**ООО «МОРСЕль»**



**Политика обработки и защиты персональных данных**

**1. Общие положения**

1.1. Настоящая политика в отношении персональных данных (далее- Политика) составлена в соответствии с п.2ст.18.1 Федерального закона №152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом общества с ограниченной ответственностью «МОРСЕль» ( далее- Организация или Оператор), определяющим ключевые направления его 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 защиты ПДн, полученных до её утверждения.

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

- Федеральным законом от 21 ноября 2011г. №323-ФЗ «Об основах охраны здоровья граждан в Российской федерации»;

- 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 трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя ( глава 14 Трудового кодекса Российской Федерации), 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 её размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу: *Свердловская область, Пригородный район, село Николо – Павловское, улица Северная корпус 5А, электронная версия Политики - на сайте по адресу: morsel-nt.ru*

**2. Термины и принятые сокращения**

**Персональные данные (ПДн)**- любая информация, относящаяся к прямо или косвенно определённому 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 неопределённому кругу лиц.

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

**Блокировка 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 –** обработкам 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.

**Пациент** - физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

**Медицинская деятельность** – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз. Медицинских осмотров и медицинских освидетельствований, санитарно- противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) её компонентов в медицинских целях.

**Лечащий врач-** врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

**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 документах уполномоченных государственных органов в области обработки и защиты персональных данных;

- системность: обработка ПДн в Организации осуществляется с учётом всех взаимосвязанных, и 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 учётом 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 Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

- минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объёме, необходимом для выполнения их должностных обязанностей;

- гибкость: обеспечение выполнение функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных организации, а также объёма и состава обрабатываемых ПДн;

- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляется работниками, имеющими необходимую квалификацию и опыт;

- эффективность процедур отбора кадров: кадровая политика организации предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

- 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 постоянно 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 их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаются или обезличиваются.

3.4. При обработке ПДн обеспечивается 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**

4.1. Получение ПДн

4.1.1. Все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получать только у третьей стороны, то субъект должен уведомить 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 путём:

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

б) внесения сведений в учётные формы;

в) получение 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 внутренними регулятивными документами Организации.

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 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 общедоступным субъектом персональных данных).

Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов организации.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

Организацией производится устранение нарушений законодательства при обработке и защиты ПДн.

4.2.2. Цели обработки ПДн:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенции в соответствии с Федеральными законами от 21 ноября 2011г. №323 ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010г. №61-ФЗ « Об обращении лекарственных средств», правилами предоставления медицинскими организациями платных медицинских услуг, утверждёнными постановлением Правительства Российской Федерации от 04 октября 2012г. №1006;

- осуществление трудовых отношений;

- осуществление гражданско - правовых отношений.

4.2.3. Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;

- физические лица, уволившиеся из учреждения;

- физические лица, являющиеся кандидатами на работу;

- физические лица, состоящие с учреждением в гражданско- правовых отношениях;

- физические лица, обратившиеся в учреждение за медицинской помощью.

4.2.4. ПДн, обрабатываемые Организацией:

- данные, полученные при осуществлении трудовых отношений;

- данные, полученные для осуществления отбора кандидатов на работу в Организацию;

- данные, полученные при осуществлении гражданско- правовых отношений;

- данные, полученные при оказании медицинской помощи.

4.2.5. Обработка персональных данных ведётся:

- 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.

4.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (регистратура).

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 путём сожжения, дробления ( измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается

применение шредера.

4.4.2. ПДн на электронных носителях уничтожается путём стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанных членами комиссии.

4.5. Передача ПДн

5.5.1. Организация передает ПДн третьим лицам в следующих случаях:

- субъект выразил своё согласие на такие действия;

- передача предусмотрена российскими 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 учёта (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;

- бюро кредитных историй ( с согласия субъекта)

- юридические фирмы, работающие в рамках законодательства Р, при неисполнении обязательств по договору займа (с согласия субъекта).

**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 комплекс правовых, организационно - распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в ебя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнёрами 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. Назначение лица, ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждениеми его работниками требований к защите ПДн;

5.5.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД и разработка мер и мероприятий по защите ПДн;

5.5.3. Разработка политики в отношении обработки персональных данных;

5.5.4. Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учёта всех действий, совершаемых с ПДн в ИСПД;

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

5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учёт машинных носителей ПДн, обеспечение их сохранности;

5.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

5.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;

5.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;

5.5.10.Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

5.5.11. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учёта действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

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

5.5.13. Обучение работников организации, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

5.5.14. Осуществление внутреннего контроля и аудита.

**6. Основные права субъекта ПДн и обязанности организации**

6.1. Основные права субъекта ПДн

Субъект ПДн имеет право на получение информации, касающейся 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 (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник 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 осуществлённой 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 Федеральным законом или другими федеральными законами.

Субъект ПДн вправе требовать от оператора уничтожения 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, определяющего 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.