Утверждаю
Заведующий МБДОУ
«ЦРР – д/с №34 «Рябинушка»
_____ А.В. Почернина
«01» 09 2016г.

Разрешительная система доступа к персональным данным,
содержащимся в базах данных
Муниципального бюджетного дошкольного образовательного учреждения
«Центр развития ребенка – детский сад №34 «Рябинушка» муниципального
образования город-курорт Геленджик

г-к. Геленджик, 2016г.

Содержание

1. Общие положения

Настоящее Положение устанавливает правила доступа сотрудников МБДОУ «ЦРР – д/с №34 «Рябинушка» (далее - ДОУ) и сторонних организаций к персональным данным, содержащимся в базах данных (далее – персональные данные).

В настоящем Положении используются следующие основные понятия:

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

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 (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания (в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»).

Информационные ресурсы ОУ, содержащие персональные данные – отдельные документы и массивы документов, а также документы и массивы документов в информационных системах (банках данных, архивах), доступ к которым ограничен в соответствии с действующим законодательством и локальными нормативными документами ОУ, и которые содержат персональные данные.

Доступ пользователя к информационным ресурсам – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

2. Порядок предоставления доступа

Предоставление доступа сотрудникам к любым информационным ресурсам должно осуществляться только на основании заявок, оформленных в соответствии с данным документом (Приложение 1).
Перед предоставлением сотруднику доступа к информационным ресурсам ДОУ, содержащим персональные данные, необходимо:
1. Отразить в трудовом договоре с сотрудником обязательства о неразглашении персональных данных, которые будут ему известны при исполнении служебных обязанностей, и о соблюдении требований локальных нормативных актов ДОУ, регулирующих порядок обращения с персональными данными.
2. Ознакомить сотрудника под подпись со следующими документами:
- Перечень персональных данных ДОУ;
- Инструкция по обеспечению безопасности обрабатываемых персональных данных;
- Инструкции пользователей информационных систем персональных данных (для всех ИСПДн, используемых в ДОУ).

На основании решения заведующего ДОУ (в случае необходимости) и руководителей структурных подразделений (подразделения работника и подразделения, располагающего ресурсами, к которым необходим допуск) осуществляется допуск пользователя к персональным данным, в объеме, необходимом для выполнения им своих функциональных обязанностей.
При переводе на другую должность основанием для допуска служит приказ о переводе. В этом случае допуск работника по предыдущей должности прекращается, и он допускается к сведениям по новой должности.
Перечень персональных данных ДОУ необходимо держать в актуальном состоянии.

3. Порядок получения разрешения на предоставление доступа

Предоставление пользователям доступа к персональным данным ДОУ осуществляется следующим образом:
а) заявка на предоставление доступа к ресурсу, подписанная начальником подразделения, направляется ответственному за этот ресурс лицу;
б) подписанная ответственным за ресурс лицом заявка согласовывается с администратором информационной безопасности и направляется системному администратору для предоставления доступа пользователю к запрашиваемому ресурсу.

Срок рассмотрения заявки на предоставление доступа пользователей к информационным ресурсам ДОУ каждым из причастных подразделений не должен превышать одного рабочего дня.

4. Порядок прекращения доступа

Прекращение предоставления доступа пользователям к персональным данным ДОУ осуществляется следующим образом:
а) в случае увольнения (перевода на другую должность) сотрудника заявка на отключение доступа к ресурсу, подписанная начальником подразделения, направляется ответственному за этот ресурс лицу;
б) подписанная ответственным за ресурс лицом заявка направляется системному администратору и администратору информационной безопасности для отключения доступа пользователя к ресурсу.
В случае компрометации аутентификационных данных пользователя начальник подразделения извещает в письменном виде администратора информационной безопасности о факте компрометации. Администратор информационной безопасности должен уведомить в письменном виде ответственного за ресурс и лицо, выполняющее функции системного администратора, о необходимости отключения доступа пользователя к ресурсу и инициировать служебное расследование в соответствии с \4\.

5. Контроль доступа к информационным ресурсам

Контроль правомерности предоставления доступа пользователей к информационным ресурсам возлагается на администратора информационной безопасности в соответствии с \5\.

6. Ответственность

Сотрудники ДОУ, допущенные к работе с персональными данными, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность за разглашение персональных данных в соответствии с законодательством Российской Федерации, а также материальную ответственность за нарушение установленных в ДОУ требований по защите персональных данных.

7. Перечень нормативных документов, использованных при разработке данного порядка

1. Перечень защищаемой информации в ДОУ;
2. Инструкция пользователя ИСПДн.
3. Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности (Инструкция пользователя ИСПДн на случай возникновения внештатных ситуаций).
4. Инструкция администратора ИБ.

Приложение 1

Заявка на доступ к информационным ресурсам

Наименование информационного ресурса	
ФИО сотрудника, получающего доступ	
Права	
Основание получения доступа	

Подпись руководителя структурного подразделения сотрудника, запрашивающего доступ:

_____ _____ _____

(должность) (подпись) (ФИО)

Согласовано:

Администратор информационной безопасности _____ _____

(подпись) (ФИО)

Доступ предоставлен:

Администратор ИСПДн

_____ _____ _____

(название ИСПДн) (подпись) (ФИО)

Отметка об ознакомлении пользователя с нормативными документами по информационной безопасности:

- Перечень персональных данных ОУ;
- Положение о порядке организации и проведения работ по защите персональных данных ОУ;
- Инструкция пользователя ИСПДн _____.

(название ИСПДн)

Дата	Подпись