КАК РОСКОМНАДЗОР ПРОВЕРЯЕТ РАБОТУ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Статья для справочника «Главный врач» изд-ва «Актион МФЦЭР».
Авторский вариант

Светлана Сергеевна Суворова,
канд. мед. наук, независимый эксперт по организации здравоохранения и управлению персоналом медицинских организаций, Москва

Штрафы за нарушения при обработке персональных данных доходят до 75 тыс. рублей. В рекомендации я рассмотрю, что проверяет Роскомнадзор, какие документы подготовить, какие права и обязанности закон установил для инспекторов и руководителей медорганизаций.

Что проверяет Роскомнадзор

Роскомнадзор проверяет, соблюдает ли медорганизация требования закона к обработке и защите персональных данных. Во внимании ведомства:

- документы, которые содержат персональные данные, условия их хранения, формы согласий на обработку;
- локальные нормативные акты по работе с персональными данными;
- системы обработки персональных данных (на бумажных и электронных носителях), информационные технологии и технические средства защиты;
- информационные таблички о видеонаблюдении, если оно ведется в организации.

Какие документы нужно подготовить к проверке

Задача юриста или главврача — задокументировать систему обработки персональных данных в организации. Перечислим, какие документы необходимы для проверки.

Уведомление об обработке персональных данных. Медицинская организация является оператором персональных данных. Она должна уведомить Роскомнадзор о факте обработки данных и получить номер в реестре операторов. Необходимо составить уведомление и направить его в ведомство.

Уведомление — документ установленной формы. Форма размещена на портале персональных данных (https://pd.rkn.gov.ru/operators-registry/notification/form/).

После его направления Роскомнадзор включает организацию в Реестр операторов персональных данных. Если организация включена в Реестр, она имеет право обрабатывать персональные данные. Если не включена — то может обрабатывать только те данные, обработка которых не требует уведомления.

Коммерческие медорганизации, работающие только по договору оказания медуслуг и использующие персональные данные только для его исполнения, могут не направлять уведомления на основании подпункта 2 части 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Обработка персональных данных, которые предоставляют работники при трудоустройстве, также не требует уведомления. Это следует из подпункта 1 части 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ.

Положение об обработке персональных данных. Это основной документ медорганизации. Положение включает:

1. Перечни должностных лиц с полным и ограниченным доступами к персональным данным. Для лиц, которым доступ ограничен – цели, для которых они могут использовать данные.
2. Правила доступа к персональным данным работников медучреждения и представителей сторонних организаций.
3. Правила предоставления данных третьих лиц и передачи персональных данных третьим лицам. Имеется в виду предоставление данных лица, не являющегося субъектом персональных данных (то есть чужих), или предоставление данных лицам или организациям, не являющимся оператором персональных данных, получившим согласие.
4. Правила регистрации и учета всех действий с персональными данными в информационной системе, описание базы персональных данных и информационных технологий, которые обеспечивают их обработку.
5. Правила хранения документов, которые содержат персональные данные.
6. Угрозы безопасности при обработке персональных данных на бумажных и электронных носителях, меры по преодолению этих угроз.

С положением должны быть ознакомлены все сотрудники медорганизации.

Важно! Работники, трудоустроенные в медорганизацию после утверждения Положения об обработке персональных данных, должны быть ознакомлены с ним до подписания трудового договора (подтверждается датой ознакомления). В противном случае административная ответственность по статье 5.27 КоАП РФ при проверке Инспекции труда.

Политика обработки персональных данных. Документ информирует третьих лиц о том, как в организации обрабатывают их персональные данные. Документ необходимо разместить на официальном сайте медорганизации и в бумажной версии в учреждении (п. 2 ст. 18.1 Закона о персональных данных).

Инструкция по заполнению документов, которые содержат персональные данные. Должна содержать информацию о заполнении разделов персональных данных в каждой из применяемых форм первичной медицинской документации.

Журналы учета. В организации должен быть журнал учета доступа к персональным данным, журнал учета выдачи персональных данных работников организациям и государственным органам, журнал регистрации однократного пропуска на территорию медорганизации. Не забудьте также подготовить журнал учета проверок.

Журнал однократного допуска ведется в произвольной форме, утвержденной приказом руководителя организации. Журнал учета проверок — по форме, утвержденной Приложением 4 к Приказу Министерства экономического развития РФ от 30 апреля 2009 г. N 141 "О реализации положений Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

Сертификаты на средства защиты информации. Необходимы сертификаты на антивирусные программы, системы видеонаблюдения, систему контроля и управления доступом (СКУД), криптографические системы, межсетевые экраны и пр.

Формы согласия на обработку персональных данных и соглашений о неразглашении. Разрабатывают отдельные формы согласия для работников, соискателей и пациентов. Параметры, которые необходимо включить в форму, указаны в п. 4 ст. 9 Закона о персональных данных.

Роскомнадзор проверяет оформленные согласия на всех работников и пациентов, а также соискателей, чьи персональные данные хранятся в кадровой службе в электронном виде и в видк запоненных анкет и резюме. Если в компьютере кадровика найдутся резюме соискателей, нужно будет доказать, что они получены из открытых источников. К этому времени соискатель уже может найти работу и удалить свое резюме с сайта рекрутеров. То же с бумажными анкетами.

Также ведомство проверяет соглашения о неразглашении персональных данных пациентов и работников. Медицинский персонал подписывает соглашение о неразглашении данных пациентов, кадровая служба ― о неразглашении данных работников, администрация — оба соглашения.

Что включает форма согласия

Согласие на обработку персональных данных включает фамилию, имя, отчество субъекта персональных данных, место жительства, паспортные данные. Если согласие подписывает законный представитель, указывают реквизиты доверенности или иного документа, который подтверждает полномочия представителя.

В согласии указывают наименование и адрес медорганизации, которая будет обрабатывать персональные данные, цель обработки, перечень данных, которые подлежат обработке и возможные действия с ними. Также должен быть указан срок, в течение которого действует согласие, и способ его отзыва. Согласие заверяется подписью (п. 4 ст. 9 Закона о персональных данных).

Совет

Не вывешивайте в помещениях медорганизации списки работников с указанием дней их рождения. Инспектор Роскомнадзора может запросить письменное согласие каждого из сотрудников на размещение этой информации в открытом доступе. При отсутствии хотя бы одного согласия медоганизацию оштрафуют.

Форма согласия на обработку биометрических данных. На обработку биометрических данных требуется отдельное согласие (ст. 11 Закона о персональных данных), его можно включить в основную форму.

К биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта (Разъяснения Роскомнадзора "О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки"). Если медорганизация эти данные не использует, можно согласие не брать. Но если инспектор проверит конкретные случаи, проверяемая организация должна быть готова показать, какова была цель обработки.

Согласие субъекта на трансграничную передачу данных. Данное согласие должно быть, если медорганизация передавала персональные данные в другие страны (ст. 12 Закона о персональных данных). Также необходимы документы, которые подтверждают, что

организация зашифровала эти данные и направила по защищенным каналам, в соответствии с ГОСТ 28147-89.

Документы по обработке специальных категорий персональных данных. Обработка таких данных, как расовая принадлежность, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь, не допускается, кроме как в ситуациях, предусмотренных законом. Конкретные ситуации могут быть связаны (п. 2 ст. 10 Закона о персональных данных):

- с решением вопросов о выделении социальной помощи или назначении пенсии;
- с защитой жизни, здоровья или жизненно важных интересов субъекта персональных данных или лица, которое не может предоставить свои персональные данные самостоятельно;
- с установлением и соблюдением прав субъекта персональных данных (третьих лиц), или в связи с осуществлением правосудия;
- с решением вопросов, связанных с усыновлением детей;
- с решением вопросов, связанных с предоставлением (или лишением) гражданства РФ;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

Если медорганизации приходилось обрабатывать такие данные, нужно подготовить документы, которые подтверждают, почему это было необходимо. Также обязательны документы, которые доказывают, что обработку прекратили сразу же, как только необходимость в этом отпала.

Другие документы. Если в Роскомнадзор поступали жалобы на нарушения в области обращения персональных данных, необходимы документы, которые опровергают или подтверждают (чтобы затем показать, что устранены все нарушения) изложенные в жалобе факты.

Если медорганизация получала предписание от Роскомнадзора, необходимы документы, которые подтверждают, что организация устранила нарушения в назначенный срок.

Для проверки подготовьте также акты уничтожения персональных данных, если истек срок их хранения или если пациент отозвал свои данные.

Какие документы должен предъявить инспектор

При выездной проверке инспектор предъявляет руководителю медорганизации или его уполномоченному представителю копию приказа о проверке и служебное удостоверение проверяющего.

В приказе Роскомнадзор указывает фамилии, имена, отчества, должности инспекторов, наименование медорганизации и ее адрес, цели, задачи, основания проверки, перечень документов для проверки, виды и объемы мероприятий по контролю, сроки и условия проверки. На приказе должна стоять печать территориального подразделения Роскомнадзора, которое проводит проверку.

Если в приказе есть ошибки (например, название медорганизации указано неверно), руководитель вправе инспектора в учреждение не допускать.

Проверяющим может быть только тот человек, чьи фамилия, имя и отчество указаны в приказе. В случае сомнений руководитель медорганизации (или его уполномоченный) вправе потребовать у проверяющего предъявить паспорт. Если состав должностных лиц изменился, у инспектора должен быть приказ, который подтверждает изменения.

Совет

Если сомневаетесь в подлинности документов, которые предъявил инспектор, или подозреваете, что документы неправильно оформлены, обратитесь в территориальное подразделение Роскомнадзора. Также можно обратиться в центральную справочную Роскомнадзора по вопросам проверок − телефон: +7 (495) 987-68-00, электронный адрес: rsoc_in@rsoc.ru.

Проверка без приказа Роскомнадзора — грубое нарушение требований закона (ч. 4 п. 2 ст. 20 Федерального закона от 26.12.2008 № 294-ФЗ). Результаты такой проверки недействительны. Чтобы их отменить, обратитесь в вышестоящий орган госнадзора или в суд.

Важно! Вы можете ознакомиться с регламентом проверки до ее начала. Потребуйте регламент у инспектора или обратитесь в Роскомнадзор с заявлением.

Ситуация. Возможна ли проверка, если руководителя медорганизации нет на работе?

Инспекторы не вправе проводить проверку в отсутствие руководителя (исключение — проверку проводят из-за подозрения на то, что гражданам причинен вред жизни или здоровью).

Сколько продолжается проверка, за какой срок о ней уведомляют руководителя?

Роскомнадзор направляет уведомление о документарной проверке не позднее, чем за 3 рабочих дня до ее начала.

Все проверки начинаются как документарные. Выездная проверка — это продолжение документарной. При возникновении необходимости проведения выездной проверки инспектор предъявляет приказ о переходе документарной проверки в выездную. В уведомлении он указывает дату начала и окончания проверки. Проводить проверку вне этого интервала инспектор не вправе, если нет приказа о продлении или переносе срока.

Уведомление о проведении внеплановой проверки направляется не позднее, чем за 24 часа до начала ее проведения.

Документы для документарной проверки медорганизация предоставляет в течение 10 рабочих дней.

Общая продолжительность как документарной, так и выездной проверки — не более 20 рабочих дней. Роскомнадзор может продлить срок выездной проверки, если есть на это обоснованная причина — например, требуется экспертиза. Но продлить срок можно не более, чем на 20 рабочих дней.

Руководитель Роскомнадзора вправе приказом приостановить проверку не более, чем на 10 рабочих дней. Приостанавливать проверку повторно он уже не может.

Какие полномочия закон установил для инспектора Роскомнадзора

Инспектор вправе:

- проводить проверки в установленном порядке и при наличии документов беспрепятственно в любое время суток;
- запрашивать и безвозмездно получать от работодателей документы, объяснения, информацию, которые необходимы для проверки;

- получать доступ к информационным системам персональных данных в режиме просмотра;
- предъявлять предписания об устранении нарушений;
- приостанавливать или прекращать обработку персональных данных, если медорганизация проводит ее с нарушением законодательства;
- требовать уточнить, блокировать или уничтожить недостоверные или полученные незаконным путем персональные данные;
- привлекать к проверке экспертов и экспертные организации.

Инспектор не вправе:

- проверять то, что не относится к полномочиям Роскомнадзора;
- проводить выездную проверку в отсутствие руководителя или его уполномоченного представителя (исключение — проверка по основанию «причинение вреда жизни или здоровью граждан»);
- требовать документы, информацию, которые не относятся к предмету проверки, изымать оригиналы этих документов;
- нарушать сроки проверки;
- выдавать предписания или предложения о проведении проверок на коммерческой основе;
- распространять информацию, которая составляет государственную, коммерческую, служебную, иную охраняемую законом тайну, за исключением случаев, которые предусмотрены законодательством.

Отнесение той или иной информации к государственной тайне определяется законодательством о гостайне; если такая информация в организации имеется, руководитель всегда в курсе и соответствующие локальные нормативные акты приняты. Что относится к коммерческой или служебной тайне, организации определяют самостоятельно, и руководитель издает локальные нормативные акты, с которыми знакомятся все причастные сотрудники.

Какие права и обязанности у руководителя медорганизации

Руководитель медорганизации вправе:

- присутствовать при проверке, давать объяснения по вопросам, которые относятся к предмету проверки;
- получать от инспектора информацию, которая относится к предмету проверки;
- знакомиться с результатами проверки;
- указывать в акте проверки о своем ознакомлении, согласии или несогласии с результатами проверки, а также с действиями инспекторов;
- обжаловать в административном или судебном порядке действия инспекторов, заявлять о нарушении прав медорганизации при проверке.

Руководитель медорганизации обязан:

- предоставить инспектору в полном объеме информацию и документы, которые связаны с целями, задачами и предметом проверки;
- обеспечить доступ инспектора, а также привлеченных экспертов на территорию, в помещения, к оборудованию, где обрабатываются персональные данные;

- обеспечить присутствие при проверке руководителя или уполномоченного лица (или присутствовать самому, или заблаговременно уполномочить приказом кого-то из подчиненных);
- предоставить инспектору журнал учета проверок по типовой форме, которая установлена приказом Миниэкономиразвития России от 30.04.2009 № 141.

Как инспектор должен оформить результаты проверки

По результатам проверки инспектор составляет акт. Один из экземпляров акта он вручает руководителю медорганизации. Если инспектор не предоставил акт руководителю, то результаты проверки можно признать недействительными (ч. 4 п. 2 ст. 20 Федерального закона от 26.12.2008 № 294-ФЗ).

Что должно быть указано в акте проверки?

1. Установленные в ходе проверки факты соответствия или несоответствия методов обработки и способов хранения персональных данных действующему законодательству в области работы с персональными данными.
2. Подробные сведения о выявленных нарушениях обязательных требований в сфере работы с персональными данными.
3. Имевшие место случаи неповиновения законному распоряжению или требованию инспектору Роскомнадзора, а также воспрепятствования осуществлению им своих служебных обязанностей (если такие случаи были).
4. Если в ходе проверки выявленное нарушение было устранено, об этом делается запись в акте проверки.
5. Имевшие место случаи неповиновения законному распоряжению или требованию инспектору Роскомнадзора, а также воспрепятствования осуществлению им своих служебных обязанностей (если такие случаи были).

Совет

Если инспектор выявил нарушение, в акте проверки он обязан указать статью нормативного акта. Когда инспектор даст вам ознакомиться с актом проверки, откройте соответствующую статью документа в Интернете и проверьте, действительно ли этот факт является нарушением и какая ответственность за него предусмотрена.

Если ссылки на законодательство в акте проверки нет, вы вправе потребовать от инспектора включить ее в документ.

К сведению

Не торопитесь подписывать акт. Если у вас есть замечания и возражения, или вы обнаружили несоответствия, требуйте, чтобы инспектор внес их в акт, или оформите как приложение к акту. Подписывайте документ, только когда инспектор выполнил все ваши требования. После подписи вносить какие-либо изменения в акт запрещено, поэтому ваши замечания не учтут и доказать свою правоту вам будет сложнее.

Если в результате проверки инспектор выявил нарушения, то вместе с актом проверки он выдает руководителю предписание об устранении нарушения.

Если нарушения влекут административную ответственность (или уголовную — например, нарушение неприкосновенности частной жизни; УК РФ, ст. 137), инспектор вправе составить протокол. Протокол передается в правоохранительные органы (прокуратуру, органы

дознания, суд) и возбуждается административное или уголовное дело. И уже по результатам рассмотрения этого дела в суде накладывается ответственность.