

«Утверждаю»
Главный врач СПб ГБУЗ ГВФД



Положение о персональных данных

Санкт-Петербургского государственного бюджетного учреждения здравоохранения
«Городской врачебно-физкультурный диспансер»

1. Общие положения

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников СПб ГБУЗ ГВФД (далее - организация).

1.2. Цель настоящего Положения - защита персональных данных работников организации от несанкционированного доступа и разглашения. Персональные данные являются конфиденциальной, строго охраняемой информацией.

1.3. Основанием для разработки настоящего Положения являются: Конституция РФ, гл. 14 Трудового кодекса РФ, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных", другие действующие нормативно-правовые акты РФ.

1.4. Настоящее Положение и изменения к нему утверждаются главным врачом организации и вводятся в действие приказом. Все работники организации должны быть ознакомлены с данным Положением и изменениями к нему под роспись.

1.5. Ответственным за сбор персональных данных является работник, на которого возложено ведение кадрового учета в организации.

1.6. Ответственными за обработку персональных данных являются: работник, на которого возложено ведение кадрового учета в организации, работники бухгалтерии.

2. Понятие персональных данных

2.1. Персональными данными является любая информация, относящаяся к конкретному работнику, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность, и используемая работодателем, в частности, в целях выполнения требований:

- трудового законодательства при приеме на работу и заключении трудового договора, в процессе трудовых отношений, при предоставлении гарантий и компенсаций и др.;
- налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также страховых взносов во внебюджетные фонды;
- пенсионного законодательства при формировании и представлении персонализированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение;
- заполнения первичной статистической документации в соответствии с Постановлением Госкомстата России от 05.01.2004 № 1 "Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты".

2.2. Персональные данные являются строго конфиденциальными, любые лица, получившие к ним доступ, обязаны хранить эти данные в тайне, за исключением данных, относящихся к следующим категориям:

- обезличенные персональные данные - данные, в отношении которых невозможно определить их принадлежность конкретному физическому лицу;

- общедоступные персональные данные.

2.3. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении соответствующего срока хранения.

3. Носители персональных данных

3.1. В организации осуществляется обработка персональных данных следующих субъектов:

- кандидаты на трудоустройство
- работники

- пациенты диспансера

3.2. В организации обрабатываются следующие виды и категории персональных данных:

- ФИО

- дата рождения

- место рождения

- гражданство

- адрес регистрации и проживания, номера домашнего и мобильного телефонов

- семейное, социальное, имущественное положение и доходы

- сведения об образовании, ученых степенях и научных званиях

- профессия, квалификация, стаж работы, должности и места прежней трудовой деятельности, характеристики, аттестация

- сведения, содержащиеся в документах медицинского освидетельствования

- паспортные данные

- сведения о наличии или отсутствии судимости

- сведения о воинской обязанности

- сведения о наградах и поощрениях

- личное фото

- биография

- идентификационный номер налогоплательщика (ИНН)

- страховой номер индивидуального лицевого счета (СНИЛС)

- полисы ОМС

- сведения, необходимые для работы с финансовыми организациями и свершения банковских операций

- иные сведения.

3.2. Бумажные носители персональных данных:

- трудовая книжка;

- журналы учета трудовых книжек;

- журнал учета командировок, листков нетрудоспособности;

- листки нетрудоспособности;

- материалы по учету рабочего времени;

- личная карточка Т-2;

- входящая и исходящая корреспонденция военкомата, страховой компании, службы судебных приставов;

- приказы по кадрам, основания к приказам по личному составу;

- ксерокопии документов удостоверяющих личность, дающих социальные гарантии, об образовании, содержащих другие сведения персонального характера;

- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

- копии отчетов, направляемые в органы статистики.

3.2. Электронные носители персональных данных - база данных по учету работников организации.

3.3. Персональные данные на бумажных носителях хранятся в сейфе.

3.4. При приеме работников кадровые документы, находящиеся в работе, могут

находиться на рабочих столах или в специальных папках только в течение рабочего дня. По окончании рабочего дня данные документы должны убираться в запирающиеся шкафы.

3.5. Персональные данные на электронных носителях защищены паролем доступа, доступ к специализированной программе осуществляется только через личный доступ - пароль, право на использование персональных данных имеют только работники, ответственные за обработку персональных данных.

4. Личное дело работника

4.1. Личное дело работника оформляется после издания приказа о приеме на работу.

4.2. Личное дело ведется на протяжении всей трудовой деятельности работника в данной организации, а после его увольнения хранится в организации в течение установленных законодательством сроков.

4.3. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

4.4. Перечень документов, содержащихся в личном деле работника при приеме на работу:

- копия паспорта;
- копия страхового пенсионного свидетельства;
- копия военного билета (у военнообязанных);
- копия документов об образовании (в том числе и дополнительного образования, если работник представляет их при приеме на работу или это требуется при выполнении определенных трудовых функций);
- копия свидетельства ИНН
- копия водительского удостоверения и документов на машину, если это требуется в связи с выполнением трудовой функции работника;
- личная карточка Т-2;
- трудовой договор;
- документы о прохождении обучения, испытательного срока;
- документы о составе семьи работника, необходимые для предоставления ему гарантий, связанных с выполнением семейных обязанностей;
- иные документы персонального учета, относящиеся к персональным данным работника.

4.5. Перечень возможных документов, содержащихся в личном деле работника:

- анкета претендента, резюме, характеристики, рекомендации, предъявляемые работником при принятии решения о заключении трудового договора претендента;
- дополнительные соглашения к трудовому договору;
- документы о повышении квалификации (письменные аттестации, дипломы, свидетельства и т.д.);
- документы о состоянии здоровья детей и других близких родственников, когда с наличием таких документов связано предоставление работнику каких либо гарантий и компенсаций;
- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством;
- документы о беременности работницы и возрасте детей для предоставления матери (отцу, другим родственникам) установленных законом условий труда, гарантий и компенсаций;
- медицинская справка о прохождении медицинского осмотра;
- иные документы персонального учета, относящиеся к изменениям персональных данных работника.

5. Доступ к персональным данным работника

5.1. Внутренний доступ (доступ внутри организации):

- руководство организации;
- работник, ответственный за ведение кадрового учета в организации;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- работники бухгалтерии - к тем данным, которые необходимы для выполнения конкретных функций;
- сам работник.

5.2. Внешний доступ. Массовые потребители персональных данных вне организации - государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

5.3. Другие организации. Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

5.4. Родственники и члены семей:

- персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

6. Сбор и обработка персональных данных работников

6.1. Работник обязан представлять работодателю комплекс достоверных документированных персональных данных, перечень которых установлен данным Положением.

6.2. Своевременно, в разумный срок, не превышающий пять рабочих дней, работник обязан лично либо через своего законного представителя сообщать работнику, ответственному за сбор информации, об изменении своих персональных данных либо представить соответствующие документы.

6.3. Представление работником подложных документов при поступлении на работу является основанием для расторжения трудового договора.

6.4. Работник, ответственный за сбор информации, при получении персональных данных или получении измененных персональных данных работника должен:

- проверить достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами;
- сделать копии представленных документов;
- сформировать или присовокупить к личному делу работника;
- внести соответствующие изменения в кадровые документы;
- при необходимости подготовить и подписать соответствующие документы, в которых отразить соответствующие изменения;
- донести до сведения работников, ответственных за обработку персональных данных, сведения об изменении этих данных.

6.5. Если персональные данные работника возможно получить только у третьей стороны, то работник, ответственный за ведение кадрового учета:

- уведомляет работника не позднее пяти рабочих дней до даты запроса о получении

данных у третьей стороны, сообщив работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

- получает от работника письменное согласие;
- при получении согласия делает запрос и получает необходимые данные.

6.6. В случае выявления неправомерных действий с персональными данными работника:

- работник или его законный представитель либо уполномоченный органа по защите прав субъектов персональных данных обращается к главному врачу с заявлением;

- главный врач издает приказ о блокировании персональных данных, относящихся к соответствующему работнику, с момента такого обращения или получения такого запроса на период проверки, и назначает ответственного за проведение служебного расследования;

- если в ходе служебного расследования подтвердился факт использования недостоверных персональных данных, то работник, ответственный за получение персональных данных, обязан уточнить персональные данные, внести соответствующие изменения и поправки в документы и снять их блокирование;

- если в ходе служебного расследования выявлен факт неправомерных действий с персональными данными, то работник, ответственный за обработку данных и допустивший подобные действия, в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений данный работник в срок, не превышающий трех рабочих дней с даты такого выявления, обязан уничтожить носитель персональных данных. Об устранении допущенных нарушений или об уничтожении носителя персональных данных работник, ответственный за сбор персональных данных, обязан уведомить работника или его законного представителя, а в случае если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

7. Передача персональных данных работника

7.1. При передаче персональных данных работника работники, ответственные за получение и обработку персональных данных, должны соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные работника, 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 работника, обязаны соблюдать конфиденциальность;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

7.2. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций;

- все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации;

- хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

8. Защита персональных данных

8.1. 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.

8.2. 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.

8.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

8.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

8.5. «Внутренняя защита».

8.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, 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.

8.5.2. Внутренняя защита персональных данных работников обеспечивается:

- ограничением и регламентацией состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

- строгим избирательным и обоснованным распределением документов и информации между работниками;

- рациональным размещением рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знанием работником требований нормативно – методических документов по защите информации и сохранении тайны;

- наличием необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- организацией порядка уничтожения информации;

- воспитательной и разъяснительной работой с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только главному врачу, работникам отдела кадров и в исключительных случаях, по письменному разрешению главного врача, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

8.5.3. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается руководителю отдела кадров и руководителю службы информационных технологий

8.6. «Внешняя защита».

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

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

8.6.3. Внешняя защита персональных данных сотрудников обеспечивается:

- порядком приема, учета и контроля деятельности посетителей;
- пропускным режимом организации;
- техническими средствами охраны, сигнализации;
- порядком охраны территории, зданий, помещений, транспортных средств;
- требованиями к защите информации при интервьюировании и собеседованиях.

8.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

8.8. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

9. Ответственность за разглашение информации, связанной с персональными данными работника

9.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.