Приложение 1
к приказу № 43-орг
от «21»февраля 2018 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в
Санкт-Петербургском государственном бюджетном учреждении здравоохранения
«Бюро судебно-медицинской экспертизы»

СОГЛАСОВАНО:

Заместитель начальника по кадрам _____ А.В. Арбенина

Юрисконсульт _____ А.В. Федорова

«21» февраля 2018г.

1. Общие положения

1.1. Целью данного Положения является защита персональных данных объектов судебно-медицинской экспертизы и исследований (трупы, обследуемые лица), работников и иных лиц от несанкционированного доступа, разглашения, неправомерного их использования или утраты.

1.2. СПб ГБУЗ «БСМЭ» при обработке персональных данных руководствуется требованиями законодательства и иных нормативных правовых актов Российской Федерации: Конституции, Уголовно-процессуального кодекса, Гражданского процессуального кодекса, Кодекса об административных правонарушениях, Трудового кодекса, Гражданского кодекса, Федерального закона от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 31.05.2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», Федерального закона от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 29.07.04 № 98-ФЗ «О коммерческой тайне», Федерального закона от 22.10.04 № 125-ФЗ «Об архивном деле в Российской Федерации», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказа Минздравсоцразвития России от 12.05.2010 г. № 346н «Об утверждении Порядка организации и производства судебно-медицинских экспертиз в государственных судебно-экспертных учреждениях Российской Федерации» и иных нормативно-правовых актов.

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, а также в других случаях, предусмотренных федеральными законами.

Прекращается обработка персональных данных в СПб ГБУЗ «БСМЭ» в случаях ликвидации СПб ГБУЗ «БСМЭ» или прекращении деятельности, исполнении обязательств по договорам и в течение срока исковой давности, отзыве согласия на обработку персональных данных, если иное не предусмотрено законодательством Российской Федерации, либо в течение срока хранения документов согласно установленным срокам хранения для определенных категорий документов, если иное не предусмотрено действующим законодательством.

1.4. Настоящее Положение утверждается и вводится в действие приказом Начальника СПб ГБУЗ «БСМЭ» (далее – Оператор), и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

Цели обработки персональных данных

1.5.1. СПб ГБУЗ «БСМЭ» осуществляет обработку персональных данных в следующих целях:

- в отношении работников: содействие в трудовой деятельности, обеспечение личной безопасности, учет результатов исполнения договорных обязательств, осуществление безналичных платежей на счет работника, обеспечение работоспособности и сохранности ресурсов и имущества работодателя, осуществление коллективного взаимодействия и совместного использования информационных ресурсов, аттестация, повышение квалификации, а также наиболее полное исполнение обязательств в соответствии с Трудовым кодексом Российской Федерации и другими нормативно-правовыми актами в сфере трудовых отношений.

- в отношении контрагентов: с целью исполнения договорных отношений, государственных контрактов, а также требований законодательства Российской Федерации.

- в отношении лиц (их законных представителей), трупов, частей трупов и иных объектов судебно-медицинской экспертизы и исследования: с целью исполнения требований законодательства Российской Федерации (Уголовно-процессуального кодекса РФ, Гражданского процессуального кодекса РФ, Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации» от 31.05.2001 г. № 73-ФЗ, приказа Минздравсоцразвития РФ «Об утверждении Порядка организации и производства судебно-медицинских экспертиз в государственных судебно-экспертных учреждениях Российской Федерации» от 12.05.2010 г. № 346н и др.).

2. Понятие и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия в соответствии с законодательством о персональных данных:

1) 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) персональные данные работника – информация, необходимая Оператору в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

3) персональные данные объектов судебно-медицинской экспертизы и исследований (трупы, лица, являющиеся объектов экспертных исследований и иные лица) – информация, необходимая Оператору для производства судебно-медицинской экспертизы и/или исследования. Под информацией об объектах судебно-медицинской экспертизы и исследований (трупы, обследуемые лица) понимается информация, позволяющая идентифицировать его как личность (Ф.И.О., пол, дата рождения, место жительства и контактный телефон), а также данные о состоянии его здоровья, диагнозе и иные сведения, полученные при его обследовании.

4) врачебная тайна - соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении;

5) обработка персональных данных – сбор, систематизация, накопление, хранение,

уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, удаление, уничтожение персональных данных;

6) конфиденциальность персональных данных – обязательное для соблюдения назначенным ответственным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания;

7) распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

8) использование персональных данных – действия (операции) с персональными данными, совершаемые уполномоченным должностным лицом в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных, либо иным образом затрагивающих их права свободы или права и свободы других лиц;

9) блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

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

11) обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

12) общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.2. При поступлении на работу работник заполняет анкету, в которой указывает следующие сведения о себе: фамилия, имя, отчество; пол; дату рождения; семейное положение; наличие детей, их даты рождения; воинскую обязанность; место жительства и контактный телефон; образование, специальность; стаж работы по специальности; предыдущее(ие) место(а) работы; о прохождения курсов повышения квалификации; наличие ученых степеней и званий; наличие грамот, благодарностей и иных наград и поощрений; знание иностранного языка.

2.3. При заключении трудового договора лицо, поступающее на работу, предъявляет документы в соответствии со ст. 65 ТК РФ.

2.4. Работодатель имеет право проверять достоверность сведений, представляемых работником. По мере необходимости работодатель истребует у работника дополнительные сведения и документы, подтверждающие достоверность этих сведений.

2.5. При оформлении работника сотрудники отдела кадров заполняют

унифицированную форму № Т-2 "Личная карточка работника" и формируют личное дело, которое хранится в отделе кадров.

2.6. Личное дело работника состоит из следующих документов: трудовой договор; личная карточка формы № Т-2; фотография; копия трудовой книжки; характеристики, рекомендательные письма; паспорт (копия); документ об образовании (копия); военный билет (копия); свидетельство о регистрации в налоговом органе (ИНН) (копия); страховое свидетельство пенсионного государственного страхования (СНИЛС) (копия); свидетельство о заключении брака (копия); свидетельство о рождении детей (копия); копия документа о праве на льготы (удостоверение почетного донора, медицинское заключение о признании лица инвалидом, др.); результаты медицинского обследования (в случаях, установленных законодательством); документы, связанные с трудовой деятельностью (заявления работника, информация о заработной плате, отпусках, командировках, листах нетрудоспособности, аттестационные листы и документы, подтверждающие квалификацию, приказы о поощрениях и взысканиях, документы, связанные с переводом, дополнительные соглашения к трудовому договору, копии приказов, информация о негосударственном пенсионном обеспечении и др.).

2.7. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, электронные базы). В общедоступные источники персональных данных могут включаться фотография, фамилия, имя, отчество, должность, подразделение, данные об образовании, повышении квалификации, служебные телефоны и адрес электронной почты работников. Другие персональные данные (например, дата рождения и т.д.) могут включаться в справочники только с письменного согласия работников.

2.8. Сведения о режиме работы работников, оценке их профессиональной деятельности в СПб ГБУЗ «БСМЭ» к персональным данным не относятся, обладателем этих сведений является СПб ГБУЗ «БСМЭ», который распоряжается этими сведениями в соответствии с правовыми и нормативными документами.

3. Обработка персональных данных.

3.1. Под обработкой персональных данных понимается любое действие (операция) или совокупность действий (операций), совершаемых с персональными данными с использованием автоматизации или без использования таких средств.

3.2. В целях обеспечения прав, свобод и интересов человека и гражданина Оператор и его представители при обработке персональных данных обязаны соблюдает следующие общие требования:

3.2.1. Обработка персональных данных осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

3.2.2. Обработка персональных данных осуществляется только с письменного согласия субъекта персональных данных или в порядке, установленным законодательством или иными нормативными правовыми актами Российской Федерации.

3.2.3. При определении объема и содержания обрабатываемых персональных данных субъекта Оператор руководствуется Конституцией Российской Федерации, Трудовым Кодексом, федеральными законами, иными нормативно-правовыми актами.

3.2.4. Получение персональных данных может осуществляться как путем представления их самим субъектом, так и путем получения их из иных источников.

3.2.5. Персональные данные получают у субъекта персональных данных с его согласия. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

3.2.6. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, либо с деятельностью работодателя данные о частной жизни субъекта персональных данных (информация о сфере семейных бытовых, личных отношений, сведения о состоянии здоровья) могут быть получены и обработаны работодателем только с его письменного согласия.

3.2.7. Оператор не получает и обрабатывает персональные данные работников об их членстве в общественных объединениях или их профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. Доступ к персональным данным работников имеют сотрудники СПб ГБУЗ «БСМЭ», привлеченные к обработке, передаче и хранению персональных данных, которые необходимы Оператору и его должностным лицам (работникам) для выполнения ссвоих полномочий и функций, предусмотренных учредительными документами и должностными инструкциями: начальник СПб ГБУЗ «БСМЭ»; заместитель начальника по экспертной работе; директор; заместитель начальника по экономическим вопросам; заместитель начальника по кадрам; заместитель начальника по МОБ работе и ГО; главный бухгалтер; заведующий канцелярией; медицинский регистратор общеучрежденческого медицинского персонала; главная медицинская сестра; юрисконсульт; специалист по охране труда; специалист гражданской обороны; специалист по кадрам; инженер-программист; техник-программист; руководители структурных подразделений/заведующие отделениями; врачебный персонал, средний медперсонал, младший медперсонал и прочий медперсонал; сотрудники бухгалтерии.

3.4. Копировать и делать выписки персональных данных работников разрешается исключительно в служебных целях и с письменного разрешения заместителя начальника по кадрам, при этом разрешается получать только те персональные данные, которые необходимы для выполнения конкретных функций и полномочий, установленных учредительными документами и должностными инструкциями.

3.5. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.5.1. Персональные данные не используются Оператором в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в

соответствии с законодательством.

3.6. Передача персональных данных субъекта возможна только с их согласия или в случаях, прямо предусмотренных действующим законодательством.

3.6.1. При передаче персональных данных работников работодатель соблюдает следующие требования:

- не сообщать персональные данные субъектов в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции и обеспечения его безопасности.

3.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.8. Не допускается предоставление информации, содержащей персональные данные, по телефону или факсу.

3.9. Оператор обеспечивает хранение персональных данных в порядке, исключающем их утрату или их неправомерное использование.

3.10. При принятии решений, затрагивающих интересы субъекта персональных данных, Оператор не основывается на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Доступ к персональным данным.

4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Перечень лиц, имеющих доступ к персональным данным субъекта обозначен в п. 3.3 настоящего Положения.

4.1.2. Перечень лиц, имеющих доступ к персональным данным субъекта, определяется действующим законодательством и иными нормативными правовыми актами, а также начальником СПб ГБУЗ «БСМЭ» при утверждении локальных организационно-распорядительных актов и должностных инструкций.

4.2. Внешний доступ. К числу массовых потребителей персональных данных в соответствии с действующим законодательством и иными нормативными правовыми актами вне организации относятся государственные и негосударственные органы в рамках своей компетенции:

4.2.1. налоговые органы; правоохранительные и судебные органы; органы государственной статистики; страховые организации; военкоматы; органы социального страхования; пенсионные фонды; подразделения муниципальных органов управления;

4.2.2. надзорно-контрольные органы.

4.2.3. родственники субъекта или его законные представители (с письменного разрешения самого субъекта).

4.2.4. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных законом.

4.2.5. С письменного согласия гражданина или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

4.2.6. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

3.1) в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с законом;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти и федеральных государственных органов, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность, и в соответствии с законом;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с настоящим Федеральным законом.

4.2.5. При приеме на работу нового работника непосредственный руководитель подразделения (отдела, отделения, лаборатории) СПб ГБУЗ «БСМЭ», осуществляет ознакомление работника с должностной инструкцией под личную подпись и документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования персональных данных.

5. Защита персональных данных.

5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3. Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности Оператора.

5.4. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Оператором за счет его средств в порядке, установленном федеральным законом.

5.5. «Внутренняя защита».

5.5.1. Возможным источником несанкционированного доступа к персональным данным является персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

5.5.2. Для обеспечения внутренней защиты персональных данных соблюдаются ряд

мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к конфиденциальной информации;
- избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключается бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и специального режима охраняемой законом тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) для работы во внутренней сети Бюро и базы данных;
- утверждение порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

5.5.3. Защита персональных данных на электронных носителях:

- информация, содержащая персональные данные, должна быть разграничена по степени доступности и защищена паролем;
- при обработке информации, содержащей персональные данные, на средствах вычислительной техники должно быть установлено антивирусное программное обеспечение (с плановым обновлением антивирусной базы);
- сотрудники СПб ГБУЗ «БСМЭ», обрабатывающие на средствах вычислительной техники персональные данные, при подключении к локальной сети обязаны принимать максимальные меры по обеспечению безопасности.

5.6. «Внешняя защита».

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение сведениями ограниченного доступа и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Оператора, посетители, работники других организаций. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

5.6.3. Для обеспечения внешней защиты персональных данных работники обязаны соблюдать ряд утвержденных мер:

- порядок приема, учета и контроля деятельности посетителей;

- правила внутреннего трудового распорядка и пропускной режим Учреждения;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при приеме посетителей.
- По возможности персональные данные обезличиваются.
- Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.
- К мерам, применяемым для защиты Оператором персональных данных относятся:
- назначение Оператором работника, ответственного за организацию обработки персональных данных в СПб ГБУЗ «БСМЭ»;
- осуществление работником, ответственным за организацию обработки персональных данных в СПб ГБУЗ «БСМЭ», и иными должностными лицами внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;
- разработка документов, определяющие политику СПб ГБУЗ «БСМЭ» в отношении обработки персональных данных, локальных организационно-распорядительных документов по вопросам обработки персональных данных;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, с требованиями к защите персональных данных и охраняемой законом тайны, с документами, определяющими политику СПб ГБУЗ «БСМЭ» в отношении обработки персональных данных, локальными документами по вопросам обработки персональных данных;
- опубликование в сети Интернет на официальном сайте СПб ГБУЗ «БСМЭ» настоящего положения;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение прошедшей в установленном порядке процедуры оценки соответствия средств защиты информации;
- систематическое осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;
- осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

5.7. Работники Оператора должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны быть ознакомлены руководителем соответствующего подразделения с требованиями безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также знать свои обязанности по обеспечению такой защиты.

- Работникам запрещается устанавливать постороннее программное обеспечение,

подключать личные мобильные устройства и носители информации в целях скачивания (записи) на них защищаемую информацию.

- Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.
- При работе с персональными данными работники Оператора обязаны обеспечить отсутствие возможности просмотра персональных данных третьими лицами с мониторов.
- Работники обязаны без промедления сообщать обо всех наблюдаемых подозрительных случаях работы с персональными данными, могущих повлечь за собой угрозу безопасности персональным данным, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, своему непосредственному руководителю и (или) лицу, отвечающему за немедленное реагирование на угрозу безопасности персональных данных.

6. Права и обязанности субъекта персональных данных.

6.1. Закрепление прав субъекта, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2. Работники и их представители должны быть ознакомлены сотрудниками отдела кадров под подпись с документами Оператора, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся у Оператора, субъект персональных данных имеет право (с ограничениями, установленными действующим законодательством):

- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

6.4. Субъект персональных данных обязан:

- передавать Оператору или его представителю достоверные, по возможности, документированные персональных данных;
- своевременно сообщать Оператору об изменении своих персональных данных.

6.5. В целях защиты частной жизни, личной и семейной тайны субъекты персональных данных не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие

обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за правомерность данного разрешения.

7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским кодексом РФ лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается по закону.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору, использованию персональных данных может быть установлена в судебном порядке.

8. Заключительные положения.

8.1. Настоящее положение вступает в силу с момента его утверждения Начальником СПб ГБУЗ «БСМЭ.

8.2. Настоящее Положение в полном объеме распространяется на все подразделения, на всех должностных лиц и работников СПб ГБУЗ «БСМЭ».

8.2.1. Настоящее Положение доводится до сведения всех работников, участвующих в обработке персональных данных в СПб ГБУЗ «БСМЭ», под личную подпись.

8.2.2. СПб ГБУЗ «БСМЭ» имеет право вносить изменения в настоящее Положение. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Положения вступает в силу с момента его утверждения и подлежит размещению в сети Интернет на официальном сайте СПб ГБУЗ «БСМЭ», если иное не предусмотрено новой редакцией Положения.

8.2.3. За разглашение охраняемой законом тайны (коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника трудовой договор может быть расторгнут.