращений клиентов с сайта: Обработка заявок и обращений, заключение и исполнение договоров
Категории ПДн	иные. Перечень: ФИО; дата рождения; паспортные данные; адрес; телефон; СНИЛС; ИНН; сведения о трудовой деятельности; адрес эл. почты; файлы cookie
Категории субъектов	работники; бывшие работники; кандидаты; клиенты; посетители сайта
Правовое основание	трудовой договор; закон; согласие; договор
Перечень действий	сбор; запись; систематизация; накопление; хранение; уточнение; использование; передача; удаление; уничтожение
Способы обработки	смешанная; автоматизированная
Меры по ст. 18.1 и 19 152-ФЗ	назначен ответственный; утверждены политика и локальные акты; антивирус, межсетевой экран, разграничение доступа, резервное копирование; уровни защищённости: «1С:Зарплата и управление персоналом» — УЗ-4; «Сайт и CRM» — УЗ-4
Средства криптографической защиты	не используются
Ответственный за организацию обработки	Петров Пётр Петрович, pd@example.ru, +7 495 000-00-01
Дата начала обработки	01.01.2024
Срок или условие прекращения обработки	50 лет для кадровых документов по Закону об архивном деле; иное — до достижения цели; 3 года после последнего обращения или до отзыва согласия
Трансграничная передача	не осуществляется

Место нахождения баз данных	Российская Федерация, г. Москва, ЦОД провайдера
Информационные системы	1С:Зарплата и управление персоналом; Сайт и CRM

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____ (фамилия, имя, отчество), документ, удостоверяющий личность: _____ серия _____ № _____, выдан _____, адрес: _____,

свободно, своей волей и в своём интересе даю согласие Общество с ограниченной ответственностью «Пример» (ИНН 7700000000, ОГРН 1027700000000, адрес: 123456, г. Москва, ул. Примерная, д. 1) на обработку моих персональных данных на следующих условиях:

Цель обработки	Обработка заявок и обращений, заключение и исполнение договоров
Перечень персональных данных	ФИО; телефон; адрес эл. почты; файлы cookie
Действия с персональными данными	сбор, запись, хранение, использование, удаление, уничтожение
Способ обработки	автоматизированная
Третьи лица, которым передаются данные	нет
Срок действия согласия	3 года после последнего обращения или до отзыва согласия

Согласие может быть отозвано мной в любой момент письменным заявлением по адресу 123456, г. Москва, ул. Примерная, д. 1 или по эл. почте pd@example.ru. Мне разъяснены права субъекта персональных данных (ст. 14 Федерального закона № 152-ФЗ).

«___» _____ 20__ г. _____ / _____ /

УТВЕРЖДЕНО
приказом ООО «Пример»
от «___» _____ 20__ г. № ____

ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Общество с ограниченной ответственностью «Пример»

1. Что считается инцидентом

Неправомерная или случайная передача (предоставление, распространение, доступ) персональных данных, повлёкшая нарушение прав субъектов (ч. 3.1 ст. 21 Федерального закона № 152-ФЗ): утечка базы, отправка данных не тому адресату, взлом учётной записи, потеря носителя, публикация данных по ошибке.

2. Сроки — обязательны

Действие	Срок
Сообщить ответственному за организацию обработки ПДн	немедленно, как только инцидент обнаружен
Первичное уведомление Роскомнадзора	в течение 24 часов с момента выявления (ч. 3.1 ст. 21)
Уведомление о результатах внутреннего расследования	в течение 72 часов с момента выявления (ч. 3.1 ст. 21)
Взаимодействие с ГосСОПКА (компьютерные инциденты)	в порядке, установленном ФСБ России

3. Кто что делает

Работник, обнаруживший инцидент, сразу сообщает ответственному (Юрисконсульт Петров Пётр Петрович, pd@example.ru, +7 495 000-00-01) и не пытается устранить его самостоятельно, если это может уничтожить следы.

Ответственный фиксирует инцидент в Журнале инцидентов, оценивает, какие данные и сколько субъектов затронуто, и организует меры по прекращению утечки.

Не позднее 24 часов ответственный направляет первичное уведомление на pd.rkn.gov.ru (раздел «Инциденты») по шаблону 1 ниже.

Не позднее 72 часов — дополнительное уведомление с результатами расследования по шаблону 2.

Руководитель утверждает отчёт о расследовании и меры, исключающие повторение.

Шаблон 1. Первичное уведомление (24 часа)

Поле	Значение
Оператор	Общество с ограниченной ответственностью «Пример», ИНН 7700000000, ОГРН 1027700000000, 123456, г. Москва, ул. Примерная, д. 1
Дата и время выявления инцидента	«___» _____ 20__ г., __:__ МСК
Что произошло	_____
Предполагаемые причины	_____
Предполагаемый вред правам субъектов	_____
Категории и примерное число затронутых субъектов, перечень данных	_____
Принятые меры по устранению последствий	_____
Лицо, уполномоченное взаимодействовать с Роскомнадзором	Петров Пётр Петрович, pd@example.ru, +7 495 000-00-01

Шаблон 2. Результаты внутреннего расследования (72 часа)

Поле	Значение
Номер первичного уведомления	_____
Результаты внутреннего расследования	_____
Лица, действия которых стали причиной инцидента (при наличии)	_____
Меры, исключающие повторение	_____

Генеральный директор _____ / Иванов Иван Иванович /

УТВЕРЖДЕНО
приказом ООО «Пример»
от «___» _____ 20__ г. № ____

ПРОГРАММА ЕЖЕГОДНОГО ОБУЧЕНИЯ РАБОТНИКОВ ПРАВИЛАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общество с ограниченной ответственностью «Пример»

Обучение проходят все работники, допущенные к обработке ПДн: при приёме на работу и далее ежегодно. Проводит Юрисконсульт Петров Пётр Петрович. Продолжительность — 1 час, затем тест. Зачёт — 8 правильных ответов из 10.

Темы

1. Что такое персональные данные и какие из них обрабатывает наша организация (Реестр процессов).

2. Согласия: когда нужны, как оформляются, отзыв согласия.

3. Правила работы: доступ только по служебной необходимости, пароли, чистый стол, запрет личной почты и мессенджеров.

4. Запросы граждан: куда передавать, сроки ответа.

5. Утечка: признаки, кому сообщать немедленно, сроки уведомления Роскомнадзора (24 и 72 часа).

6. Ответственность: дисциплинарная, административная (ст. 13.11 КоАП), уголовная (ст. 137, 272.1 УК).

Тест

1. Что такое персональные данные?

а) Только паспортные данные

б) Любая информация, относящаяся к прямо или косвенно определённому лицу

в) Только данные из кадровых документов

2. Можно ли отправить список клиентов на личную почту, чтобы поработать из дома?

а) Да, если почта защищена паролем

б) Нет, только через разрешённые оператором системы

в) Да, если файл небольшой

3. Вы отправили документ с данными клиента не тому адресату. Что делать?

а) Ничего, письмо уже ушло

б) Сразу сообщить ответственному за обработку ПДн

в) Попросить адресата удалить и забыть

4. За какой срок оператор обязан первично уведомить Роскомнадзор об утечке?

а) 24 часа

б) 3 рабочих дня

в) 30 дней

5. Клиент отозвал согласие. В какой срок нужно прекратить обработку и уничтожить данные (если нет иных оснований)?

а) 1 год

б) 30 дней

в) Не нужно, согласие уже было

6. Можно ли ставить отметку «Согласен на обработку» в форме сайта заранее?

а) Да, так удобнее

б) Нет, согласие должно быть активным действием

в) Можно для постоянных клиентов

7. Где можно хранить распечатки с данными клиентов?

а) На рабочем столе

б) В запираемом шкафу или помещении с ограниченным доступом

в) Где удобно

8. Коллега из другого отдела просит выгрузку базы клиентов «для отчёта». Ваши действия?

а) Выгрузить, он же коллега

б) Передать только при наличии служебной необходимости и разрешения

в) Скинуть в мессенджер

9. Можно ли использовать пароль от рабочей системы на других сайтах?

а) Да

б) Нет

в) Только на проверенных

10. Кто отвечает за организацию обработки ПДн у нас?

а) Любой руководитель

б) Ответственный, назначенный приказом

в) Системный администратор

Ключ (для ответственного)

1-б; 2-б; 3-б; 4-а; 5-б; 6-б; 7-б; 8-б; 9-б; 10-б

Ведомость

№	**ФИО работника**	**Должность**	**Дата, результат теста**	**Подпись**
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				