



УТВЕРЖДЕНО
Генеральный директор
ООО «Гостиница «Саранск»
Дьяков В.А.
2025 г.

Положение ООО «Гостиница «Саранск» об обработке персональных данных

1. Общие положения

- 1.1. Настоящее Положение разработано во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ № 687 от 15.09.2020, Приказа Роскомнадзора № 21 от 10.02.2017 и иных нормативных правовых актов Российской Федерации, устанавливающих правила обработки персональных данных.
- 1.2. Оператор персональных данных: ООО «Гостиница «Саранск», ИНН 1326231125, ОГРН 1151326001078, юридический адрес: Республика Мордовия, г. Саранск, ул. Коммунистическая, д. 35/1.
- 1.3. Ответственный за организацию обработки персональных данных и контроль соблюдения данного Положения (далее – Ответственный): Генеральный директор Дьяков Вадим Александрович, контактный e-mail: vd.dyakov@hotelsaransk.ru, тел. +7 8342 77-00-35.
- 1.4. Настоящее Положение применяется ко всем структурным подразделениям, обособленным подразделениям и проектным группам Оператора, а также ко всем физическим лицам — сотрудникам, подрядчикам и стажёрам, имеющим доступ к персональным данным.
- 1.5. Цель Положения: установить единый подход к защите прав субъектов персональных данных, определить полномочия, обязанности и ответственность подразделений и должностных лиц за организацию обработки и защиту персональных данных.

2. Сферы и этапы обработки персональных данных

- 2.1. Сбор (запись) данных
- 2.1.1. Бумажные формы: регистрационные карты гостей, анкеты при приёме на работу, договора с контрагентами.
- 2.1.2. Электронные формы: веб-формы на сайте <https://hotelsaransk.ru/>, интерфейс системы Yclients, корпоративная сеть 1С.
- 2.1.3. Обратная связь и e-mail: письма от гостей, жалобы и отзывы, направление запросов по обработке данных.
- 2.1.4. Принцип минимизации: при заполнении форм указаны только обязательные для достижения целей обработки поля, не более 10 полей для каждого типа субъекта.

2.2. Систематизация и накопление

2.2.1. Классификация по категориям: «Сотрудники», «Гости», «Контрагенты», «Практиканты», «Посетители сайта».

2.2.2. Используемые ИСПДн:

- 1С (модули «Кадры» и «Бухгалтерия») — хранение данных сотрудников и контрагентов;
- ОТЕЛЬ 2.3 и ТРЕВЕЛЛАЙН — регистрация и проживание гостей;
- PERCo 20S — данные контроля доступа сотрудников;
- Yclients и Яндекс.Метрика — данные посетителей сайта и онлайн-бронирования;
- Видеохранилище локальной сети — записи видеонаблюдения.

2.2.3. Формирование учётных записей: каждому сотруднику и группе доступа присваиваются уникальные логин и пароль, изменяемые не реже одного раза в 90 дней.

2.3. Использование данных

2.3.1. Доступ по служебной необходимости: правило «необходимости знать» — сотрудник видит только те поля и записи, которые нужны для исполнения его должностных функций.

2.3.2. Процедуры корректировки: субъект ПДн подаёт заявление в отдел кадров или через e-mail, после чего Ответственный в течение 5 рабочих дней проверяет достоверность и вносит изменения.

2.3.3. Логирование операций: все попытки доступа, изменения, удаления фиксируются автоматизированной системой с указанием даты, времени и пользователя.

2.4. Передача и распространение

2.4.1. Внутри Оператора: передача по защищённым каналам (VPN, SSL/TLS) между подразделениями; оформление распоряжения руководителя с указанием перечня передаваемых полей.

2.4.2. Третьим лицам: только с письменного согласия субъекта или на основании договора-поручения, заверенного подписью Генерального директора и печатью.

2.4.3. Исключительные случаи: экстренная передача без согласия — по требованию правоохранительных органов или суда на основании официального документа.

2.5. Блокирование и уничтожение

2.5.1. Блокирование: при жалобе субъекта или выявлении недостоверности данных; срок блокирования не превышает 30 дней, после проверки данные либо корректируются, либо уничтожаются.

2.5.2. Уничтожение: бумажные носители уничтожаются машинным шредером, электронные — удаляются с перезаписью в соответствии со стандартом ГОСТ Р 50922-96.

2.5.3. Документальное оформление: Акт блокирования и Акт уничтожения с подписями Ответственного и специалиста ИТ-отдела, дата, причины и перечень уничтоженных полей.

3. Категории персональных данных и их источники

3.1. Сотрудники:

- Источник: документы кадрового отдела, личные анкеты, данные PERCo 20S;

– ПДн: ФИО, дата и место рождения, пол, паспортные данные, СНИЛС, ИНН, сведения о санитарной книжке, адрес регистрации, контактный телефон, e-mail, сведения о трудовой деятельности.

3.2. Контрагенты:

– Источник: договоры, реестры бухгалтерии, электронная переписка;

– ПДн: наименование организации или ФИО ИП, ИНН, ОГРН, банковские реквизиты, контактные данные уполномоченных лиц, адрес.

3.3. Гости:

– Источник: регистрационные карты, онлайн-бронирование, сторонние платформы ([Booking.com](https://www.booking.com), [Expedia](https://www.expedia.com));

– ПДн: ФИО, дата рождения, паспортные данные, контактный телефон, e-mail, сведения платёжных карт, данные о заезде/выезде.

3.4. Практиканты-студенты:

– Источник: направления вузов, анкеты стажёров;

– ПДн: ФИО, образовательное учреждение, номер студенческого билета, контактные данные, период прохождения практики.

3.5. Посетители сайта:

– Источник: cookies, логи веб-сервера, Яндекс.Метрика;

– ПДн: IP-адрес, местоположение (город), браузер, время сессии, целевые действия на сайте.

4. Правовые основания и условия обработки

4.1. Обработка на основании добровольного и информированного согласия в форме электронного или бумажного документа (ст. 24–26 ФЗ-152).

4.2. Обработка без согласия:

– выполнение обязательств по трудовому и налоговому законодательству (ст. 6 ФЗ-152);

– защита жизни, здоровья или имущества субъекта или третьих лиц;

– проведение госмониторинга, статистических или иных исследований в обезличенном виде.

4.3. Договорная обработка: данные контрагентов обрабатываются в целях исполнения договора и расчётов, основания — ст. 6 п. 1 «б» ФЗ-152.

5. Технические и организационные меры

5.1. Организационные меры:

– Утверждённые приказы о назначении Ответственного за обработку и Ответственного за безопасность ИСПДн;

– Разработанные и внедрённые инструкции для сотрудников, допущенных к ПДн;

– Обучение и проверка знаний персонала по ПДн не реже одного раза в год;

– Служебные проверки соблюдения процедур.

5.2. Технические меры:

- 5.2.1. Сегментирование сети: выделенные VLAN для ИСПДн-систем.
- 5.2.2. Аутентификация и авторизация: комплексная система паролей и смарт-карты для входа в 1С и PERCo 20S;
- 5.2.3. Шифрование: SSL/TLS для веб-форм, шифрование баз данных 1С (AES-256);
- 5.2.4. Резервное копирование: ежедневные автоматические бэкапы на NAS-сервере в защищённом ЦОДе в РФ;
- 5.2.5. Антивирусная защита: централизованное обновление сигнатур и контроль исполнения сканирования;
- 5.2.6. Межсетевые экраны и IDS/IPS: контроль входящего трафика, аномальное поведение;
- 5.2.7. Тестирование на проникновение: привлечение внешнего подрядчика для ежегодного pentest.
- 5.3. Документирование и аудит: все изменения конфигураций и регистрации доступа фиксируются в журнале ИТ-отдела; ежемесячные отчёты о состоянии безопасности.

6. Права и обязанности сторон

6.1. Права субъектов персональных данных:

- Запрашивать у Оператора информацию о своих ПДн и условиях их обработки;
- Требовать уточнения, блокирования или уничтожения ПДн;
- Отозвать согласие на обработку в любой момент;
- Обжаловать действия Оператора в органах по защите прав субъектов ПДн или в суде.

6.2. Обязанности сотрудников:

- Соблюдать нормы законодательства и локальные акты при работе с ПДн;
- Немедленно сообщать Ответственному о выявленных инцидентах или попытках несанкционированного доступа;
- Хранить логины и пароли в безопасном месте, не передавать третьим лицам.

6.3. Обязанности Оператора:

- Обеспечивать конфиденциальность, целостность и доступность ПДн;
- Рассматривать обращения субъектов не позднее 30 календарных дней;
- Сообщать Роскомнадзору о фактах утечки персональных данных в течение 72 часов с момента выявления.

7. Контроль и ответственность

7.1. Внутренний контроль:

- Проведение проверок не реже одного раза в год;
- Оформление результатов Актом внутреннего контроля с указанием выявленных нарушений и предложений по их устранению;
- Протоколирование корректирующих мероприятий и контроль их выполнения.

7.2. Внешний аудит: при необходимости – по требованию проверяющих органов или в рамках

страхования ответственности.

7.3. Ответственность:

- Сотрудники: дисциплинарная, административная и уголовная ответственность в соответствии с Трудовым кодексом РФ и Кодексом об административных правонарушениях;
- Оператор: административная ответственность по статье 13.11 КоАП РФ, возможна приостановка деятельности ИСПДн по решению суда.

8. Взаимосвязь с другими локальными актами

8.1. Политика ООО «Гостиница «Саранск» в отношении обработки персональных данных.

8.2. Приказы о назначении:

- Ответственного за обработку ПДн;
- Ответственного за безопасность ИСПДн;
- Лиц, уполномоченных на обработку и доступ к ПДн.

8.3. Инструкции:

- Ответственного за организацию обработки ПДн;
- Ответственного за обеспечение безопасности ИСПДн.

8.4. Регламенты:

- Внутреннего контроля и аудита соответствия обработок требованиям ФЗ-152;
- Резервного копирования и восстановления ПДн.

8.5. Реестры и акты:

- Реестр процессов и мест хранения ПДн;
- Реестр ИСПДн и перечень лиц с доступом;
- Акты блокирования и уничтожения ПДн.

9. Вступление в силу и изменение документа

9.1. Документ утверждается приказом Генерального директора ООО «Гостиница «Саранск» и вступает в силу с даты подписания.

9.2. Изменения и дополнения вносятся приказом на основании:

- Изменений в законодательстве РФ;
- Результатов внутреннего или внешнего аудита;
- Инцидентов информационной безопасности.