

## **Законодательство по теме персональных (в т.ч. биометрических) данных**

- Конституция Российской Федерации
- ФЗ\_152\_27.07.2006\_О персональных данных (ред.2021)
- ФЗ\_149\_27.07.2006\_Об информации, информационных технологиях и о защите информации (ред. 2021)
- ГОСТ\_58833-2020\_Защита информации ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ
- Письмо МинЦР 17.07.2020№ ОП-П24-070-19433  
Разъяснения Министерства цифрового развития, связи и массовых коммуникаций РФ о некоторых нормах Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных"
- Приказ МинЦР N930\_10.09.21\_Об утверждении порядка обработки биометрических персональных данных ..... в единой биометрической системе и иных информационных системах, обеспечивающих идентификацию и аутентификацию с использованием биометрических персональных данных .....
- ПостПравРФ\_1799\_20.10.21\_ Об аккредитации организаций, владеющих информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающих услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц"

### **Статья 24 Конституции Российской Федерации**

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Решения для защиты персональных данных в российских компаниях и учреждениях формируются на базе мер организационно-технического характера. Они должны соответствовать нормам правовых актов: Конституции Российской Федерации (статья 24), Федерального закона №152-ФЗ «О персональных данных» и специальным требованиям регуляторов. Функции регуляторов выполняют:

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор;

Федеральная служба по техническому и экспортному контролю – ФСТЭК;

Федеральная служба безопасности – ФСБ.

## **Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"**

### **СТАТЬЯ 3. ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ФЗ**

1) **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

1\_1) персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом; (Пункт дополнительно включен с 1 марта 2021 года Федеральным законом от 30 декабря 2020 года N 519-ФЗ)

2) **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами 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;

3) **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;

### **СТАТЬЯ 6. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

.....

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона

### **СТАТЬЯ 8. ОБЩЕДОСТУПНЫЕ ИСТОЧНИКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных

### **СТАТЬЯ 10. СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частями 2 и 2\_1 настоящей статьи

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

.....

## **СТАТЬЯ 11. БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**

1. Сведения, которые характеризуют физиологические и биологические особенности человека, **на основании которых можно установить его личность** (биометрические персональные данные) и которые **используются оператором для установления личности** субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных **может осуществляться без согласия** субъекта персональных данных в связи с реализацией **международных договоров** Российской Федерации **о реадмиссии**, в связи с осуществлением **правосудия** и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации **об обороне, о безопасности, о противодействии терроризму**, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

## **СТАТЬЯ 9. СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБРАБОТКУ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и **даёт согласие на их обработку свободно, своей волей и в своем интересе**. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. ....

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется **только с согласия в письменной форме** субъекта персональных данных. равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме **на бумажном носителе** признается согласие в форме **электронного документа**, подписанного в соответствии с федеральным законом **электронной подписью**.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

- 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- 3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- 4) цель обработки персональных данных;
- 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- 8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- 9) подпись субъекта персональных данных.

## **СТАТЬЯ 10\_1. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, РАЗРЕШЕННЫХ СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ РАСПРОСТРАНЕНИЯ**

1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, **оформляется отдельно от иных согласий** субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

**биометрические персональные данные:** сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

**аутентификация:** Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

#### 6 Основы аутентификации

6.1 Процесс аутентификации при доступе субъекта доступа к объекту доступа должен включать в себя действия по проверке подлинности субъекта доступа, а также принадлежности субъекту доступа предъявленного идентификатора и аутентификационной информации.

**идентификация:** Действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

#### 5 Основы идентификации

5.1 Процесс идентификации должен включать в себя действия по подготовке, формированию идентификационной информации субъекта (объекта) доступа, присвоению субъекту (объекту) доступа идентификатора и их последующей регистрации, а при доступе субъекта доступа к объекту доступа — действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа, в перечне присвоенных идентификаторов.

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

#### СТАТЬЯ 22. УВЕДОМЛЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

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.

2. Оператор вправе осуществлять **без уведомления** уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с **трудовым законодательством**;

2) полученных оператором в связи с **заключением договора**, стороной которого является субъект персональных данных, **если** персональные данные **не распространяются**, а также **не предоставляются третьим лицам** без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

.....

5) включающих в себя **только фамилии, имена и отчества** субъектов персональных данных;

6) необходимых **в целях однократного пропуска** субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

\*\*\*\*\*

**Приказ МинЦР N930\_10.09.21\_Об утверждении порядка обработки биометрических персональных данных** ..... в единой биометрической системе и иных информационных системах, обеспечивающих идентификацию и аутентификацию с использованием биометрических персональных данных .....

**ПостПравРФ\_1799\_20.10.21\_Об аккредитации организаций, владеющих информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающих услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц"**

**Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»**

**Аннотация кратко:**

*В Закон о персональных данных вносились многочисленные изменения. В связи с этим пересмотрены требования по защите этих данных при их обработке в соответствующих информационных системах.*

*Система защиты персональных данных призвана нейтрализовывать актуальные угрозы их безопасности. Она включает в себя организационные и (или) технические меры.*

*Последние зависят от установленного уровня защищенности персональных данных. Он определяется исходя из типа угроз (приведена их классификация), вида персональных данных (биометрические, общедоступные и пр.), количества их субъектов и прочих факторов.*

*За безопасность персональных данных отвечает оператор системы, который их обрабатывает, или уполномоченное им лицо. Оператор системы выбирает средства защиты информации в соответствии с нормативными актами ФСБ России и ФСТЭК России.*

*Выполнение требований контролируется оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юрлиц и ИП. Последние должны иметь лицензию на занятие деятельностью по технической защите конфиденциальной информации. Контроль проводится не реже 1 раза в 3 года.*

**3. Безопасность** персональных данных при их обработке в информационной системе **обеспечивает оператор** этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора. ....

**4. Выбор средств** защиты информации для системы защиты персональных данных **осуществляется оператором** в соответствии с нормативными правовыми актами, принятыми ФСБ РФ и ФСТЭК во исполнение части 4 статьи 19 ФЗ "О персональных данных".

\*\*\*\*\*

Меры, которые помогают предотвратить несанкционированный доступ, усилить надежность и отказоустойчивость ИСПДн, сохранить целостность и доступность информации внутри системы, перечислены в 152-ФЗ.

Закон предписывает:

1. Определить масштаб информационной системы и категорию ПДн, смоделировать угрозы безопасности.

2. Внедрить организационно-технические механизмы безопасности в соответствии с четырьмя уровнями защищенности. Определение уровней содержится в постановлении правительства №1119.

3. Использовать средства информационной защиты, возможности которых подтверждены сертификатами соответствия ФСТЭК и/или ФСБ.

4. Провести до начала обработки ПДн комплексный аудит безопасности, включая аудит информационной системы, компонентов защиты, исполнения требований внутренних организационных и методических распоряжений.

5. Внедрить систему учета всех видов носителей информации ограниченного использования, в том числе ПДн.

6. Заложить в информационной системе функции резервирования и восстановления ПДн в случае несанкционированных изменений или уничтожения.

7. Установить регламент доступа сотрудников оператора к персональным данным в ИС. Уровни доступа должны сегментироваться в зависимости от должностных обязанностей.

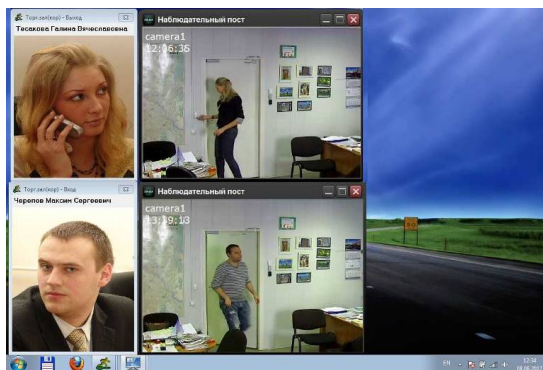
8. Внедрить инструменты аудита и журналирования действий сотрудников с персональными данными.

9. Контролировать исполнение правил безопасности эксплуатации персональных данных и непрерывность работы защитных аппаратно-программных сервисов ИСПДн.

## Письмо МинЦР 17.07.2020№ ОП-П24-070-19433

Разъяснения Министерства цифрового развития, связи и массовых коммуникаций РФ о некоторых нормах Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных"

**Фотографические изображения** посетителей организации, содержащиеся в системе контроля управления доступа(СКУД), будут являться биометрическими персональными данными, поскольку они характеризуют физиологические и биологические особенности человека, позволяют установить, принадлежит ли данному лицу предъявляемый СКУД пропуск, на основе которого можно установить его личность путем сравнения фото с лицом предъявителя пропуска и указываемых владельцем пропуска фамилии, имени и отчества с указанными в СКУД.



Таким образом, фотографическое изображение и иные сведения, используемые для обеспечения однократного и/или многократного прохода на охраняемую территорию и установления личности гражданина, также относятся к биометрическим персональным данным.

В качестве одного из оснований обработки биометрических персональных данных установлено **наличие согласия в письменной форме** субъекта персональных данных.

\*\*\*\*\*

Таким образом, обработка **биометрических персональных данных учащихся** с согласия в письменной форме законного представителя субъекта персональных данных на обработку его биометрических персональных данных **не допускается**, за исключением случаев, предусмотренных ч.2 ст.11 Закона о персональных данных



Таким образом, законодательством Российской Федерации в области персональных данных **порядок и условия обработки биометрических персональных данных несовершеннолетних лиц не предусмотрены**, что исключает наличие оснований для осуществления такой обработки образовательными учреждениями.

В этой связи в случае осуществления образовательными учреждениями обработки биометрических персональных данных несовершеннолетних лиц, необходимо **принять меры по прекращению** обработки биометрических персональных данных учащихся (несовершеннолетних) **и их уничтожению** (при наличии базы данных).