

## **ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **ОСНОВНЫЕ ПОЛОЖЕНИЯ**

В настоящем Положении об обработке персональных данных (далее – Положение) установлены требования по организации и непосредственному функционированию процессов обработки персональных данных (далее – ПДн) Благотворительного фонда помощи тяжелобольным людям “Гольфстрим” (далее – Фонд) в соответствии с требованиями нормативных правовых актов РФ в области обработки и защиты ПДн.

Требования настоящего Положения распространяются на всех работников Фонда.

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

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

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

Настоящее Положение должно быть доведено до всех работников Фонда под подпись. Подпись работника на листе ознакомления означает его согласие со всеми требованиями, указанными в настоящем Положении.

### **ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

В настоящем Положении применяются следующие термины с соответствующими определениями:

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

**Безопасность ПДн** – состояние защищенности ПДн от неправомерных действий, характеризующееся 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.

**Пользователь ИСПДн** – должностное лицо, участвующее в процессах(е) обработки ПДн или использующее результаты такой обработки, а также имеющее доступ к ИСПДн Фонда.

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

**Процесс обработки ПДн** – бизнес-процесс Фонда, в рамках которого осуществляется обработка персональных данных.

**Работник** – лицо, заключившее трудовой договор или договор гражданско-правового характера (договор подряда) с Фондом.

**Режим конфиденциальности информации** – совокупность установленных в Фонде 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 Фонда).

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

**Третьи стороны** – юридические (редко – физические) лица, участвующие в обработке ПДн, совместно с Фондом. Данные лица участвуют в обработке ПДн в силу того, что они получают ПДн от Фонда 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).

В настоящем Положении использованы следующие сокращения:

**ИС** – информационная система;

**ИСПДн** – информационная система персональных данных;

**Фонд** – Благотворительный фонд «Гольфстрим»;

**ПДн** – персональные данные;

**СЗИ** – средство защиты информации;

**СЗПДн** – система защиты персональных данных;

**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.

## **ПОЛИТИКА В ОБЛАСТИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В целях обеспечения неограниченного доступа к документу, определяющему политику Фонда в отношении обработки ПДн и к сведениям о реализуемых требованиях к защите ПДн, разрабатывается документ «Политика в области обработки и обеспечения безопасности ПДн» (далее – Политика). Политика содержит:

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

Политика подлежит размещению на официальном веб-сайте Фонда.

## **ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**

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

Детальный состав сведений, относящихся к ПДн, приводится в Перечне персональных данных, обрабатываемых в БФ «Гольфстрим» (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.

Перечень ПДн формируется на основе предложений от руководителей программ Фонда (или владельцев процессов). Пересмотр содержания Перечня ПДн проводится по мере необходимости, но не реже чем через 3 года.

Ответственность за актуализацию Перечня ПДн возлагается на Ответственного за организацию обработки ПДн.

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

### ***Биометрические персональные данные***

В Фонде обрабатываются биометрические персональные данные (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) подопечных Фонда только на основании их письменного согласия.

### ***Специальные категории персональных данных***

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

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

## **ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

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

### ***Сбор и накопление персональных данных***

Фонд может получать ПДн из следующих источников:

- непосредственно от субъекта ПДн;

- от третьей стороны, в целях исполнения договорных обязательств или исполнения требований нормативных документов РФ.

В процессе деятельности происходит накопление ПДн в результате:

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

### ***Хранение и учет персональных данных***

Хранение ПДн в Фонде 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.

Фонд осуществляет хранение ПДн следующими способами:

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

Места хранения и сроки хранения ПДн утверждаются приказом Президента Фонда.

### ***Использование персональных данных***

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

### ***Общедоступные источники персональных данных***

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

В целях информационного обеспечения своей деятельности Фонд 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 e-mail).

### ***Блокирование персональных данных***

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

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

### ***Уничтожение персональных данных***

Фонд 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.

Уничтожение документов, содержащих ПДн, производится в соответствии с Регламентом обеспечения безопасности ПДн.

## **ОЗНАКОМЛЕНИЕ РАБОТНИКОВ С ПРАВИЛАМИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Все работники в обязательном порядке должны проходить процедуру ознакомления с документами Фонда, устанавливающими порядок обработки и обеспечения безопасности ПДн, включая настоящее Положение.

Ознакомление с документами Фонда производится под подпись либо иным способом, позволяющим достоверно установить факт ознакомления работников с содержанием указанных документов. Ответственным за организацию проведения ознакомления работников Фонда является Ответственный за организацию обработки персональных данных.

Актуальные версии нормативных документов Фонда по вопросам обработки и обеспечения безопасности ПДн размещаются на общем сетевом хранилище в папке «Персональные данные». Ответственность за актуальность размещенных документов СЗПДн возлагается на Ответственного за организацию обработки персональных данных.

## **ВЗАИМОДЕЙСТВИЕ С СУБЪЕКТАМИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОРГАНАМИ ВЛАСТИ**

### ***Взаимодействие с субъектами***

Порядок взаимодействия с субъектами ПДн или их законными представителями описан в Регламенте взаимодействия с субъектами персональных данных.

### ***Взаимодействие с органами власти***

Взаимодействие с органами власти осуществляется в соответствии с законодательством РФ.

Оценка законности и мотивированности запросов органов власти на предоставление информации о процессах обработки ПДн (в т. ч. на предоставление ПДн) проводится Ответственным за организацию обработки ПДн.

При взаимодействии с органами власти обязательным является принятие решения о подаче Уведомления в уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку ПДн. Форма и детальный состав Уведомления определяется в соответствии с нормативными документами Уполномоченного органа по защите прав субъектов ПДн. Ответственным за подачу Уведомления является Ответственный за организацию обработки ПДн.

Уполномоченным органом по защите прав субъектов ПДн (основным регулятором в сфере обработки ПДн) является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор). Роскомнадзор, в частности, уполномочен:

- осуществлять проверку сведений, содержащихся в Уведомлении, и привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
- обращаться к операторам с требованиями по уточнению, блокированию или уничтожению недостоверных или полученных незаконным путем ПДн;
- принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением установленных требований;
- направлять в ФСБ России и ФСТЭК России сведения о мерах по обеспечению безопасности ПДн, указанных в Уведомлении;
- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

- привлекать к административной ответственности лиц, виновных в нарушении установленных требований.

ФСБ России и ФСТЭК России могут быть наделены решением Правительства РФ полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности ПДн, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных. В т.ч. это касается отдельных решений Правительства РФ о проведении контрольных мероприятий.