



Разрешительная система доступа к персональным данным,  
содержащимся в базах данных ОГБУ «РЦРО»

Томск 2015

## Содержание

1. Общие положения.....	3
2. Порядок получения доступа.....	3
3. Порядок получения разрешения на предоставление доступа.....	3
4. Порядок прекращения доступа.....	3
5. Контроль доступа к информационным ресурсам.....	3
6.Ответственность.....	3
7. Перечень нормативных документов, использованный при разработке данного порядка.....	3
8. Приложение 1.....	4

## **1. Общие положения**

Настоящее Положение устанавливает правила доступа сотрудников ОГБУ «РЦРО» 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 ОГБУ «РЦРО», 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 ОГБУ «РЦРО», 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 ОГБУ «РЦРО», 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 ОГБУ «РЦРО», регулирующих порядок обращения с персональными данными.
2. Ознакомить сотрудника под подпись со следующими документами:
  - Перечень персональных данных ОГБУ «РЦРО»;
  - Инструкция по обеспечению безопасности обрабатываемых персональных данных;
  - Инструкции пользователей информационных систем персональных данных (для всех ИСПДн, используемых в ОГБУ «РЦРО»).

На основании решения директора ОГБУ «РЦРО» (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 ОГБУ «РЦРО» необходимо держать в актуальном состоянии.

### **3. Порядок получения разрешения на предоставление доступа**

Предоставление пользователям доступа к персональным данным ОГБУ «РЦРО» 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 ОГБУ «РЦРО» каждым из причастных подразделений не должен превышать одного рабочего дня.

### **4. Порядок прекращения доступа**

Прекращение предоставления доступа пользователям к персональным данным ОГБУ «РЦРО» 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 п. 4.

### **5. Контроль доступа к информационным ресурсам**

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

### **6. Ответственность**

Сотрудники ОГБУ «РЦРО», 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 ОГБУ «РЦРО» требований по защите персональных данных.

### **7. Перечень нормативных документов, использованных при разработке данного порядка**

1. Перечень защищаемой информации в ОГБУ «РЦРО»;
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.

## Заявка на доступ к информационным ресурсам

<b>Наименование информационного ресурса</b>	
<b>ФИО сотрудника, получающего доступ</b>	
<b>Права</b>	
<b>Основание получения доступа</b>	

Подпись руководителя структурного подразделения сотрудника, запрашивающего доступ:

\_\_\_\_\_ (должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (ФИО)

**Согласовано:**  
Администратор  
информационной безопасности \_\_\_\_\_ (подпись) \_\_\_\_\_ (ФИО)

**Доступ предоставлен:**  
Администратор ИСПДн \_\_\_\_\_ (подпись) \_\_\_\_\_ (ФИО)

\_\_\_\_\_ (название ИСПДн) \_\_\_\_\_ (подпись) \_\_\_\_\_ (ФИО)

**Отметка об ознакомлении пользователя с нормативными документами по  
информационной безопасности:**

- Перечень персональных данных ОГБУ «РЦРО»;
- Положение о порядке организации и проведения работ по защите персональных данных ОГБУ «РЦРО»;
- Инструкция пользователя ИСПДн

ИСПДн	Дата	Подпись