УТВЕРЖДАЮ
Главный врач ГБУЗ «ГКБ имени В.М. Буянова ДЗМ»
А.В. Саликов

СВЕДЕНИЯ

о реализуемых требованиях к защите персональных данных, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в ГБУЗ «ГКБ имени В.М. Буянова ДЗМ»

СОДЕРЖАНИЕ

1. Термины и определения....3
2. Организационные и правовые меры....4
3. Права субъектов персональных данных и порядок обращения....6
4. Меры по обеспечению безопасности персональных данных....6
на официальном сайте....6
5. Технические меры защиты персональных данных....7
в информационных системах Оператора....7
6. Меры реагирования на инциденты и взаимодействие с контролирующими органами....8
7. Меры по обеспечению безопасности баз данных персональных данных (исполнение ч. 5 ст. 18 Федерального закона № 152-ФЗ)....8
8. Заключительные положения....9

1. Термины и определения

Персональные данные (далее - ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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. В настоящем документе под Оператором понимается ГБУЗ «ГКБ имени В.М. Буянова ДЗМ».

Субъект персональных данных (далее - субъект ПДн) – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

СЗИ от НСД — средства защиты информации от несанкционированного доступа.

Пользователь – любое физическое лицо, являющееся субъектом персональных данных, которое взаимодействует с Оператором, в том числе посредством официального сайта Оператора, и чьи персональные данные обрабатываются Оператором.

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.

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

Информационная система персональных данных (далее - ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Блокирование 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.

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

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

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

Материальный носитель персональных данных – материальный носитель (дела, книги и журналы учёта, договоры, иные съёмные носители информации, содержащие персональные данные) с зафиксированной на нём в любой форме информацией,

содержащей персональные данные субъектов персональных данных в виде текста, фотографии и (или) их сочетания.

Сайт – официальный сайт ГБУЗ «ГКБ имени В.М. Буянова ДЗМ», расположенный по адресу: https://gkb-buyanova.ru/

Cookie – небольшой фрагмент данных, отправленный веб-сервером и хранимый на устройстве пользователя, который веб-сервер отправляет при попытке открыть страницу соответствующего сайта.

2. Организационные и правовые меры

2.1 Назначено лицо, ответственное за организацию обработки персональных данных. Ответственный выполняет свои функции в соответствии с должностной инструкцией.

2.2 Разработаны и утверждены все необходимые локальные нормативные акты, определяющие политику обработки персональных данных, включая:

- Политику обработки персональных данных;
- Положение об обработке персональных данных;
- Настоящие Сведения о реализуемых требованиях к защите персональных данных;
- Инструкции и регламенты для работников, работающих с персональными данными;
- Инструкции для работников, работающих со средствами криптографической защиты информации;
- Политика конфиденциальности официального сайта;
- иные локальные нормативные акты, регламентирующие порядок обеспечения безопасности персональных данных, учет и обращение с материальными носителями, действия при инцидентах и взаимодействие с субъектами персональных данных.

2.3 Все работники, непосредственно обрабатывающие персональные данные, под подпись ознакомлены с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами в области персональных данных, а также локальными актами Оператора. При изменении законодательных и иных нормативных актов Российской Федерации, а также локальных актов Оператора проводится своевременное уведомление работников. Ознакомление (в том числе в форме инструктажа по информационной безопасности) проводится в следующих случаях:

- при приёме на работу (первичный инструктаж) - до начала самостоятельной работы с ПДн;
- после каждого зафиксированного инцидента, связанного с нарушением безопасности персональных данных (повторный инструктаж по факту инцидента) – в течение 3 рабочих дней после завершения служебного расследования;
- не реже одного раза в год (плановый инструктаж) – для актуализации знаний по информационной безопасности.

Результаты каждого ознакомления (инструктажа) фиксируются в журнале проведения инструктажа по информационной безопасности с указанием даты, Ф.И.О. работника, его должности и подписи.

2.4 Согласия на обработку персональных данных оформляются в виде отдельных документов, содержащих все обязательные сведения, предусмотренные ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», и не объединяются с иными согласиями. Обработка персональных данных без согласия допускается в случаях, установленных ч. 2 ст. 6 настоящего Федерального закона.

2.5 На Сайте сбор персональных данных осуществляется посредством веб-форм с простановкой отметки о согласии в чек-боксе, формы согласий размещены на Сайте. При первом посещении Сайта отображается информационный баннер об использовании файлов cookie и аналитических сервисов, предоставляющий пользователю возможность принять обработку cookie путём нажатия кнопки «Принять» либо отказаться от неё, отключив cookie в настройках браузера.

2.6 От работников (в том числе медицинских работников) получены отдельные согласия на распространение их фотографий в случаях, предусмотренных законодательством РФ и локальными актами Оператора.

2.7 В Роскомнадзор подано уведомление о начале обработки персональных данных (регистрационный номер 11-0187221 от 24.03.2011). В случае изменения ранее представленных сведений (изменение целей, перечня обрабатываемых данных, места нахождения баз данных и т.д.) Оператор обязан уведомить Роскомнадзор не позднее 15 числа месяца, следующего за месяцем, в котором произошли такие изменения. Актуализация сведений в Реестре Операторов осуществляется своевременно.

2.8 Внутренний контроль соответствия обработки персональных данных требованиям законодательства осуществляется на регулярной основе (плановые проверки проводятся не реже одного раза в год, внеплановые – по факту инцидентов). Результаты оформляются актами.

2.9 Проведена оценка вреда, который может быть причинён субъектам персональных данных при нарушении законодательства.

2.10 Обеспечен доступ субъектов персональных данных к своим персональным данным. Субъект вправе получить информацию о своих обрабатываемых данных, а также требовать их уточнения, блокирования или уничтожения.

Для реализации своих прав субъект направляет в адрес оператора запрос (обращение), который может быть подан:

- в письменной форме на бумажном носителе (лично или почтовым отправлением);
- в форме электронного документа, подписанного электронной подписью в соответствии с законодательством Российской Федерации (например, через официальный сайт, по электронной почте или через систему электронного документооборота).

Срок рассмотрения:

- предоставление информации – 10 рабочих дней с даты получения запроса. Срок может быть продлен не более чем на 5 рабочих дней при направлении субъекту мотивированного уведомления с указанием причин продления (итого – до 15 рабочих дней);

— уточнение персональных данных и снятие блокирования – 7 рабочих дней со дня предоставления субъектом сведений, подтверждающих неточность данных;
— уничтожение персональных данных – 10 рабочих дней с даты выявления неправомерной обработки, если обеспечить правомерность обработки невозможно. В случае, когда данные являются незаконно полученными или не являются необходимыми для заявленных целей обработки, уничтожение производится в срок, не превышающий 7 рабочих дней со дня предоставления субъектом подтверждающих сведений.

2.11 Вопросы запрета на использование иностранных сервисов и программных средств написаны в рамках инструктажа при ознакомлении работников с локальными актами Оператора. Перечень запрещенных к использованию в рабочих целях иностранных сервисов и программных средств утвержден в соответствии с требованиями Департамента информационных технологий города Москвы и Комиссии по информационной безопасности при Мэре Москвы.

3. Права субъектов персональных данных и порядок обращения

3.1 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, а также вправе требовать уточнения, блокирования или уничтожения своих персональных данных в случаях, предусмотренных законодательством, и отозвать согласие на обработку.

3.2 Для реализации своих прав субъект направляет Оператору запрос (обращение) в письменной форме на бумажном носителе или в форме электронного документа, подписанного электронной подписью.

3.3 Порядок и сроки рассмотрения обращений субъектов персональных данных, а также перечень сведений, необходимых для идентификации субъекта, подробно описаны в Политике обработки персональных данных, размещённой на Сайте.

4. Меры по обеспечению безопасности персональных данных на официальном сайте

4.1 На Сайте ГБУЗ «ГКБ имени В.М. Буянова ДЗМ» в сети «Интернет» по адресу: https://gkb-buyanova.ru/ в открытом доступе размещена Политика обработки персональных данных, а также Политика конфиденциальности. Документы содержат полную информацию о целях, сроках, способах обработки, категориях субъектов и принимаемых мерах безопасности. Ссылки на документы являются кликабельными и ведут на страницы, доступные без регистрации всем посетителям Сайта.

4.2 Передача данных между сайтом и посетителем Сайта осуществляется по защищенному протоколу HTTPS с использованием действующего SSL/TLS-сертификата

4.3 Программное обеспечение сайта (система управления, все установленные модули и плагины) регулярно обновляется до актуальных версий. Обновления производятся ежемесячно, а критические обновления безопасности устанавливаются незамедлительно (в течение 24 часов с момента выхода).

4.4 Организовано ежедневное резервное копирование баз данных сайта, содержащих персональные данные. Резервные копии хранятся на серверах, расположенных на территории Российской Федерации.

4.5 Хостинг-провайдер обеспечивает фильтрацию трафика и защиту от кибератак.

4.6 На постоянной основе осуществляется мониторинг безопасности сайта: ежемесячно проводится сканирование на наличие вредоносного кода, уязвимостей и несанкционированных изменений с использованием специализированных программных средств.

4.7 На всех формах сбора персональных данных на Сайте предусмотрены чек-боксы для получения информированного согласия субъекта на обработку его персональных данных.

5. Технические меры защиты персональных данных в информационных системах Оператора

5.1 Организована система разграничения прав доступа работников к информационным системам, содержащим персональные данные. Доступ предоставляется строго в соответствии с должностными обязанностями. Пересмотр прав производится при каждой смене должности или увольнении работника. Только уполномоченные работники Оператора имеют доступ к базам данных с ПДн.

5.2 На всех рабочих станциях и серверах, задействованных в обработке ПДн, применяются антивирусные средства и СЗИ от НСД, сертифицированные ФСТЭК России.

5.3 При передаче персональных данных по открытым каналам связи (в том числе при удалённом доступе работников) применяются средства криптографической защиты данных в соответствии с требованиями ФСБ России (используются сертифицированные средства шифрования).

5.4 В ГБУЗ «ГКБ имени В.М. Буянова ДЗМ» организован и проводится внутренний контроль соответствия обработки персональных данных требованиям законодательства. Порядок, сроки и формы проведения внутреннего контроля регламентированы.

Плановые проверки проводятся не реже одного раза в год, внеплановые – по факту инцидентов или изменения законодательства РФ. Результаты проверок оформляются актами.

5.5 Обеспечена физическая защита помещений, в которых обрабатываются персональные данные: установлена система контроля доступа (электронные пропуска), ведётся видеонаблюдение, доступ посторонних лиц ограничен.

5.6 Уничтожение персональных данных осуществляется в соответствии с требованиями законодательства и локальным нормативным актом ГБУЗ «ГКБ имени В.М. Буянова ДЗМ». Сроки хранения документов, содержащих персональные данные, определяются номенклатурой дел учреждения, составленной на основе перечней типовых управленческих архивных документов, утверждённых Федеральным архивным агентством, и ведомственных перечней документов, образующихся в деятельности Министерства здравоохранения Российской Федерации и подведомственных организаций, с указанием сроков хранения. По факту уничтожения составляется акт, который хранится в течение 3 лет. Уничтожение производится способом, исключающим возможность восстановления информации (перезапись, физическое уничтожение носителя, сжигание или измельчение бумажных носителей).

5.7 При внедрении новых информационных технологий (искусственный интеллект, виртуализация, облачные вычисления, мобильные устройства, удалённый доступ и иные) разрабатываются и внедряются дополнительные организационные и технические меры защиты персональных данных в соответствии с актуальными требованиями ФСТЭК России. В случае выявления угроз безопасности персональных данных, для которых отсутствуют утверждённые меры защиты, разрабатываются компенсирующие меры. Оценка эффективности реализованных мер проводится перед началом обработки данных, не реже одного раза в 3 года, а также после каждого компьютерного инцидента.

5.8 В ГБУЗ «ГКБ имени В.М. Буянова ДЗМ» действует запрет на использование иностранных сервисов и программных средств, не имеющих подтверждения соответствия требованиям защиты информации (включая публичную электронную почту, интернет-мессенджеры, средства видео-конференц-связи и облачные хранилища), установленный требованиями ДИТ и ДЗМ города Москвы. Контроль за соблюдением запрета возложен на отдел ИТ и лицо, ответственное за организацию обработки персональных данных. В случае производственной необходимости использование альтернативных сервисов допускается только после проведения оценки их соответствия требованиям информационной безопасности.

6. Меры реагирования на инциденты и взаимодействие с контролирующими органами

6.1 Утвержден и действует порядок действий при выявлении фактов несанкционированного доступа к персональным данным или иных инцидентов безопасности.

6.2 В случае инцидента оперативно организуется уведомление субъектов персональных данных, Роскомнадзора, а также Департамента здравоохранения города Москвы в сроки, установленные законодательством.

6.3 По каждому зафиксированному инциденту проводится служебное расследование, разрабатываются и внедряются дополнительные меры по недопущению повторения подобных ситуаций. Результаты расследования оформляются актами и доводятся до всех заинтересованных лиц.

7. Меры по обеспечению безопасности баз данных персональных данных (исполнение ч. 5 ст. 18 Федерального закона № 152-ФЗ)

7.1 В соответствии с частью 5 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» категорически запрещается любое использование баз данных, находящихся за пределами территории Российской Федерации, для осуществления действий по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению) и извлечению персональных данных граждан Российской Федерации. Все указанные действия выполняются исключительно с использованием баз данных, физически размещённых на территории РФ. Нарушение данного запрета не допускается и влечёт ответственность в соответствии с законодательством.

7.2 Серверное оборудование (включая серверы, на которых размещён сайт организации, и серверы баз данных), используемое для обработки персональных данных граждан РФ, размещено на территории Российской Федерации.

7.3 Все информационные системы и программные средства, используемые для первичного сбора, записи, накопления и хранения персональных данных (включая CRM-системы, формы обратной связи на сайте, облачные сервисы, а также любые иные средства), должны использовать исключительно базы данных, расположенные на территории Российской Федерации. Использование любых иностранных облачных сервисов (в том числе Google Таблицы, зарубежные CRM, облачные хранилища и аналоги) для указанных целей строго запрещено. При внедрении новых программных средств обязательной проверке подлежит факт размещения используемых баз данных на территории РФ.

7.4 При использовании иностранных сервисов для целей, не связанных с первичным сбором, записью, накоплением и хранением ПДн, соблюдаются требования статьи 12 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» о трансграничной передаче персональных данных. О начале трансграничной передачи оператор обязан уведомить Роскомнадзор.

8. Заключительные положения

8.1 Все вышеуказанные меры введены в действие и выполняются на постоянной основе с момента их внедрения.

8.2 Контроль за актуальностью и эффективностью мер возложен на лицо, ответственное за организацию обработки персональных данных.

8.3 Настоящие Сведения являются действующим документом, подтверждающим выполнение Оператором требований законодательства о персональных данных, включая требования о локализации баз данных на территории Российской Федерации и своевременном уведомлении Роскомнадзора, размещён на Сайте ГБУЗ «ГКБ имени В.М. Буянова ДЗМ» по адресу в сети «Интернет»: https://gkb-buyanova.ru/normativnye-dokumenty/ в разделе «Правовые документы», доступен для ознакомления любому заинтересованному лицу без регистрации, а его актуальная версия поддерживается в соответствии с изменениями законодательства и внутренними регламентами.