

ПЕРСОНАЛЬНЫЕ ДАННЫЕ — ОБРАБАТЫВАЙТЕ И ХРАНИТЕ БЕЗ РИСКА ПРАВОНАРУШЕНИЯ

Работу с персональными данными и обеспечение их безопасности регламентируют федеральное законодательство и внутренние документы компании.

Персональные данные — это любая информация, которая относится к конкретному человеку (субъекту персональных данных).

ФИО ▪ пол ▪ дата / место рождения ▪ адрес ▪ образование / профессия ▪ место работы ▪ электронная почта ▪ номер телефона ▪ и другие сведения

— все это персональные данные (ваши, а также других работников и клиентов компании)

СОДЕРЖАНИЕ

Кого допускают к обработке персональных данных 01

Как безопасно передавать персональные данные 02

Как хранить персональные данные 03

Как обрабатывать персональные данные в информационной системе 04

КОГО ДОПУСКАЮТ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ (01)

В должностные инструкции уполномоченных работников включают обязанности, связанные с обработкой персональных данных, а также положения об ответственности за их разглашение, нарушение требований нормативных правовых актов Российской Федерации и нормативных документов ОАО «РЖД».

Чтобы минимизировать риски, важно соблюдать порядок доступа к персональным данным:

- доступ должен быть только у работников, уполномоченных на обработку персональных данных,
- уполномоченные работники дают обязательства об их неразглашении, а также — знакомятся с нормативными правовыми актами Российской Федерации и нормативными документами ОАО «РЖД» в области персональных данных,
- список таких работников и должностные инструкции утверждает руководитель подразделения.

КАК БЕЗОПАСНО ПЕРЕДАВАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ (02)

Передавайте персональные данные в электронном виде только с применением шифрования или пароля.

! Напоминаем: нельзя собирать, хранить, передавать (пересылать) персональные данные с использованием общедоступных мессенджеров, файловых и облачных хранилищ (WhatsApp, Telegram, eXpress и других).

Отправка персональных данных без шифрования или пароля создает угрозу утечки и неправомерной обработки информации. Такие действия могут квалифицировать как административное правонарушение (часть 1 статьи 13.11 КоАП РФ).



ЧЕРЕЗ КОРПОРАТИВНУЮ ЭЛЕКТРОННУЮ ПОЧТУ



ВАРИАНТ 1

- Архивируйте пересылаемые файлы с защитой паролем (например, 7-Zip, WinRAR).
Как сделать пароль для 7-Zip:
 1. Клик по файлу правой кнопкой мыши
 2. 7-Zip Добавить к архиву
 3. Шифрование
 4. Введите пароль.
- Пароль передайте любым удобным способом: в телефонном разговоре, по SMS и т. п.
- Требования к паролю: длина не менее восьми символов, состоит из цифровых, буквенных значений и специальных символов.

ВАРИАНТ 2

- Зашифруйте пересылаемые файлы с применением сертифицированных средств криптографической защиты информации (например, КриптоПро CSP).

Подробнее о КриптоПро CSP — в Распоряжении ОАО «РЖД» от 16.03.2018 № 508/р.

ПО ЕАСД



- При отправке документа не забудьте поставить отметку «Ограниченный доступ».

КАК ХРАНИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

(03)

Персональные данные хранят на машинных (DVD и CD-диски • флеш-карты • карты памяти • внешние / внутренние жесткие диски) и бумажных носителях в помещениях из перечня, утвержденного руководителем подразделения (Приказ ОАО «РЖД» от 20.07.2016 № 60).

Для дополнительной защиты поместите съемные устройства и документы в сейф или запираемый шкаф.

МАШИННЫЕ НОСИТЕЛИ

- Использовать машинные носители для обработки персональных данных можно только после их регистрации в Журнале учета машинных носителей персональных данных.
- Если устройство необходимо отдать в ремонт или вывести из обращения, предварительно удалите с него персональные данные без возможности восстановления.
- При уничтожении устройства оставьте запись об этом в Журнале.

БУМАЖНЫЕ НОСИТЕЛИ

- Документы с персональными данными необходимо зарегистрировать в ЕАСД, ЕК АСУТР или другой системе, а хранить — в делах в соответствии с номенклатурой дел.
- Черновики можно не регистрировать, используйте их только на рабочем месте без доступа к ним третьих лиц.
- Документы уничтожают в установленном в компании порядке с составлением акта, а черновики — измельчают или уничтожают другим способом без возможности восстановления.

КАК ОБРАБАТЫВАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

(04)

Для доступа к информационной системе, в которой обрабатывают персональные данные, сначала нужно получить допуск (см. раздел 01).

Затем в АС ОЗ формируют заявку с указанием информационной системы и типом подключения.

Приложите к заявке копии приказа о назначении работника на должность и документа с его трудовыми обязанностями, в том числе — функциями по обработке персональных данных и обязательствами об их неразглашении.



После одобрения заявки вы получите логин для подключения к информационной системе.

Придумайте пароль — длина не менее восьми символов из цифровых, буквенных значений и специальных символов.



ВАЖНО:



- Размещать ПК необходимо в кабинетах, внесенных в утвержденный перечень помещений (Приказ ОАО «РЖД» от 20.07.2016 № 60).
- Экран компьютера должны видеть только вы.
- Во время перерывов в работе блокируйте экран ПК с помощью хранителя экрана.
- Убедитесь, что антивирус включен и стабильно работает.
- Не разглашайте логины и пароли для доступа к ПК и/или информационной системе третьим лицам, в том числе – другим работникам.

ОТНОСИТЕСЬ К РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ ОТВЕТСТВЕННО – ЭТО ПОМОЖЕТ ИЗБЕЖАТЬ НАРУШЕНИЙ.