

ПОЛИТИКА
обработки и защиты персональных данных
Ставропольской краевой общественной организации
«Ассоциация психиатров, психотерапевтов, клинических психологов
и социальных работников»

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом Ставропольской краевой общественной организации «Ассоциация психиатров, психотерапевтов, клинических психологов и социальных работников» (далее – СПА, Ассоциация, Организация или Оператор), определяющим ключевые направления её деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Обработка ПДн в Организации осуществляется в связи с выполнением Организацией функций, предусмотренных ее учредительными документами, и определяемых:

- Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 19 мая 1995 г. № 82-ФЗ «Об общественных объединениях»;
- Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных»;

- Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в Организации осуществляется в ходе достижения уставных целей, осуществления уставных задач и направлений деятельности, а также в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу: 355029, г. Ставрополь, ул. Ленина, д. 441; электронная версия Политики – на сайте по адресу: <https://stavpb.ru/8942-2>.

2. Термины и принятые сокращения

Общественная организация – основанное на членстве общественное объединение, созданное на основе совместной деятельности для защиты общих интересов и достижения уставных целей объединившихся граждан;

Члены общественной организации – физические лица и юридические лица - общественные объединения, чья заинтересованность в совместном решении задач данного объединения в соответствии с нормами его устава оформляется соответствующими индивидуальными заявлениями или документами, позволяющими учитывать количество членов общественного

объединения в целях обеспечения их равноправия как членов данного объединения;

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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;

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;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

- законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;
- системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;
- комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;

- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на членов СПА в пределах их обязанностей, связанных с обработкой и защитой ПДн;
- минимизация прав доступа: доступ к ПДн предоставляется членам СПА только в объеме, необходимом для исполнения уставных задач;
- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПДн;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаются или обезличиваются.

3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

4. Обработка персональных данных

СПА вправе осуществлять обработку персональных данных членов Организации без уведомления уполномоченного органа при соблюдении следующих условий:

- осуществляется обработка персональных данных членов Организации;
- обработка осуществляется для законных целей, предусмотренных учредительными документами Организации;
- персональные данные не распространяются или раскрываются третьим лицам без согласия в письменной форме субъектов персональных данных.

4.1. Получение ПДн

4.1.1. Все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПДн создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

б) внесения сведений в учетные формы;

в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

4.2. Обработка ПДн

4.2.1. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

4.2.2. Цели обработки ПДн

СПА обрабатывает персональные данные в целях осуществления деятельности, предусмотренной Уставом Организации, а именно:

- объединения усилий членов организаций, входящих в Ассоциацию, для защиты и реализации гражданских прав и социальных интересов врачей и иных специалистов, работающих в психиатрии; пациентов, а также для развития практической и научной деятельности в области психиатрии, психотерапии, психологии;

- объединения врачей-психиатров, клинических психологов, социальных работников, других специалистов в области психиатрии и психотерапии с целью обеспечения защиты их гражданских прав и социальных интересов, повышения их профессионального уровня, развития психиатрической науки, повышения престижа психиатрии;
- осуществления разработки текущих и перспективных планов развития здравоохранения в области психиатрии и психотерапии, психологии в Ставропольском крае.
- в интересах достижения уставных целей и задач, а также исполнения обязательств, установленных законодательством Российской Федерации и иными нормативно-правовыми актами.

4.2.3. Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов:

- субъекты персональных данных, являющиеся членами СПА;
- субъекты персональных данных, состоящие в трудовых отношениях с Оператором;
- субъекты персональных данных, состоящие с Оператором в гражданско-правовых отношениях;
- субъекты персональных данных, являющиеся кандидатами на соискание вакантной должности или исполнение услуг;
- субъекты персональных данных, обратившиеся в Организацию за оказанием услуг или действующие совместно в целях достижения уставных целей и задач.
- иные субъекты персональных данных, добровольно и в своем интересе давшие согласие СПА на обработку их персональных данных.

4.2.4. Обработка персональных данных ведется:

- с использованием средств автоматизации;
- без использования средств автоматизации.

4.3. Хранение ПДн

4.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.4. Уничтожение ПДн

4.4.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

4.4.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.5. Передача ПДн

4.5.1. Организация передает ПДн третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.5.2. Перечень лиц, которым передаются ПДн

Третьи лица, которым передаются ПДн:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);

- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- иные органы, осуществляющие контроль и надзор за общественными организациями.

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

5.5. Основными мерами защиты ПДн, используемыми Организацией, являются:

5.5.1. Персональная ответственность за обработку ПДн, соблюдение членами Организацией требований к защите ПДн;

5.5.2. Разработка политики в отношении обработки персональных данных;

5.5.3. Установление правил доступа к ПДн, обрабатываемым в ИСПД;

5.5.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

5.5.5. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

5.5.6. Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ;

5.5.7. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

5.5.8. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.5.9. Обучение членов Организации непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

6. Основные права субъекта ПДн и обязанности Организации

6.1. Основные права субъекта ПДн

Субъект ПДн имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;

- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Обязанности Организации

Организация обязана:

- при сборе ПДн предоставить информацию об обработке его ПДн;
- в случаях если ПДн были получены не от субъекта ПДн уведомить субъекта;

- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;
- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.