

Приложение № 1

к Приказу № 217 от «02» декабря 2013г.

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ГОСУДАРСТВЕННОГО УНИТАРНОГО ПРЕДПРИЯТИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ
«СВЕРДЛОВСКОЕ ОБЛАСТНОЕ ОБЪЕДИНЕНИЕ ПАССАЖИРСКОГО ТРАНСПОРТА»

1. Общие положения.

1.1. Настоящее Положение определяет цели, задачи и основные мероприятия по обеспечению безопасности персональных данных в Государственного унитарного предприятия Свердловской области «Свердловское областное объединение пассажирского автотранспорта» (далее по тексту — Предприятие) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Положение разработано в соответствии с действующим законодательством Российской Федерации в области защиты персональных данных:

1.2.1. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

1.2.2. Постановления Правительства Российской Федерации от 15.09. 2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.2.3. Постановления Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

1.2.4. Нормативные документы уполномоченных органов.

1.3. Положение является основой для разработки локальных нормативных актов Предприятия по обеспечению безопасности ПДн.

1.4. Настоящее положение распространяется на сотрудников Предприятия, включая сотрудников, работающих по договору подряда, на сотрудников сторонних организаций, взаимодействующих с Предприятием на основании соответствующих нормативных, правовых и организационно-распорядительных документов, а также на физических лиц, находящихся в гражданско-правовых отношениях с Предприятием.

2. Термины и принятые сокращения.

Персональные данные (работников Предприятия, партнеров, пассажиров)(ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Система защиты персональных данных (СЗПД) – комплекс мер правовой, организационной и технической защиты.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), 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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных (ИСПД) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Персональные данные, сделанные общедоступными субъектом персональных данных - ПД, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Обработка персональных данных.

3.1. Получение ПД.

3.1.1. Все ПД следует получать от самого субъекта. Если ПД субъекта можно получить только у третьей стороны, то Субъект должен быть уведомлен об этом или от него должно быть получено согласие.

3.1.2. Оператор должен сообщить Субъекту о целях, предполагаемых источниках и способах получения ПД, перечне действий с ПД, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа Субъекта дать письменное согласие на их получение.

3.1.3. Документы, содержащие ПД (паспорт, удостоверение личности, военный билет, документ об образовании, свидетельство ИНН, удостоверение о праве на льготы, пенсионное удостоверение, справка МСЭ и др.) создаются путем:

- копирования оригиналов документов;
- внесения сведений в учетные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

3.2. Обработка ПД.

3.2.1. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

2.Цели обработки ПД:

- осуществление трудовых отношений;
- оформление проездных документов, в соответствии с законодательством РФ и/или субъекта РФ для проезда в автобусах;
- ведение учета поездок граждан, в соответствии с законодательством РФ и/или

субъекта РФ;

- осуществление гражданско-правовых отношений;
- оформление ответов на запросы уполномоченных органов;

3.2.3. Категории субъектов персональных данных:

- физические лица, состоящие в трудовых взаимоотношениях с ГУП СО «СООПА»;
- близкие родственники лиц, состоящих в трудовых взаимоотношениях с ГУП СО «СООПА»;
- физические лица, претенденты на замещение вакантной должности;
- физические лица - практиканты/стажеры;
- физические лица, и их законные представители, состоящие в гражданско-правовых взаимоотношениях с ГУП СО «СООПА»;
- физические лица, и их законные представители – пассажиры.

3.2.4. ПД, обрабатываемые Предприятием:

- данные полученные при осуществлении трудовых отношений;
- данные полученные для осуществления отбора кандидатов на работу;
- данные полученные при осуществлении гражданско-правовых отношений;
- данные полученные при оформлении проездных документов.

Полный список ПД представлен в Перечне ПД, утвержденном руководителем Предприятия.

3.2.5. Обработка персональных данных ведется:

- с использованием средств автоматизации с передачей по внутренней сети Предприятия с разграничением доступа, без передачи по сети Интернет;
- с использованием средств автоматизации с передачей по защищенному каналу сети Интернет.

•без использования средств автоматизации.

3.3. Хранение ПД.

3.3.1. ПД субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

3.3.2. ПД субъектов, зафиксированные на бумажных носителях хранятся в запираемых шкафах.

3.3.3. ПД субъектов, обрабатываемые с использованием средств автоматизации для различных целей, хранятся в разных базах данных (папках, вкладках).

3.3.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках).

3.3.5. Хранение ПД в форме, позволяющей определить субъекта ПД, осуществляется не дольше, чем этого требуют цели их обработки и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Срок хранения ПД представлен в Перечне ПД, утвержденном руководителем Предприятия.

3.4. Уничтожение ПД

3.4.1. Уничтожение документов (носителей), содержащих ПД производится путем сожжения, дробления (измельчения). Для уничтожения бумажных документов допускается применение шредера.

3.4.2. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

3.4.3. Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

3.5. Передача ПД.

3.5.1. Предприятие осуществляет передачу ПД третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры;
- передача предусмотрена гражданско-правовыми взаимоотношениями.

3.5.2. Перечень лиц, которым передаются ПД.

Третьи лица, которым передаются ПД:

- Пенсионный фонд РФ для учета (на законных основаниях);
- налоговые органы РФ (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- перевозчики (юридические лица и индивидуальные предприниматели) (на основании договора);
- юридические и коллекторские фирмы, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта).

3.5.3. Методы передачи ПД третьим лицам:

- с использованием средств автоматизации с передачей по защищенному каналу сети Интернет;
- без использования средств автоматизации – информация с содержанием ПД на бумажных носителях и/или на флэш-картах (дисках) передается в закрытом (запечатанном, упакованном) виде потребителю (инспектору, перевозчику и др.) и/или его представителю с обязательной регистрацией в Журнале передачи корреспонденции под роспись.

4. Защита персональных данных.

4.1. В соответствии с требованиями нормативных документов в Предприятии создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

4.2. Подсистема правовой защиты представляет собой комплекс правовых,

организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

4.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами.

4.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.

4.5. Основными мерами защиты ПД, используемыми Предприятием, являются:

4.5.1. Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением Предприятием и его работниками требований к защите ПД;

4.5.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД, и разработка мер и мероприятий по защите ПД;

4.5.3. разработка локальных нормативных актов в отношении обработки персональных данных;

4.5.4. Установление правил доступа к ПД, обрабатываемым в ИСПД.

4.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их должностными обязанностями;

4.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

4.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;

4.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;

4.5.10. Соблюдаются условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ;

4.5.11. Обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

4.5.12. Восстановление ПД, модифицированных или уничтоженных вследствие

несанкционированного доступа к ним;

4.5.13. Обучение работников Предприятия, непосредственно осуществляющих обработку персональных данных, в рамках требований законодательства Российской Федерации в части защиты персональных данных, в том числе документам, определяющими политику Предприятия в отношении обработки персональных данных, локальным нормативным актам по вопросам обработки персональных данных;

4.5.14. Осуществление внутреннего контроля и аудита.

5. Основные права субъекта ПД и обязанности оператора.

5.1. Основные права субъекта ПД:

5.1.1 Субъект персональных данных имеет право требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.1.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

5.1.3 Обращения к оператору и направлению ему запросов;

5.1.4 Обжалование действий или бездействия оператора.

5.2. Обязанности Оператора:

Оператор обязан:

- при сборе персональных данных предоставить субъекту персональных данных по его просьбе информацию о полученных ПД,
- в случаях если ПД были получены не от субъекта ПД, уведомить субъекта персональных данных;
- в случае отказа субъекта ПД в предоставлении ПД субъекту разъясняются юридические последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД а также от иных неправомерных действий в отношении ПД;
- давать ответы на запросы и обращения Субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.