
**Политика «О защите
персональных данных»**

версия 1.0

Уровень доступа: общий

Содержание

1. Общие положения	5
2. Определения	5
3. Сокращения	6
4. Принципы обработки и обеспечения безопасности ПДн	6
5. Основные требования к обработке ПДн	7
6. Мероприятия по обеспечению безопасности ПДн	7
7. Права субъектов ПДн	8
8. Обязанности сотрудников Компании	8
9. Подразделение ответственное за контроль соблюдения Политики	8
10. Ответственность за несоблюдение Политики	9
11. Заключительное положение	9

1. Общие положения

- 1.1. Настоящая внешняя Политика « О защите персональных данных» (далее – Политика) разработана на основании:
- 1.2. Федеральный закон № 152 « О защите персональных данных» от 27.07.2006.
- 1.3. Постановления Правительства РФ №687 « Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008.
- 1.4. Постановления Правительства РФ №781 « Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.10.2007.
- 1.5. Целями настоящей Политики являются определение обработки и обеспечения безопасности персональных данных.
- 1.6. Настоящая Политика распространяется на все бизнес процессы компании и обязательна к выполнению всеми сотрудниками Общероссийской общественной организации содействия развитию медицинской реабилитологии "Союз реабилитологов России" (далее – Компания).
- 1.7. В связи с общедоступностью настоящей Политики, более детальное описание процессов обработки и обеспечения безопасности персональных данных описано во внутренних нормативных документах.

2. Определения

- 2.1. персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 2.2. 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;
- 2.3. 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;
- 2.4. автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- 2.5. распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 2.6. предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 2.7. блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 2.8. уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- 2.9. обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 2.10. информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 2.11. машинный носитель - магнитный диск, магнитная лента, лазерный диск и иные материальные носители, используемые для записи и хранения информации с помощью электронно-вычислительной техники.

3. Сокращения

ДЗБ – департамент защиты бизнеса
ИБ – информационная безопасность
ИСПДн – информационная система персональных данных
НСД – несанкционированный доступ ПДн – персональные данные РФ – Российская Федерация
ФЗ – федеральный закон

4. Принципы обработки и обеспечения безопасности ПДн

- 4.1. Принципы обработки ПДн в Компани:
 - 4.1.1. Обработка ПДн должна осуществляться на законной и справедливой основе.
 - 4.1.2. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.
 - 4.1.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.
 - 4.1.4. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.
 - 4.1.5. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
 - 4.1.6. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
- 4.2. Компания как оператор, осуществляет обработку ПДн физических лиц в рамках требований законодательства РФ в целях:
 - 4.2.1. Организации кадрового учета Компании, обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам; ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства, заполнения первичной статистической документации, в соответствии с Трудовым кодексом

РФ, Налоговым кодексом РФ, федеральными законами, в частности: « Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования».

- 4.2.2. Многократного пропуска субъектов ПДн на территорию Компании.
- 4.2.3. Заключение, исполнения и прекращения гражданско-правовых договоров с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством.
- 4.2.4. Предоставление физическим лицам разнообразных услуг, требующих осуществлять сбор и обработку ПДн.
- 4.3. В Компании используется смешанная обработка ПДн. Под смешанной обработкой понимается автоматизированная и неавтоматизированная обработка ПДн.
- 4.4. В случае достижения целей обработки ПДн, если другое не предусмотрено законодательством РФ, Компания прекращает обработку и производит уничтожение ПДн. Уничтожение ПДн, в электронном виде, и ПДн, содержащихся на материальных носителях, производится ответственными за этот процесс лицами согласно внутренней документации Компании.
- 4.5. В Компании используются современные и безопасные технологические решения для автоматизированной обработки, передачи и хранения персональных данных, исключающих несанкционированный доступ и утечку.

5. Основные требования к обработке ПДн

- 5.1. Обработка ПДн в Компании должна осуществляться с согласия субъекта ПДн кроме случаев, когда такое согласие не требуется или же по поручению, в тех случаях когда Компания не является оператором ПДн субъектов.
- 5.2. В случаях предусмотренных законодательством обработка ПДн осуществляется с согласия субъекта ПДн, оформляемого в соответствии со статьей 9 ФЗ №152.
- 5.3. Рекомендации к порядку получения согласия субъекта ПДн и виду согласия описаны во внутренней документации Компании.
- 5.4. В Компании ведется учет работников, допущенных к обработке ПДн. Учет ведется в согласованном Перечне лиц допущенных к обработке ПДн.
- 5.5. Во избежание НСД к ПДн рекомендуется:
 - 5.5.1. При неавтоматизированной обработке руководствоваться требованиями предъявляемыми постановлением Правительства РФ №687 « Об утверждении положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации» от 15.09.2008.
 - 5.5.2. При автоматизированной обработке руководствоваться требованиями предъявляемыми постановлением Правительства РФ №781 « Об утверждении положения об обеспечении безопасности ПДн при их обработке в информационных системах ПДн» от 17.10.2007 и приказом ФСТЭК России №58 "Об утверждении положения о методах и способах защиты информации в информационных системах ПДн".

6. Мероприятия по обеспечению безопасности ПДн

- 6.1. Мероприятия по обеспечению безопасности ПДн реализуются:
 - 6.1.1. определение угроз безопасности ПДн при их обработке в информационных системах ПДн;
 - 6.1.2. применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимых для выполнения требований к защите ПДн;
 - 6.1.3. оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;

- 6.1.4. учет машинных носителей ПДн;
- 6.1.5. обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
- 6.1.6. восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 6.1.7. установление правил доступа к персональным данным, обрабатываемым в информационной системе ПДн, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе ПДн.

7. Права субъектов ПДн

- 7.1. Субъект ПДн согласно ФЗ имеет следующие права:
 - 7.1.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн.
 - 7.1.2. Субъект ПДн вправе требовать от оператора уточнения его ПДн, 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.
 - 7.1.3. Сведения, предоставляются субъекту ПДн на основании запроса. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8. Обязанности сотрудников Компании

- 8.1. Работники Компании, допущенные к обработке ПДн, обязаны:
 - 8.1.1. Ознакомиться с данной Политикой и внутренними документами, регламентирующими процесс обработки ПДн, и выполнять требования этих документов.
 - 8.1.2. Обрабатывать ПДн только в рамках выполнения своих должностных обязанностей.
 - 8.1.3. Не разглашать ПДн, к которым был получен доступ в рамках исполнения своих трудовых обязанностей
 - 8.1.4. Информировать о фактах разглашения (уничтожения, искажения) ПДн сотрудников ИБ.

9. Подразделение ответственное за контроль соблюдения Политики

- 9.1. Контроль обеспечения безопасности ПДн и соблюдения требований настоящей Политики осуществляется ДЗБ и сотрудниками по ИБ.
- 9.2. Контроль осуществляется путем разрешения инцидентов ИБ согласно внутренним документам Компании, а так же в рамках иных контрольных мероприятий.

10. Ответственность за несоблюдение Политики

10.1. Сотрудники Компании, допустившие несоблюдение настоящей Политики, повлекшее за собой разглашение, утрату или нарушение целостности ПДн несут ответственность в соответствии с действующим законодательством.

11. Заключительное положение

11.1. Изменения в настоящую Политику могут быть внесены Генеральным директором Компании, ДЗБ, сотрудниками по ИБ.

11.2. Настоящая Политика обязательна для соблюдения всеми сотрудниками Компании.

11.3. Режим конфиденциальности ПДн снимается в случаях их обезличивания, если иное не определено законодательством РФ.