



## Защита персональных данных в Библиотеке

В соответствии со ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» субъектом персональных данных является физическое лицо, а персональными данными — любая информация, прямо или косвенно его индивидуализирующая.

Все организации осуществляющие обработку персональных данных должны быть зарегистрированы как операторы. Библиотеки обрабатывают персональные данные пользователей, посетителей (не записанные в библиотеку лица) и сотрудников. На оператора персональных данных субъекта возлагается обязанность по их защите (ч. 1 ст. 19 Закона о персональных данных).

**В качестве мер защиты ч. 2 ст. 19 Закона о персональных данных предусмотрено:**

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

**Помимо этого, оператор должен:**

- назначить ответственного за организацию обработки персональных данных;

- издать документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;
- осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- производить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Законом;
- знакомить своих работников, непосредственно осуществляющих обработку персональных данных, с положениями российского законодательства о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников (ст. 18.1 Закона о персональных данных).

**Специальные требования к защите персональных данных установлены также:**

- главой 14 Трудового кодекса РФ;
- Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

**Необходимо отметить ответственность оператора за нарушение законодательства о персональных данных:**

Статьи о неразглашении персональных данных, по которым нарушители могут привлекаться к ответственности, предусмотрены в различных федеральных законах. Рассмотрим их:

**1. Вид ответственности:**

Дисциплинарная (ст. 192 ТК РФ)

**Условия применения и/или санкция:**

Работодатель вправе применить следующие виды взысканий:

- замечание;
- выговор;
- увольнение.

**2. Вид ответственности:**

Материальная (ст. 232, 233 ТК РФ)

**Условия применения и/или санкция:**

Наступает, если в результате разглашения работником персональных данных работодателю причинен материальный ущерб, при условии что соглашением, заключенным между работником и работодателем, предусмотрено привлечение к такому виду ответственности

**3. Вид ответственности:**

Гражданко-правовая (п. 2 ст. 24 закона «О персональных...» от 27.07.2006 № 152-ФЗ, ст. 151 ГК РФ)

**Условия применения и/или санкция:**

Возмещение морального вреда, причиненного потерпевшему лицу

**4. Вид ответственности:**

Административная (ст. 13.14 КоАП РФ)

**Условия применения и/или санкция:**

Наложение административного штрафа в размере:

- от 500 руб. до 1 тыс. руб. — на граждан;
- 4–5 тыс. руб. — на должностных лиц

**5. Вид ответственности:**

Уголовная (ст. 137 УК РФ)

**Условия применения и/или санкция:**

Возникает, если лицо, получившее доступ к персональным данным, распространило их в СМИ или в публичном информационном пространстве. Предусмотрены различные виды наказаний — от штрафа до реального лишения свободы.

**И подробнее из «Кодекса Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 02.08.2019):**

Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных

(в ред. Федерального закона от 07.02.2017 N 13-ФЗ)

1. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи, если эти действия не содержат уголовно наказуемого деяния, —

влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей; на должностных лиц — от пяти тысяч до десяти тысяч рублей; на юридических лиц — от тридцати тысяч до пятидесяти тысяч рублей.

2. Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, —

влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц — от десяти тысяч до двадцати тысяч рублей; на юридических лиц — от пятнадцати тысяч до семидесяти пяти тысяч рублей.

3. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных —

влечет предупреждение или наложение административного штрафа на граждан в размере от семисот до одной тысячи пятьсот рублей; на должностных лиц — от трех тысяч до шести тысяч рублей; на индивидуальных предпринимателей — от пяти тысяч до десяти тысяч рублей; на юридических лиц — от пятнадцати тысяч до тридцати тысяч рублей.

4. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, —

влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц — от четырех тысяч до шести тысяч рублей; на индивидуальных предпринимателей — от десяти тысяч до пятнадцати тысяч рублей; на юридических лиц — от двадцати тысяч до сорока тысяч рублей.

5. Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, —

влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц — от четырех тысяч до десяти тысяч рублей; на индивидуальных предпринимателей — от десяти тысяч до двадцати тысяч рублей; на юридических лиц — от двадцати пяти тысяч до сорока пяти тысяч рублей.

6. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и

исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния — влечет наложение административного штрафа на граждан в размере от семисот до двух тысяч рублей; на должностных лиц — от четырех тысяч до десяти тысяч рублей; на индивидуальных предпринимателей — от десяти тысяч до двадцати тысяч рублей; на юридических лиц — от двадцати пяти тысяч до пятидесяти тысяч рублей.

7. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных — влечет предупреждение или наложение административного штрафа на должностных лиц в размере от трех тысяч до шести тысяч рублей.

В данной консультации представляем Вам часть обязательного пакета документов библиотеки с шаблонами, разработанного и обновленного согласно нормативно-правовым актам РФ на 30.10.2019. За основу данной консультации взят «Примерный перечень документов, которые должен иметь оператор персональных данных во исполнение требований законодательства в области персональных данных» по версии [сайта Роскомнадзора](#) на 20.07.2017.

Документы из этого списка должны быть у всех в обязательном порядке, именно их первыми и запрашивают проверяющие органы. Обращаем внимание, что большая часть задач по защите персональных данных, представленных в перечне решена при формировании [«Политики обработки и защиты персональных данных ...библиотеки...»](#) и [Приказа «О мерах защиты персональных данных субъектов»](#).

В перечне Роскомнадзора 16 пунктов для проверки документов. В данной консультации 15, объединены в один пункты о наличии согласия субъекта персональных данных, т.к. оно необходимо только в письменной форме. В консультации даны как требования нормативно-правовых актов, так и шаблоны и примеры документов по каждому пункту. Часть документов находится в разработке. По окончании они также будут представлены здесь. В завершении настоящего материала представляется возможность скачать все файлы одним архивом, в котором шаблоны документов представлены в формате docx.

Идем по порядку:

## 1. Уведомление об обработке персональных данных

**Требование нормативного правового акта**

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

## Статья 22. Уведомление об обработке персональных данных

ч. 1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

Заполняется на [сайте Роскомнадзора](#), распечатывается сразу из браузера и подается в местный орган Роскомнадзора.

## 2. Изменения в уведомление об обработке персональных данных

## **Требование нормативного правового акта**

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

### **Статья 22. Уведомление об обработке персональных данных**

ч. 7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

### **Статья 25. Заключительные положения**

ч. 2\_1. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в пунктах 5, 7\_1, 10 и 11 части 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2013 года.

Заполняется на [сайте Роскомнадзора](#), распечатывается сразу из браузера и подается в местный орган Роскомнадзора.

### **3. Приказ (распоряжение) о назначении ответственного за организацию обработки персональных данных у оператора**

#### **Требование нормативного правового акта**

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

### **Статья 22\_1. Лица, ответственные за организацию обработки персональных данных в организациях**

ч. 1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

[Шаблон приказа \(Пункт 7 Приказа «О мерах защиты персональных данных субъектов»\)](#)

### **4. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных**

#### **Требование нормативного правового акта**

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

### **Статья 9. Согласие субъекта персональных данных на обработку его персональных данных**

ч. 1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

ч. 4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

Согласие пользователя включено в договор на библиотечное обслуживание (Приложения 2 и 3 к «Политике обработки и защиты персональных данных ...библиотеки...» )

Шаблон Согласия сотрудника библиотеки (Приложение 4 к «Политике обработки и защиты персональных данных ...библиотеки...» )

5. Документы, подтверждающие предоставление субъекту персональных данных определенной Федеральным Законом «О персональных данных» информации, в случае если персональные данные получены не от субъекта персональных данных

**Требование нормативного правового акта**

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Статья 18. Обязанности оператора при сборе персональных данных

ч. 3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- 1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные настоящим Федеральным законом права субъекта персональных данных;
- 5) источник получения персональных данных.

Пункт 5.1.4 «Политики обработки и защиты персональных данных ...библиотеки...»

6. Документы, определяющие политику оператора в отношении обработки персональных данных

**Требование нормативного правового акта**

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Статья 18\_1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

ч. 1 п. 2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

- 1) Пункт 1 и пункт 19 Приказа «О мерах защиты персональных данных субъектов»
- 2) Приложение 1 к Приказу «Политика обработки и защиты персональных данных ...библиотеки...»

Рекомендации:

Внимание! Необходимо выполнить требование ч. 2 ст. 18\_1 132-ФЗ опубликовать или иным образом обеспечить неограниченный доступ к документу.

## 7. Документы, содержащие положения о принятии оператором ПД правовых, организационных и технических мер для защиты персональных данных

### Требование нормативного правового акта

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке.

ч. 1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

- 1) Приказ «О мерах защиты персональных данных субъектов»
- 2) «Политика обработки и защиты персональных данных ...Библиотеки...»

### 3) Анализ защищенности.

### 4) План мер по защите персональных данных

5) Дополнения в должностные инструкции персонала библиотеки

Рекомендации:

С целью принятия мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ, работники оператора, непосредственно осуществляющие обработку персональных данных, **должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и (или) должны быть обучены** (п. 6 ч. 1 ст. 18\_1).

## 8. Документы по организации приема и обработке обращений и запросов субъектов персональных данных

### Требование нормативного правового акта

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Статья 22\_1. Лица, ответственные за организацию обработки персональных данных в организациях.

ч. 4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

п. 3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

- 1) Пункт 28 Приказа «О мерах защиты персональных данных субъектов»

- 2) Приложение 8-14 к «Политике обработки и защиты персональных данных ...Библиотеки...»

9. Документы, определяющие категории обрабатываемых персональных данных, особенности и правила их обработки без использования средств автоматизации

**Требование нормативного правового акта**

ПОЛОЖЕНИЕ об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации УТВЕРЖДЕНО постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

п. 6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки

- 1) Ознакомительные листы к Приказу «О мерах защиты персональных данных субъектов»
- 2) ЖУРНАЛ прохождения инструктажа работниками, допускаемыми к работе с персональными данными
- 3) Раздел 4 «Политики обработки и защиты персональных данных ...библиотеки...»

**10. Типовые формы документов**

**Требование нормативного правового акта**

ПОЛОЖЕНИЕ об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации УТВЕРЖДЕНО постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

п. 7. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее — типовая форма), должны соблюдаться определенные условия.

Приложения к «Политике обработки и защиты персональных данных ...библиотеки...»

Рекомендации:

Здесь необходимо утвердить все формы с персональными данными негосударственного образца, которые используются в библиотеке. В настоящем примере даны договоры с читателями.

**11. Документ, устанавливающий требования к ведению журналов (реестров, книг ...), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию**

**Требование нормативного правового акта**

ПОЛОЖЕНИЕ об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации УТВЕРЖДЕНО постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

п. 8. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться определенные условия.

«Положение о пропускном и внутриобъектовом режиме».

Данный документ должен быть в библиотеке для обеспечения безопасности и разработан ранее вне данного пакета документа.

## 12. Документ, устанавливающий требования к хранению материальных носителей содержащих персональные данные

### Требование нормативного правового акта

ПОЛОЖЕНИЕ об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации УТВЕРЖДЕНО постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687.

п. 15. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

- 1) Приказ об утверждении мест хранения носителей персональных данных с приложениями;
- 2) Перечень помещений, в которых ведется обработка персональных данных;
- 3) Порядок доступа сотрудников ...Библиотеки... в помещения, в которых ведется обработка или хранение персональных данных

*Требуемые документы в разработке.*

## 13. Документ о классификации информационных систем

### Требование нормативного правового акта

Порядок проведения классификации информационных систем персональных данных.

Утвержденный приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20.

п. 18. Результаты классификации информационных систем оформляются соответствующим актом оператора

В настоящее время данный документ ФСТЭК отменен. Требуется определение уровня защищенности персональных данных.

## 14. Список лиц, которым необходим доступ к персональным данным, обрабатываемым в информационной системе, утвержденный оператором или уполномоченным лицом

### Требование нормативного правового акта

ПОЛОЖЕНИЕ об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных УТВЕРЖДЕНО постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781.

п. 14. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

Приказ о допуске к обработке персональных данных

15. Документ, устанавливающий порядок обработки персональных данных работников

**Требование нормативного правового акта**

ТРУДОВОЙ КОДЕКС РФ от 30 декабря 2001 года № 197-ФЗ

Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты:

п. 8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Статья 87. Хранение и использование персональных данных работников;

Статья 88. Передача персональных данных работников.

Приложение 1 к Приказу «Политика обработки и защиты персональных данных ...библиотеки...»

Рекомендации:

Рекомендуется здесь разработать отдельное «Положение об обработке персональных данных». Мы предлагаем сначала выполнить все обязательные требования, а уж потом детализировать и пока эти функции возложить на «Политика обработки и защиты персональных данных ...библиотеки...».