УТВЕРЖДЕНО

Приказом № 1 – П от «28» ноября 2019г.

Исполнительный директор Карасева В.В.

# ПОЛОЖЕНИЕ об обработке персональных данных в Общероссийской общественной организации «Российское общество клинической онкологии»

Москва

Содержание

1. Область применения ..... 3
2. Нормативные ссылки ..... 4
3. Термины, определения, обозначения и сокращения ..... 5
4. Общие положения ..... 7
5. Политика организации в отношении обработки персональных данных ..... 8
6. Обрабатываемые персональные данные ..... 9
7. Правила обработки персональных данных ..... 10
8. Ознакомление работников с правилами обработки персональных данных ..... 12
9. Ответственность ..... 13

# 1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. В настоящем Положении об обработке персональных данных в Общероссийской общественной организации «Российское общество клинической онкологии» (далее - Положение) установлены требования по организации и непосредственному функционированию процессов обработки персональных данных (далее - ПДн) в Общероссийской общественной организации «Российское общество клинической онкологии» (далее - организации) в соответствии с требованиями нормативно-правовых актов РФ в области обработки и защиты ПДн.

1.2. Требования настоящего Положения распространяются на всех работников организации.

1.3. Требования настоящего Положения распространяются на все процессы обработки ПД всех категорий субъектов ПД, независимо от формы представления ПД.

## 2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. В настоящем Положении использованы ссылки на следующие документы:

- Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

## 3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

3.1. В настоящем Положении применяются следующие термины с соответствующими определениями:

**Безопасность ПДн** - состояние защищенности ПДн от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность ПДн при их обработке, независимо от формы их представления.

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

**Биометрические ПДн** - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

**Доступность ПДн** - возможность беспрепятственного получения санкционированного доступа к персональным данным лицами, имеющими право на такой доступ.

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

**Конфиденциальность ПДн** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта ПДн или иного законного основания.

**Материальный носитель** - материальный объект (изделия, документы, дискеты, магнитные ленты, магнитооптические, лазерные диски, фото- и видео негативы и позитивы, и другие), в том числе физические поля, в которых сведения находят свое отображение в виде файлов, символов, образов, сигналов, технических решений, процессов и т.п.

**Обработка ПДн** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с ПДн.

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

**Пользователь ИСПДн** - должностное лицо, участвующее в процессах(е)

обработки ПДн или использующее результаты такой обработки, а также имеющее доступ к ИСПДн организации.

**Предоставление ПДн** - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

**Процесс обработки ПДн** - бизнес-процесс Общероссийской общественной организации «Российское общество клинической онкологии», в рамках которого осуществляется обработка персональных данных.

**Работник** - лицо, заключившее трудовой договор с Общероссийской общественной организации «Российское общество клинической онкологии».

**Режим конфиденциальности информации** - совокупность установленных в Организации правовых, организационных, технических и иных мер по обеспечению хранения, защиты, доступа, передачи и предоставления конфиденциальной информации с целью недопущения ее разглашения.

**Средство защиты информации** - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**Субъект ПДн** - физическое лицо, к которому относятся ПДн (в том числе работник Общероссийской общественной организации «Российское общество клинической онкологии»).

**Трансграничная передача ПДн** - передача ПДн на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Третьи лица** - юридические и физические лица, участвующие в обработке ПДн, обрабатываемых Организацией. Данные лица участвуют в обработке ПДн в силу того, что они получают ПДн от Организации и/или передают эти данные в определенных целях.

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

**Целостность ПДн** - способность средства вычислительной техники или информационной системы обеспечивать неизменность персональных данных в условиях случайного и/или преднамеренного их искажения (разрушения).

3.2. В настоящем Положении использованы следующие сокращения:

**ИС** - информационная система;

**ИСПДн** - информационная система персональных данных;

**Организация** - Общероссийская общественная организация «Российской общество клинической онкологии»;

**ПДн** - персональные данные;

**СЗИ** - средство защиты информации;

**СЗПДн** - система защиты персональных данных;

**СКУД** - система контроля и управления доступом;

**ТК РФ** - Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ;

**ФСБ России** - Федеральная служба безопасности Российской Федерации;

**ФСТЭК России** - Федеральная служба технического и экспортного контроля.

## 4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. При работе с ПДн во всех случаях, не урегулированных настоящим Положением и другими внутренними нормативными документами организации, необходимо руководствоваться действующим законодательством РФ.

4.2. Гриф конфиденциальности для документов и материальных носителей информации, содержащей ПДн, не предусмотрен.

# 5. ПОЛИТИКА ОРГАНИЗАЦИИ В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В целях обеспечения неограниченного доступа к документу, определяющему политику организации в отношении обработки ПДн и к сведениям о реализуемых требованиях к защите ПДн, разработан документ «Политика Общероссийской общественной организации «Российское общество клинической онкологии» в области обработки и обеспечения безопасности ПДн» (далее - Политика). Политика содержит:

- принципы обработки ПДн;
- основные правила обработки ПДн;
- реализуемые требования по обеспечению безопасности ПДн.

## 6. ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

6.1. Под ПДн понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (в том числе, работнику Организации).

6.2. Детальный состав сведений, относящихся к ПДн, приводится в Перечне персональных данных, обрабатываемых в Общероссийской общественной организации «Российское общество клинической онкологии» (далее - Перечень ПДн). В Перечне ПДн закрепляются категории субъектов ПДн, группы и детальный состав ПДн, цели и правовые основания обработки для каждой из групп и категорий субъектов ПДн.

6.3. Перечень ПДн формируется на основе предложений от руководителей структурных подразделений организации. Пересмотр содержания Перечня ПДн проводится по мере необходимости, но не реже чем через 5 лет.

6.4. Работники Организации самостоятельно или по согласованию с непосредственным руководителем на основании Перечня ПДн определяют принадлежность информации к ПДн.

### Биометрические персональные данные

6.4.1. Организация не обрабатываются биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

### Специальные категории персональных данных

6.4.2. В Организации не допускается обработка ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, а также сведений о судимости.

6.4.3. В Организации допускается обработка сведений, касающихся состояния здоровья, в случаях и в порядке, предусмотренных законодательством.

# 7. ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В соответствии с принципами обработки, описанными в Политике, в организации определены правила обработки ПДн.

### 7.2. Сбор и накопление персональных данных

7.2.1. Организация может получать ПДн из следующих источников:

- непосредственно от субъекта ПДн;
- от третьего лица, в целях исполнения договорных обязательств или исполнения требований нормативных документов РФ
- из общедоступных источников.

7.2.2. В процессе деятельности происходит накопление ПДн в результате:

- получения оригиналов документов (трудовая книжка, договоры и т.п.).
- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажные носители и в базы данных автоматизированных систем).

### 7.3. Хранение и учет персональных данных

7.3.1. Хранение ПДн в Организации осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, за исключением случаев, когда срок хранения установлен федеральным законом, договором или требованиями нормативных документов РФ.

7.3.2. Организация осуществляет хранение ПДн следующими способами:

- на машинных носителях - при автоматизированной обработке ПДн;
- на бумажных носителях - при неавтоматизированной обработке.

7.3.3. Сроки хранения ПДн определены в Перечне ПДн.

7.3.4. Обработка, в том числе архивное хранение ПДн уволенных работников, осуществляется в соответствии с законодательством Российской Федерации.

7.3.5. Хранение сведений об уволенных работниках в Организации обеспечивается отдельно от сведений о действующих работниках.

### 7.4. Использование персональных данных

7.4.1. В Организации не допускается принятие решений на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

### 7.5. Трансграничная передача

7.5.1. В Организации осуществляется трансграничная передача персональных данных в случае регистрации членов общества для участия в мероприятиях, которые проходят в других странах.

### 7.6. Общедоступные источники персональных данных

7.6.1. В Организации допускается публикация в общедоступных источниках ПДн субъектов в порядке, предусмотренном российским законодательством.

7.6.2. В целях информационного обеспечения своей деятельности организации создает общедоступные источники ПДн работников (в том числе, справочники, адресные книги и т.д.), в которые с их согласия в письменной форме включаются Ф.И.О., служебная информация (должность, структурное подразделение) и контактная информация (номер рабочего и мобильного телефона, рабочий е-таП).

### 7.7. Блокирование персональных данных

7.7.1. Организация блокирует обрабатываемые ПДн при выявлении недостоверности обрабатываемых ПДн или неправомерных действий в отношении субъекта в следующих случаях:

- по требованию субъекта ПД;
- по требованию уполномоченного органа по защите прав субъектов ПДн;
- по результатам внутренних контрольных мероприятий.

### 7.8. Уничтожение персональных данных

7.8.1. Организация уничтожает персональные данные в случае:

-достижения целей обработки ПДн или утраты необходимости в их достижении;

- получения соответствующего запроса от субъекта ПДн, при условии, что данный запрос не противоречит требованиям законодательства РФ;
- отзыва согласия субъекта на обработку его ПДн (если отзыв согласия влечет за собой уничтожение ПДн);
- получения соответствующего предписания от уполномоченного органа по защите прав субъектов.

7.8.2. Уничтожение бумажных носителей, содержащих ПДн, производится в соответствии с Регламентом обеспечения безопасности.

7.8.3. Порядок уничтожения ПДн, содержащихся в ИС, определяется ответственным владельцем ИС.

## 8. ОЗНАКОМЛЕНИЕ РАБОТНИКОВ С ПРАВИЛАМИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Все работники в обязательном порядке должны проходить процедуру ознакомления с документами Организации, устанавливающими порядок обработки и обеспечения безопасности ПДн, включая настоящее Положение, а руководители и заместители руководителей структурных подразделений также пройти инструктаж (обучение).

8.2. Ознакомление работников производится под подпись либо иным способом, позволяющим достоверно установить факт ознакомления работников с содержанием настоящего Положения и следующих документов:

- Политика в области обработки и обеспечения безопасности персональных данных Общероссийской общественной организации «Российское общество клинической онкологии»
- Регламент обеспечения безопасности персональных данных в Общероссийской общественной организации «Российское общество клинической онкологии»
- Перечень персональных данных, обрабатываемых в Общероссийской общественной организации «Российское общество клинической онкологии»
- Перечень информационных систем персональных данных в Общероссийской общественной организации «Российское общество клинической онкологии»
- Регламент взаимодействия с субъектами персональных данных в Общероссийской общественной организации «Российское общество клинической онкологии»
- Перечень лиц, допущенных к работе с персональными данными
- Инструкция работника по правилам обработки и обеспечения безопасности персональных данных.

8.3. Ответственным за организацию проведения ознакомления работников Организации является руководитель Организации.

## 9. ОТВЕТСТВЕННОСТЬ

9.1. В соответствии с настоящим Положением работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую и иную ответственность, предусмотренную действующим законодательством Российской Федерации и внутренними документами компании.