

ПОЛИТИКА
обработки персональных данных
в ООО «СберМедИИ»

(версия 2.0)

ОГЛАВЛЕНИЕ

1.	Общие положения	3
2.	Термины и определения	4
3.	Обозначения и сокращения	5
4.	Обработка персональных данных	5
5.	Обеспечение безопасности персональных данных	9
6.	Права субъектов персональных данных	11
7.	Ответственность	13
8.	Порядок пересмотра и внесения изменений.....	14

1. Общие положения

1.1. Настоящая Политика обработки персональных данных в ООО «СберМедИИ» (далее – Политика) разработана в соответствии со следующими документами:

- 1) Конституцией Российской Федерации;
- 2) Гражданским кодексом Российской Федерации;
- 3) Трудовым кодексом Российской Федерации;
- 4) Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 5) Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- 6) Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- 7) постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 8) постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 9) приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- 10) приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- 11) иными нормативными правовыми актами Российской Федерации в области обработки и обеспечения безопасности персональных данных.

1.2. Требования Политики распространяются на все процессы обработки персональных данных в ООО «СберМедИИ» (далее – Общество), осуществляемые как с использованием средств автоматизации, так и без использования таких средств, и обязательны для исполнения всеми работниками Общества.

1.3. Положения Политики служат основой для разработки внутренних документов Общества, регламентирующих отдельные процессы обработки

персональных данных и обеспечение безопасности персональных данных при их обработке в Обществе, а также устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

2. Термины и определения

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

2.2. 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 Федеральным законом «О персональных данных».

2.3. 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.

2.4. 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.

2.5. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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

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

2.9. 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.

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

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

2.12. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Обозначения и сокращения

3.1. Общество – ООО «СберМедИИ».

3.2. Политика – Политика обработки персональных данных в ООО «СберМедИИ».

4. Обработка персональных данных

4.1. Общество в соответствии с Федеральным законом «О персональных данных» является оператором, осуществляющим обработку персональных данных.

4.2. Обработка персональных данных в Обществе осуществляется на основе следующих принципов:

- 1) обработка персональных данных должна осуществляться на законной и справедливой основе;
- 2) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;
- 3) не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- 4) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- 5) обработке подлежат только персональные данные, которые отвечают целям их обработки;
- 6) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;
- 7) обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- 8) при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых

случаях и актуальность по отношению к целям обработки персональных данных;

9) должны быть приняты необходимые меры либо обеспечено их принятие по удалению или уточнению неполных или неточных данных;

10) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

11) обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

4.3. Обработка персональных данных в Обществе допускается в следующих случаях:

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

2) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

3) обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

4) обработка персональных данных осуществляется в статистических или иных исследовательских целях (за исключением обработки персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации), при условии обязательного обезличивания персональных данных;

5) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

6) обработка осуществляется в иных предусмотренных Федеральным законом «О персональных данных» случаях.

4.4. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

4.5. Общество обеспечивает конфиденциальность обрабатываемых персональных данных, не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4.6. Общество вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (поручения).

4.7. Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных», соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных указанным Федеральным законом.

4.8. В поручении должны быть определены или установлены:

- 1) перечень персональных данных;
- 2) перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных по поручению Общества;
- 3) цели обработки персональных данных;
- 4) обязанность лица, осуществляющего обработку персональных данных по поручению Общества, соблюдать конфиденциальность персональных данных;
- 5) обязанность лица, осуществляющего обработку персональных данных по поручению Общества, осуществлять сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) или извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации;
- 6) обязанность лица, осуществляющего обработку персональных данных по поручению Общества, выполнять меры, предусмотренные статьей 18.1 Федерального закона «О персональных данных»;
- 7) обязанность лица, осуществляющего обработку персональных данных по поручению Общества, обеспечивать безопасность персональных данных при их обработке,
- 8) требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных»;
- 9) требование об уведомлении Общества о случаях неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекших нарушение прав субъектов персональных данных, в соответствии с частью 3.1 статьи 21 Федерального закона «О персональных данных»;

10) обязанность лица, осуществляющего обработку персональных данных по поручению Общества, по запросу Общества в течение срока действия поручения, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение требований, установленных настоящим пунктом 4.8 Политики и частью 3 статьи 6 Федерального закона «О персональных данных».

4.9. К обрабатываемым персональным данным допускаются работники Общества, доступ которым необходим для исполнения возложенной на них трудовой функции. Доступ предоставляется на основании утверждаемого приказом Общества перечня (номенклатуры) должностей работников, осуществляющих обработку персональных данных, либо имеющих доступ к ним.

4.10. Трудовые договоры с работниками Общества, допущенными к обработке персональных данных, либо имеющих доступ к ним, а также должностные инструкции должны содержать обязательства о необходимости соблюдения конфиденциальности обрабатываемых персональных данных и исполнении требований внутренних документов Общества в области обработки и обеспечения безопасности персональных данных.

4.11. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в Обществе не допускается.

4.12. Общество не осуществляет обработку биометрических персональных данных.

4.13. Общество не осуществляет трансграничную передачу персональных данных на территории иностранных государств.

4.14. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Общество осуществляет запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

4.15. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято Обществом на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

4.16. В Обществе назначается лицо, ответственное за организацию обработки персональных данных, которое получает указания непосредственно от исполнительного органа и подотчетно ему.

4.17. Общество разрабатывает внутренние документы, регламентирующие отдельные процессы обработки персональных данных, определяющие для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также внутренние документы, регламентирующие обеспечение безопасности персональных данных при их обработке в Обществе и устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Разрабатываемые Обществом внутренние документы не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на Общество не предусмотренные законодательством Российской Федерации полномочия и обязанности.

5. Обеспечение безопасности персональных данных

5.1. В Обществе для обеспечения выполнения обязанностей, предусмотренных законодательством Российской Федерации, при обработке персональных данных должны приниматься необходимые правовые, организационные и технические меры или обеспечиваться их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.2. Обеспечение безопасности персональных данных в Обществе достигается, в частности:

- 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- 3) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- 4) учетом машинных носителей персональных данных;
- 5) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

- 6) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 7) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- 8) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;
- 9) осуществлением внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям внутренних документов Общества и законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных;
- 10) оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения требований законодательства Российской Федерации в области обработки персональных данных, соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации;
- 11) ознакомлением работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, внутренними документами Общества, определяющими политику Общества в отношении обработки персональных данных, по вопросам обработки персональных данных, и (или) обучение указанных работников;
- 12) назначением лица, ответственного за обеспечение безопасности персональных данных в Обществе, а в установленных Правительством Российской Федерации случаях созданием структурного подразделения, ответственного за обеспечение безопасности персональных данных в Обществе, либо возложением на одно из структурных подразделений Общества функций по обеспечению такой безопасности.

5.3. Общество обязано обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

5.4. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, а также контроль и (или) аудит соответствия обработки персональных данных требованиям внутренних документов Общества и законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных проводится Обществом самостоятельно и (или) с привлечением на договорной основе третьих

лиц, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанные мероприятия проводятся не реже одного раза в три года.

6. Права субъектов персональных данных

6.1. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. Общество, в случае получения согласия на обработку персональных данных от представителя субъекта персональных данных, проверяет полномочия данного представителя на дачу согласия от имени субъекта персональных данных.

6.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Общество вправе продолжить обработку персональных данных в случаях и в порядке, прямо предусмотренных законодательством Российской Федерации.

6.3. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение Обществом согласия на обработку персональных данных являются обязательными, Общество обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

6.4. Субъект персональных данных вправе требовать от Общества 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 законодательством Российской Федерации меры по защите своих прав.

6.5. Субъект персональных данных имеет право на получение следующей информации, касающейся обработки его персональных данных в Обществе, за исключением случаев ограничения указанного права, предусмотренных Федеральным законом «О персональных данных»:

- 1) подтверждение факта обработки персональных данных Обществом;
- 2) правовые основания и цели обработки персональных данных Обществом;
- 3) цели и применяемые Обществом способы обработки персональных данных;

- 4) наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом или на основании федерального закона;
- 5) обрабатываемые Обществом персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- 8) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу;
- 9) информацию о способах исполнения Обществом обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;
- 10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

6.6. Указанные сведения, предоставляются Обществом субъекту персональных данных или его представителю в течение 10 (десяти) рабочих дней с момента обращения либо получения Обществом запроса субъекта персональных данных или его представителя. Срок может быть продлен, но не более чем на 5 (пять) рабочих дней в случае направления Обществом в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.7. Запрос субъекта персональных данных или его представителя должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Обществом, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.8. Общество предоставляет сведения субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

6.9. В случае, если запрошенные сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться в Общество повторно или направить повторный запрос не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.10. Общество вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным Федеральным законом «О персональных данных». Такой отказ должен быть мотивированным.

6.11. Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований законодательства Российской Федерации или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6.12. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. Ответственность

7.1. Ответственность за соблюдение требований настоящей Политики возлагается на каждого работникам Общества.

7.2. Руководители структурных подразделений Общества обязаны организовывать работу подчиненных работников с учетом требований законодательства Российской Федерации, настоящей Политики и других внутренних документов Общества в области обработки и обеспечения безопасности персональных данных.

7.3. Работники Общества, нарушающие требования законодательства Российской Федерации, настоящей Политики и других внутренних документов Общества в области обработки и обеспечения безопасности персональных данных, могут нести материальную, дисциплинарную, административную, гражданско-правовую и (или) уголовную ответственность в соответствии с законодательством Российской Федерации.

7.4. Решение о применении и выборе мер ответственности, либо о передаче в соответствующие органы государственной власти принимается руководством Общества по результатам проведенного служебного расследования.

8. Порядок пересмотра и внесения изменений

8.1. Внесение изменений в Политику производится по необходимости или в случае изменения законодательства Российской Федерации в области обработки персональных данных.