Готовое решение: Какие меры по защите персональных данных работников должны приниматься при обработке этих данных (КонсультантПлюс, 2025)

КонсультантПлюс | Готовое решение | **Актуально на 22.01.2025**

Примечание: См. расширенную версию Готового решения.

Какие меры по защите персональных данных работников должны приниматься при обработке этих данных

Перечень мер по защите персональных данных, которые должны приниматься вами при обработке этих данных, законом не ограничен.
Как правило, к таким мерам относятся: создание специального комплекта документов (в частности, приказа о назначении ответственного за организацию обработки персональных данных, локального нормативного акта о защите персональных данных), особый режим использования и хранения персональных данных на бумажных носителях.
Также, если вы обрабатываете и храните персональные данные в электронном виде, вам нужно принять особенные организационные и технические меры, в частности определить тип угроз безопасности и подобрать соответствующий этому типу уровень защищенности. От этого уровня защищенности зависит, какие меры защиты персональных данных вам нужно принять. Для этого можете привлечь специалиста в этой области, чтобы избежать ошибок при организации таких специальных мер.
Меры по защите персональных данных вы разрабатываете сами совместно с работниками и их представителями.

Оглавление:

1. Какой комплект документов нужно создать для защиты персональных данных работников при обработке этих данных

Для защиты персональных данных работников создайте комплект следующих основных документов:

1) приказ о назначении лица, ответственного за организацию обработки персональных данных в организации (п. 1 ч. 1 ст. 18.1, ч. 1 ст. 22.1 Закона о персональных данных).

   Таким лицом может быть любой работник вашей организации, например специалист отдела по управлению персоналом. Главное, чтобы он смог выполнять обязанности, перечисленные в ч. 4 ст. 22.1 Закона о персональных данных.

   Например, он должен доводить до сведения работников положения законодательства о персональных данных, а также ваших локальных актов об обработке персональных данных (п. 2 ч. 4 ст. 22.1 Закона о персональных данных);

2) положение о защите персональных данных работников или иной локальный нормативный акт, регулирующий порядок хранения, использования, обработки таких данных. Учтите требования и ограничения к содержанию такого документа. В нем не должно быть положений, ограничивающих права работников, а также возлагающих на вас полномочия и обязанности, не предусмотренные законом (ст. 87 ТК РФ, п. 2 ч. 1 ст. 18.1 Закона о персональных данных);

    Образец положения об обработке и защите персональных данных работников (иных лиц)

3) политика в отношении обработки персональных данных. Этот документ также не должен

содержать указанных ограничений и возлагать не предусмотренные законом полномочия и обязанности (п. 2 ч. 1 ст. 18.1 Закона о персональных данных);

Образец политики оператора в отношении обработки персональных данных

4) приказ об утверждении перечня лиц, которые отвечают за обработку персональных данных работников (абз. 6 ст. 88 ТК РФ).

Ответственных за обработку персональных данных назначьте приказом. Помимо прочего определите в нем, с какой информацией работает конкретное лицо (группа лиц). Доступ ограничьте теми персональными данными, которые необходимы для выполнения конкретных функций (ст. 88 ТК РФ).

Рекомендуем у всех этих лиц взять письменное обязательство о неразглашении (соблюдении конфиденциальности) персональных данных, учитывая абз. 4 ст. 88 ТК РФ, ч. 3 ст. 6 Закона о персональных данных.

Образец обязательства о неразглашении персональных данных работников

Вы можете включить в этот комплект и другие необходимые для вас документы. Например, это могут быть журналы учета персональных данных, их выдачи и передачи другим лицам, представителям сторонних организаций и государственным органам. Кроме того, вы можете разработать форму согласия на обработку персональных данных. Такое письменное согласие требуется получать от работников (за исключением некоторых случаев) для обработки их персональных данных, включая передачу третьим лицам (п. 1 ч. 1 ст. 6, абз. 1 ч. 4 ст. 9 Закона о персональных данных, Разъяснения Роскомнадзора).

Образец согласия работника на обработку персональных данных

Образец согласия работника на обработку персональных данных, разрешенных им для распространения

Образец согласия работника на передачу его персональных данных третьей стороне

Если речь идет о защите информации ограниченного доступа, не составляющей гостайну, объекты информатизации (например, государственные информационные системы персональных данных) подлежат аттестации на соответствие требованиям по защите такой информации. Состав и содержание работ по аттестации, а также требования к форме и содержанию разрабатываемых при организации и проведении таких работ документов определены Порядком, утвержденным Приказом ФСТЭК России от 29.04.2021 N 77.

См. также: Нужно ли получать согласие работника на обработку персональных данных

2. Как организовать защиту персональных данных работников при обработке этих данных, если они хранятся на бумажных носителях

Требования к организации защиты персональных данных на бумажных носителях подробно не описаны в законе. Ключевое требование закона - вы должны принимать необходимые правовые, организационные и технические меры для защиты персональных данных работников от неправомерного использования или утраты либо обеспечить принятие таких мер (п. 7 ст. 86 ТК РФ, ч. 1 ст. 19 Закона о персональных данных).

Поэтому мы рекомендуем, в частности, следующее:

1) хранить персональные данные на бумажных носителях в специальных помещениях. Учитывайте, что нужно раздельно хранить персональные данные (материальные носители), которые обрабатываются в разных целях (п. 14 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации);

2) организовать особый режим доступа в эти помещения, в частности утвердить перечень лиц, имеющих доступ в данные помещения, с учетом требований п. 13 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации;

3) организовать охрану таких помещений, например оборудовать их сигнализацией, металлическими самозакрывающимися дверьми, решетками на окнах.

Обратите внимание, что в некоторых случаях обязательно хранить персональные данные в железных шкафах. Например, в таких шкафах должны храниться документы воинского учета, содержащие персональные данные работников (п. 21 Методических рекомендаций по ведению воинского учета в организациях).

3. Как организовать защиту персональных данных работников при обработке этих данных, если они хранятся в электронном виде

Организовать защиту персональных данных, которые хранятся в информационных системах, непросто. Основное требование закона - вы должны принимать необходимые правовые, организационные и технические меры для защиты персональных данных работников от неправомерного использования или утраты либо обеспечить принятие этих мер (п. 7 ст. 86 ТК РФ, ч. 1 ст. 19 Закона о персональных данных).

Но есть множество уточнений, которые прописаны в Приказе ФСТЭК России от 18.02.2013 N 21 и Приказе ФСБ России от 10.07.2014 N 378.

Поэтому можете привлечь специализированную организацию или ИП, у которых есть лицензия на деятельность по технической защите конфиденциальной информации (п. 2 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных).

В частности, для защиты персональных данных потребуется:

1) определить, какой у вас тип угрозы безопасности персональных данных (п. 7 Требований к защите персональных данных при их обработке в информационных системах);

2) подобрать один из четырех уровней защиты персональных данных, исходя из вашего типа угрозы, в соответствии с п. п. 8 - 16 Требований к защите персональных данных при их обработке в информационных системах.

Именно от этого и будет зависеть комплекс мер.

Например, если по итогам определения типа угрозы специалист предложит вам обеспечить минимальный (четвертый) уровень защищенности персональных данных работников, вам потребуется (п. 13 Требований к защите персональных данных при их обработке в информационных системах):

- обезопасить помещения, в которых размещена информационная система, от неконтролируемого проникновения или неправомерного доступа;
- обеспечить сохранность носителей персональных данных;
- утвердить перечень лиц, имеющих в силу трудовых обязанностей доступ к персональным данным в информационной системе;
- защитить информацию с помощью средств, прошедших процедуру оценки соответствия (в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз).

Кроме того, вы обязаны взаимодействовать с госсистемой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. В частности, потребуется уведомлять о компьютерных инцидентах, из-за которых персональные данные неправомерно переданы (предоставлены, распространены и т.д.) (ч. 12 ст. 19 Закона о персональных данных). При этом руководствуйтесь Порядком взаимодействия, утвержденным Приказом ФСБ России от 13.02.2023 N 77.

4. Что делать, если персональные данные работников неправомерно или случайно переданы (предоставлены, распространены и т.д.)

Если передача данных привела к нарушению прав работников, вы обязаны в течение 24 часов с момента ее выявления уведомить Роскомнадзор (п. 1 ч. 3.1 ст. 21 Закона о персональных данных):

- об инциденте и его предполагаемых причинах;
- возможном вреде, причиненном правам работников;
- принятых мерах по устранению последствий инцидента;

- лице, которое вы уполномочили взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

По выявленному факту вы обязаны провести внутреннее расследование. О его результатах нужно уведомить Роскомнадзор в течение 72 часов с момента обнаружения передачи данных. Кроме того, надо предоставить сведения о лицах, из-за которых произошел инцидент (если такие есть) (п. 2 ч. 3.1 ст. 21 Закона о персональных данных).

Порядок и условия взаимодействия Роскомнадзора с операторами в рамках ведения реестра учета инцидентов в области персональных данных утверждены Приказом Роскомнадзора от 14.11.2022 N 187. Документом, в частности, установлены требования к содержанию первичного и дополнительного уведомлений (п. п. 2 - 3 указанного Порядка).

Отдельные операторы, например субъекты критической информационной инфраструктуры, обязаны направлять информацию о компьютерных инцидентах, руководствуясь п. 2 Порядка взаимодействия, утвержденного Приказом ФСБ России от 13.02.2023 N 77. Такие операторы вправе обратиться в НКЦКИ за содействием в реагировании на выявленный компьютерный инцидент (п. 5 названного Порядка).

5. Какие риски возможны, если не будут приняты меры по защите персональных данных работников при обработке этих данных

В таком случае возможны следующие риски, в частности:

- административная ответственность, например, за необеспечение сохранности персональных данных при их неавтоматизированной обработке, если это повлекло неправомерный или случайный доступ к ним, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия и нет признаков уголовно наказуемого деяния. Так, для должностного лица штраф составит от 8 тыс. до 20 тыс. руб. (ч. 6 ст. 13.11 КоАП РФ);

- уголовная ответственность, например, за незаконное использование и (или) передачу (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации с персональными данными, полученной незаконным путем. Виновному грозит ответственность вплоть до лишения свободы (ч. 1, 2 ст. 272.1 УК РФ).