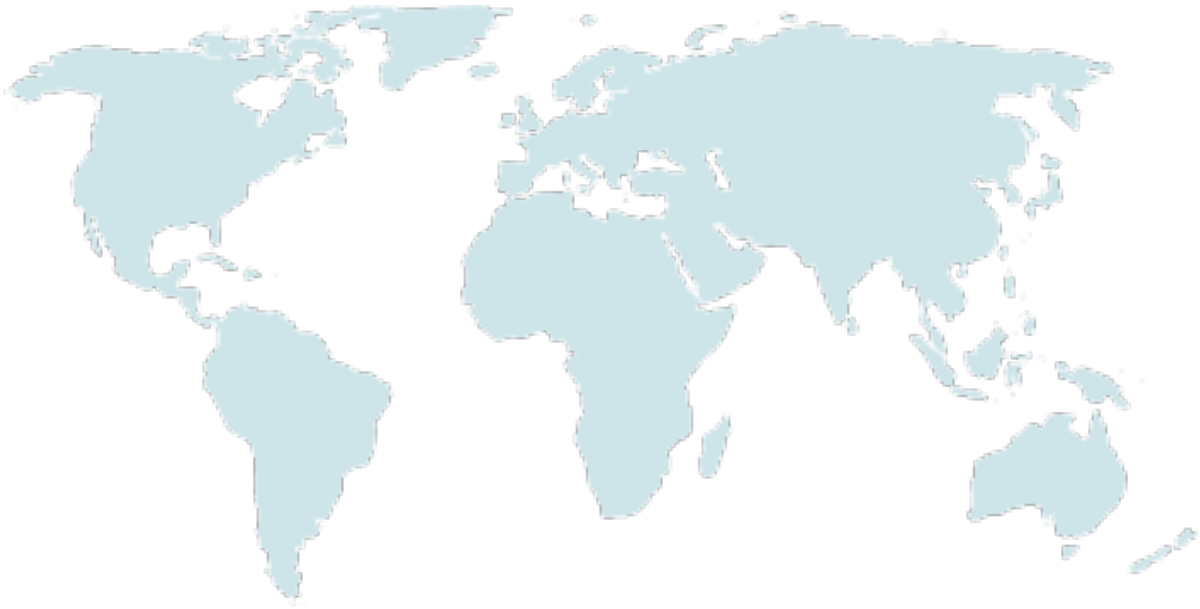
ICNL

www.icnl.org
info@icnl.org

ОБЗОР

Практическое руководство по персональным данным для организаций гражданского общества Кыргызстана



Предоставленная в руководстве информация носит исключительно общий справочный и образовательный характер. Она не предназначена и не должна рассматриваться как юридическая консультация. Содержащееся в документе не должно использоваться или применяться без получения юридической консультации, основанной на конкретных фактах и обстоятельствах, и не должно толковаться иным образом.

INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

1660 L Street NW #600
Washington, DC, 20036

Оглавление

Краткий обзор требований к защите данных 4

Что такое персональные данные? 5

Что такое специальные категории персональных данных и как с ними обращаться? 6

Что такое обработка персональных данных? 8

Кто обязан соблюдать Закон о персональной информации? 9

Какие виды обработки данных не входят в сферу действия Закона? 10

Основные принципы защиты персональных данных? 11

Когда необходимо получить согласие на сбор или использование персональных данных 13

Как получить согласие на сбор и обработку персональных данных 13

Контрольный список (чек-лист) по выполнению требований к получению согласия 14

Трансграничная передача персональных данных: что это означает и как соблюдать требования Закона 16

Когда персональные данные являются конфиденциальными и когда они могут быть обнародованы? 18

Какие ещё обязанности возникают у держателя (обладателя) массива персональных данных и у обработчика данных? 19

Нужно ли регистрироваться в качестве держателя персональных данных? Как это сделать? 20

Кто обеспечивает исполнение закона? 22

Какие штрафы предусмотрены за нарушение законодательства о персональных данных? 24

Нормативные правовые акты 28

Настоящее руководство подготовлено для организаций гражданского общества (ОГО) в Кыргызстане, которые в своей работе собирают, хранят или используют персональные данные. Распространённые примеры включают регистрацию участников мероприятий, ведение списков электронных адресов для рассылок, хранение кадровых документов или предоставление отчётов донорам. Это лишь некоторые примеры. Обработка персональных данных может принимать множество других форм. Если ваша организация так или иначе работает с персональными данными, вы обязаны соблюдать закон. Настоящее руководство объясняет требования закона простым языком и предлагает практические шаги, примеры и контрольные списки (чек-листы), которые помогут ОГО выполнить свои обязательства.

Законодательство Кыргызстана в сфере персональных данных находится в процессе реформирования:

- Закон Кыргызской Республики «Об информации персонального характера» (далее – Закон о персональной информации), принятый в 2008 году, продолжает устанавливать основные правила обращения с персональными данными и будет действовать до 8 февраля 2026 года.
- Одновременно, 19 мая 2025 года были приняты поправки в Кодекс Кыргызской Республики о правонарушениях, которые вводят штрафы за широкий круг нарушений требований по защите персональных данных. Эти положения вступят в силу 23 ноября 2025 года.
- 31 июля 2025 года Президент подписал новый Цифровой кодекс, который модернизирует правила защиты данных и отменяет обязанность организаций регистрироваться в качестве обладателей массивов персональных данных. Цифровой кодекс вступит в силу 8 февраля 2026 года. С момента вступления кодекса в силу Закон о персональной информации утратит силу.

Таким образом, возникает короткий, но важный переходный период между 23 ноября 2025 года и 8 февраля 2026 года, когда требования Закона о персональной информации продолжают действовать, и организации могут быть оштрафованы за нарушения, включая обработку персональных данных без надлежащей регистрации. Поэтому ОГО должны выполнять требования действующего закона, одновременно готовясь к новому правовому режиму, который начнёт применяться с февраля 2026 года. В целях поддержки ОГО в этот период ICNL подготовил данное руководство. Позднее будет выпущен обновлённый ресурс, который поможет организациям адаптироваться к требованиям Цифрового кодекса о защите персональных данных.

Соблюдение правил защиты персональных данных важно не только для того, чтобы избежать штрафов, но и для защиты и уважения права на частную жизнь, защиты бенефициаров от возможного вреда и укрепления доверия между сообществами, донорами и партнёрами. Ответственное обращение с персональными данными демонстрирует профессионализм, укрепит репутацию вашей организации и поможет гарантировать, что ваша деятельность не нанесет непреднамеренного ущерба вашим партнерам и бенефициарам.

Краткий обзор требований к защите данных

- √ **Определите, какие персональные данные вы обрабатываете**. К ним относятся имена, контактные данные, номера удостоверений личности/паспортов, фотографии, видео, адреса электронной почты и аналогичная информация. Специальные категории персональных данных (такие как религия, этническая принадлежность, состояние здоровья, сексуальная ориентация или политические взгляды) требуют особой осторожности. Сбор и использование специальных данных, как правило, запрещены, если только для этого нет веских оснований.
- √ **Определите законное основание для обработки данных**. В большинстве случаев для деятельности ОГО таким основанием будет согласие. Объясняйте ясно и открыто, зачем вы собираете данные и как они будут использоваться.
- √ **Собирайте и документируйте согласие надлежащим образом**. Согласие может быть в письменной или электронной форме. Для каждой цели (например, рассылка новостей, публикация фотографии, обмен данными с донорами) требуется отдельное согласие. Человек может отозвать своё согласие в любое время. В согласии должно быть чётко указано:
  - Кто собирает данные (ваша ОГО)
  - Какие данные собираются
  - Почему они собираются
  - Как они будут использоваться
  - Кому данные будут переданы (конкретные третьи лица)
  - Как долго они будут храниться
- √ **Применяйте основные принципы защиты данных:**
  - Собирайте только те данные, которые действительно необходимы.
  - Обеспечивайте безопасность данных (пароли, контроль доступа, запертые шкафы).

- Храните данные столько, сколько необходимо, затем надежно уничтожайте.
- Не объединяйте и не используйте данные для других целей без законного основания или нового согласия.
- Соблюдайте конфиденциальность, если данные не анонимизированы или человек не дал согласие сделать их публичными.

√ **Будьте осторожны при трансграничной передаче данных**. Использование таких инструментов, как Google Формы, облачное хранилище или отправка списков участников донорам за границу, считается передачей данных за пределы Кыргызстана. До опубликования официального списка стран с «надлежащим уровнем защиты» всегда получайте информированное согласие перед передачей персональных данных за границу.

Что такое персональные данные?

> Статья 3 Закона о персональной информации

Персональная информация (или персональные данные) — это любая информация о человеке, которая может быть использована для его прямой или косвенной идентификации. К ней относятся имена, адреса, номера паспортов и удостоверений личности, видеозаписи или голосовые записи, фотографии, отпечатки пальцев, адреса электронной почты, IP-адреса *(уникальные номера, связанные с устройствами, такими как компьютеры и мобильные телефоны, подключающимися к Интернету)*, генетические данные и любые другие данные, относящиеся к конкретному человеку. Эта информация может быть:

- одним фрагментом данных, который напрямую указывает на человека, или
- несколькими фрагментами данных, которые в совокупности позволяют установить личность человека.

Если информация позволяет идентифицировать конкретного человека, она считается персональными данными и охраняется законом. Однако, если данные «обезличены», они перестают считаться персональными данными. Обезличивание означает полное удаление и стирание всей идентифицирующей информации. Шифрование персональных данных или кодирование и раздельное хранение различных фрагментов данных не считается полной деперсонализацией. Лица, которые могут быть идентифицированы в массивах персональных данных, называются **субъектами персональных данных**. Закон

предоставляет субъектам определённые права в отношении их персональных данных.

ПРИМЕР

В организации Гражданская инициатива «Бирге» (далее – Инициатива «Бирге») работает 15 сотрудников. Организация собирает и хранит для каждого сотрудника полное имя, номер идентификационного налогового номера, дату рождения, домашний адрес, номер телефона, а также имя и номер телефона члена семьи для экстренной связи. Организация также работает с волонтерами по субботам утром. Приходя, волонтеры регистрируются, а уходя – отписываются. В конце дня подсчитывается количество прибывших волонтеров и общее количество отработанных ими часов. Лист регистрации уничтожается и выбрасывается.

Это персональные данные?

Данные о сотрудниках: Да. Информация в личных делах сотрудников позволяет однозначно идентифицировать каждого сотрудника (имена, контактные данные, идентификационные номера и т. д.). Это персональные данные, и Инициатива «Бирге» обязана соблюдать закон о защите персональных данных при их сборе, хранении и использовании.

Статистика по волонтёрам: Нет. Итоговая цифра «15 волонтёров отработали в общей сложности 45 часов» не идентифицирует никого лично. Поскольку данные были обезличены, требования к защите данных не применяется.

Что такое специальные категории персональных данных и как с ними обращаться?

> Статья 8 Закона о персональной информации

Некоторые виды персональных данных относятся к специальным категориям данных и требуют особой защиты. Их сбор и использование, как правило, запрещены, за исключением случаев, когда на то есть веские основания. К ним относятся данные, раскрывающие расовую или этническую принадлежность человека, его национальность, политические взгляды, религиозные или философские убеждения, состояние здоровья, сексуальную ориентацию. Важно отметить, что закон запрещает сбор и использование этих данных исключительно в целях определения этих характеристик.

ОГО могут обрабатывать такие данные только в двух случаях:

- С явного согласия человека. Пример: бенефициар письменно соглашается предоставить свою историю болезни для участия в медицинском проекте.

- В целях экстренной защиты здоровья или безопасности, когда согласие получить невозможно. Пример: в экстренной ситуации (например, при ухудшении здоровья на мероприятии) организация передаёт врачу информацию о состоянии здоровья человека для спасения его жизни.

Сбор и публикация информации о политической, религиозной, этнической или сексуальной идентичности человека без его разрешения противозаконны. Даже если человек принадлежит к уязвимой группе, которую поддерживает ваш проект (например, люди с ВИЧ, жертвы насилия, представители этнических меньшинств), вы не должны собирать и раскрывать эту информацию без его свободного осознанного согласия или без крайней необходимости для защиты жизни или безопасности человека.

НА ЗАМЕТКУ ОГО

√ Всегда задавайте себе вопрос: действительно ли нам нужны эти чувствительные сведения для достижения цели? Если нет — не собирайте их.

√ Если вам это действительно необходимо, убедитесь, что у вас есть четкое письменное согласие и приняты надежные меры безопасности хранения этих сведений.

√ Помните: защита конфиденциальных данных — это не только юридическая обязанность, но и этическая ответственность перед вашими бенефициарами.

ПРИМЕР

Политика Инициативы «Бирге» гласит, что любой сотрудник, принадлежащий к религиозному меньшинству, может взять отпуск для соблюдения религиозных праздников и обрядов. Чтобы воспользоваться этой возможностью, сотрудник должен отправить электронное письмо директору организации с просьбой о разрешении, в котором содержится информация о религии, религиозном празднике и причинах, по которым отпуск необходим для соблюдения этого праздника. Это электронное письмо затем сохраняется в личном деле сотрудника.

Следует ли Инициативе «Бирге» изменить порядок фиксации таких запросов на отпуск?

Да, организации следует изменить свои процедуры. Информация о религиозной принадлежности сотрудника относится к специальным категориям персональных данных, и её сбор или хранение создаёт правовые риски. Требование указывать религию и религиозные праздники приводит к ненужному сбору чувствительных данных.

Какие другие процедуры может внедрить Инициатива «Бирге», чтобы избежать сбора специальных категорий данных?

Организация может обновить политику так, чтобы сотрудники указывали только «отпуск по личным причинам» или «отпуск в связи с религиозным обрядом» без уточнения религии или конкретного праздника. В личных делах можно фиксировать лишь даты отпуска и его вид (ежегодный, неоплачиваемый, специальный и т. д.), не сохраняя данных, раскрывающих религиозные убеждения. Таким образом, сотрудники сохранят свои права и льготы, а организация избежит рисков, связанных с обработкой специальных категорий персональных данных.

Что такое обработка персональных данных?

> Статья 3 Закона о персональной информации

Обработка персональных данных — это широкое понятие. Оно включает любые действия с персональными данными, независимо от того, выполняются ли они вручную или с использованием компьютера. Обработка охватывает весь жизненный цикл персональных данных — от момента их сбора до хранения, обновления или уничтожения.

ПРИМЕР

Ваша организация обрабатывает персональные данные, когда вы:

- собираете имена и контактные данные при регистрации участников мероприятия;
- храните сканированные копии паспортов для организации поездок;
- обновляете список рассылки, добавляя новые адреса электронной почты или номера телефонов;
- группируете бенефициаров по возрасту, полу или региону для отчёта по проекту;
- ограничиваете доступ к конфиденциальным файлам с помощью паролей;
- удаляете устаревшие регистрационные формы участников;
- уничтожаете старые бумажные документы с персональными данными.

Если ваша организация осуществляет какую-либо из вышеперечисленных (или иную аналогичную деятельность), вы обрабатываете персональные данные и должны соблюдать правила, предусмотренные законом.

Кто обязан соблюдать Закон о персональной информации?

> Статья 3 Закона о персональной информации

Держатель (обладатель) массива персональных данных — это организация, которая осуществляет руководство и контроль за обработкой персональной информации. Держатель определяет для каких целей собираются сведения, какие именно сведения подлежат сбору, как они будут использоваться и защищаться. Если ваша ОГО собирает персональную информацию для своей деятельности (например, для проекта, мероприятия или оказания услуги), значит, именно ваша организация является держателем (обладателем) массива персональных данных. Вы несёте ответственность за то, чтобы сведения использовались законно и безопасно.

Обработчик персональной информации — это лицо или организация, которые помогают вам обрабатывать персональную информацию, но делают это исключительно на основании договора и в соответствии с вашими указаниями. Это может быть IT-компания, которая ведёт вашу базу данных, консультант, который анализирует результаты опроса, или типография, которая печатает именные сертификаты для бенефициаров. Обработчик не принимает решений о том, что делать с персональной информацией, а действует строго по поручению держателя (обладателя) массива персональных данных.

ПРИМЕР

Инициатива «Бирге» реализует программу обучения для молодёжи и собирает имена и адреса электронной почты участников для целей мониторинга и отчётности. Для организации программы она нанимает ивент-агентство, которое ведёт регистрацию участников у входа в зал. После тренинга Инициатива «Бирге» использует онлайн-сервис для сбора отзывов участников. Этот сервис предоставляется бесплатно, но у Инициативы «Бирге» есть учётная запись на платформе, что позволяет ей пользоваться услугой.

Является ли Инициатива «Бирге» держателем (обладателем) или обработчиком данных? Почему?

Инициатива «Бирге» является держателем (обладателем) массива персональных данных. Она решила собирать сведения, определила, как именно они будут использоваться, и установила, какие данные подлежат сбору.

Является ли ивент-агентство держателем (обладателем) или обработчиком данных? Почему?

Ивент-агентство является обработчиком. Оно работает от имени Инициативы «Бирге» и действует в соответствии с её указаниями о том, какие сведения собирать и как.

Является ли онлайн-платформа для опросов держателем (обладателем) или обработчиком данных? Почему?

В данном случае онлайн-платформа выступает как обработчик. Несмотря на то, что услуга предоставляется бесплатно, платформа всё равно собирает и хранит сведения от имени Инициативы «Бирге». При этом сама платформа, скорее всего, является держателем (обладателем) массива персональных данных в отношении имени, адреса электронной почты и IP-адреса сотрудника Инициативы «Бирге», который ведёт учётную запись.

Какие виды обработки данных не входят в сферу действия Закона?

> Статья 2 Закона о персональной информации

Закон распространяется практически на все ситуации, когда обрабатываются персональные данные — независимо от того, делается ли это на бумаге или с использованием цифровых инструментов, а также от того, кто осуществляет обработку: компания, государственный орган или частное лицо.

Однако существует одно важное исключение: закон не применяется, если физическое лицо обрабатывает персональные данные исключительно для личных, семейных или бытовых целей, при условии, что при этом не нарушаются права других лиц. Иными словами, закон не регулирует частную, непрофессиональную деятельность.

Когда же ОГО собирает или использует персональные данные в рамках своей деятельности (например, проектов, оказания услуг или проведения мероприятий), закон применяется всегда — даже если обработку выполняет всего один сотрудник или она осуществляется в небольшом объёме. ОГО **не может** ссылаться на исключение «для личного пользования».

ПРИМЕР

Жена исполнительного директора Инициативы «Бирге» посещает корпоративное мероприятие и делает групповую фотографию. Она распечатывает её и вешает дома в рамку. Исполнительный директор видит фотографию и решает разместить её на главной странице сайта Инициативы «Бирге».

Применяется ли Закон о персональной информации к этой фотографии?

Когда жена исполнительного директора вешает фотографию дома, это подпадает под исключение «для личного пользования», и Закон о персональной информации не применяется.

Однако действие Закона распространяется на ситуацию, когда фотография размещается на сайте организации. Поэтому исполнительный директор не должен публиковать фото в интернете без получения согласия всех изображённых на нём лиц.

Основные принципы защиты персональных данных?

> Статья 4 Закона о персональной информации

В соответствии со статьей 4 Закона о персональной информации ОГО должны соблюдать ряд основных принципов при работе с персональными данными:

1. *Законность.* Перед обработкой персональных данных ОГО необходимо убедиться в наличии законного основания и в том, что они готовы соблюдать правила и процедуры, установленные законом.
2. *Прозрачность и ограничение целей.* Организация должна ясно и открыто информировать субъектов персональных данных о цели сбора сведений. Персональная информация может использоваться только для той цели, которая была обозначена при её сборе. Например, если данные собирались для регистрации на мероприятие, организация не может добавить контактные данные участников в список рассылки для фандрайзинга без получения отдельного согласия на новую цель.
3. *Точность.* Собранные и хранящиеся персональные данные должны быть достоверными и актуальными. У субъектов персональных данных должно быть право требовать исправления неверных сведений. Например, организация обязана следить, чтобы кадровые документы сотрудников были заполнены правильно и обновлялись регулярно. Ошибка в номере ID-карты или адресе может привести к проблемам с выплатами или налоговыми документами.
4. *Ограничение срока хранения.* Персональные данные должны храниться только столько, сколько необходимо для достижения цели, ради которой они были собраны. После этого сведения подлежат надежному уничтожению[1]. Организациям не следует хранить устаревшие списки участников, анкеты или иные подобные документы неопределённо долго.

[1] «Надёжное уничтожение» означает, что персональная информация должна быть уничтожена таким образом, чтобы её невозможно было восстановить или прочитать повторно после того, как она больше не нужна. Для бумажных

- Однако существуют документы, которые подлежат обязательному хранению в течение определённых сроков, установленных законом. Например, кадровые документы, подтверждающие трудовую деятельность (приказы о приёме и увольнении, трудовые договоры и соглашения, табели и ведомости), должны храниться 60 лет.
- Для уточнения сроков хранения ОГО следует обращаться к Перечню типовых управленческих архивных документов, образующихся в процессе деятельности государственных и негосударственных организаций, с указанием сроков их хранения. Этот документ является основным нормативным источником для определения сроков хранения и отбора документов к уничтожению или передаче на постоянное хранение в государственные архивы. Кроме того, необходимо учитывать иные применимые законы.

5. *Целостность.* Если персональные данные сохраняются для исторических или иных долгосрочных целей, необходимо обеспечить их защиту. Например, при архивировании проектных материалов для отчётности или исследований нужно применять надлежащие меры безопасности (шифрование, ограничение доступа).
6. *Запрет на неправомерное объединение массивов персональных данных.* Не допускается объединение массивов персональных данных, собранных держателями (обладателями) в разных целях, для автоматизированной обработки информации. Наример, если организация собрала данные по проекту в сфере женского здоровья и отдельно по программе лидерства для молодёжи, она не может объединить эти базы и проводить автоматизированный анализ без законного основания и информированного согласия субъектов.
7. *Конфиденциальность.* Персональные данные должны храниться в условиях безопасности и быть защищены от несанкционированного доступа, изменения или уничтожения. ОГО следует использовать парольную защиту, безопасное хранение (физическое и цифровое) и систему разграничения доступа. Обрабатывать данные должны иметь право только уполномоченные лица.

документов это, как правило, измельчение в шредере или сжигание. Для электронных файлов — использование специального программного обеспечения, которое полностью удаляет файл (а не просто перемещает его в корзину), либо физическое уничтожение носителя информации при необходимости. Главная цель — исключить возможность восстановления или дальнейшего неправомерного использования персональных данных.

Эти принципы не являются исчерпывающими. В будущем в связи с изменениями законодательства Кыргызстана могут быть введены дополнительные правила. Поэтому ОГО должны следить за обновлениями законодательства о защите персональных данных и адаптировать свою практику.

Когда необходимо получить согласие на сбор или использование персональных данных

> Статья 5 Закона о персональной информации

Согласие — одно из основных правовых оснований, позволяющих организации законно обрабатывать персональные данные. Получив согласие, ОГО могут обрабатывать персональные данные, не будучи обязанными доказывать наличие какого-либо другого правового основания для обработки. Согласие защищает как права отдельных лиц, так и репутацию вашей организации и подтверждает соблюдение вами законодательства. В следующем разделе будут рассмотрены требования и процедуры получения согласия.

Как получить согласие на сбор и обработку персональных данных

> Статья 9 Закона о персональной информации
>
> *Смотрите также* Порядок получения согласия субъекта персональных данных на сбор и обработку его персональных данных, в том числе в форме электронного документа, и в целях предоставления государственных и муниципальных услуг (далее – Приказ № 27)

Существуют правила и требования по получению согласия лица перед сбором или использованием его персональных данных:

1. Чтобы обеспечить осознанное и свободное согласие субъекта персональных данных, ОГО должны убедиться, что субъект ясно проинформирован о том, что его персональные данные собираются, в момент их сбора.
2. ОГО всегда должны фиксировать согласие в письменной форме — либо на бумаге, либо в виде электронного документа, подписанного в соответствии с Законом об электронной подписи. Электронное согласие также может подтверждаться действиями, такими как ввод логина и пароля, установка отметки в чекбоксе или нажатие кнопки «принять», при условии, что подтверждения этих действий четко фиксируются.

3. Чтобы согласие считалось «информированным», ОГО должны простым языком разъяснить следующую информацию:
   - кто является лицом (организацией), собирающим данные (например, название, адрес и контактные данные ОГО);
   - какие данные собираются (например, имя, номер телефона, фотография, электронный адрес);
   - цель сбора (например, регистрация на мероприятие, рассылка, оказание услуги, отчётность перед донором);
   - предполагаемое использование персональных данных (например, хранение, публикация в социальных сетях, проверка налоговым инспектором);
   - третьи лица, которым будут переданы данные (например, конкретные доноры, ОГО, государственные органы, поставщики; следует избегать расплывчатых формулировок вроде «другие партнёры»);
   - срок действия согласия (например, конкретная дата, период или иные чёткие критерии). Если срок согласия различается для разных целей, он должен быть указан отдельно для каждой цели.
4. Лицо может отказаться от предоставления данных или отозвать согласие в любое время и без объяснения причин. Исключения составляют случаи, когда ОГО обязана хранить данные по закону или договору, однако в общем порядке ОГО должны быть готовы полностью удалить все персональные данные по запросу субъекта.
5. ОГО должны иметь возможность доказать, что согласие было получено надлежащим образом. Если возникает спор, обязанность доказать факт и корректность получения согласия лежит на ОГО (держателе массива персональных данных). Это означает, что необходимо хранить правильно оформленные формы согласия или электронные подтверждения.

Важно: Вы не можете запрашивать «общее согласие» для всех целей и способов использования данных. Каждая отдельная цель (например, передача данных донору, публикация фотографий в интернете, трансграничная передача) требует отдельного согласия.

Контрольный список (чек-лист) по выполнению требований к получению согласия

Задайте себе следующие вопросы, чтобы убедиться, что ваша организация выполняет требования закона к получению согласия:

- √ Есть ли у нас форма согласия при сборе персональных данных (в бумажном или электронном формате)?
- √ Ясно ли мы объясняем цель сбора данных?
- √ Содержит ли наша форма согласия все необходимые сведения (кто собирает данные, какие данные, зачем, как, сколько времени будут храниться данные)?
- √ Получаем ли мы отдельное согласие для каждой цели?
- √ Обеспечиваем ли мы свободу выбора? Может ли человек согласиться на одни цели и отказаться от других?
- √ Надёжно ли мы храним подтверждения согласия на протяжении всего срока использования данных?
    - Сохраняем ли мы подписанный бумажный экземпляр?
    - Сохраняем ли мы подписанные электронные документы или ведём журналы/реестры?
    - Уничтожаем ли мы записи, когда они больше не нужны?
- √ Информируем ли мы субъектов персональных данных об их правах и о порядке отзыва согласия?

НА ЗАМЕТКУ ОГО

Регистрация участников мероприятий: используйте форму с отдельными чекбоксами, чтобы участники могли выбрать вариант ответа. Пример формулировки:

- *Я приму участие в мероприятии*
- *Я хотел бы получать информационные бюллетени и обновления от [Название организации]*
- *Я согласен на фотографирование и/или видеозапись во время мероприятия*

Онлайн-формы: собирайте согласие через онлайн-форму, где участник указывает адрес электронной почты, читает краткое уведомление о конфиденциальности и нажимает «Согласен». Обязательно сохраняйте отметку времени в настройках как подтверждение согласия. Пример формулировки:

> *«Нажимая кнопку "Согласен", я подтверждаю, что ознакомился(лась) с уведомлением о конфиденциальности и даю согласие [Название организации] на обработку моих персональных данных для указанных целей».*

Имейте в виду, что многие онлайн-сервисы автоматически собирают IP-адреса. Если вы не используете IP-адреса для каких-либо конкретных целей, отключите эту функцию или обеспечьте их удаление в момент сбора. Если IP-адреса фиксируются для конкретной цели, необходимо информировать субъектов персональных данных и объяснять цель сбора IP-адресов.

Фото и видео: просите участников подписать отдельную форму согласия на использование их изображений в отчётах, на сайте или в социальных сетях. Пример формулировки:

> *«Я согласен(на) на использование моей фотографии/видеозаписи [Название организации] в публикациях, отчётах и социальных сетях. Я понимаю, что моё изображение не будет использоваться в коммерческих целях».*
>
> - *Я согласен(на)*
> - *Я не согласен(на)*

Передача данных донорам: если данные участников будут передаваться донору, укажите конкретное имя донора в форме согласия и объясните цель передачи. Пример формулировки:

> *«Ваши имя, организация и адрес электронной почты будут переданы нашему донору, [Имя донора], для подтверждения результатов проекта и обеспечения прозрачности. Ваши данные не будут использоваться для других целей».*
>
> - *Я согласен(на) на передачу моих данных [Имя донора]*
> - *Я не согласен(на)*

РЕСУРСЫ И ШАБЛОНЫ

Типовая форма согласия (в разработке): Государственное агентство по защите персональных данных (далее - Агентство по защите данных) готовит типовую форму согласия. Следите за обновлениями на их официальном сайте: dpa.gov.kg.

Существующий шаблон: Приложение к Приказу № 27 содержит типовую форму согласия, обязательную для государственных и муниципальных органов. ОГО могут адаптировать этот шаблон для своих мероприятий и деятельности.

Трансграничная передача персональных данных: что это означает и как соблюдать требования Закона

> Статья 25 Закона о персональной информации

Многие ОГО в Кыргызстане сотрудничают с международными партнёрами, донорами и сетями. Это часто требует трансграничного обмена персональными данными, например, отправки списков участников донору за рубежом, использования облачного хранилища или другого программного обеспечения, размещающего данные на серверах в других странах, передачи паспортов или других проездных документов в гостиницы и авиакомпании за пределами Кыргызстана или даже физического провоза документов и бумаг, содержащих персональные данные, в багаже при посещении конференций или мероприятий за рубежом. Статья 25 устанавливает правила, определяющие, когда и как допускается такая передача.

Согласно статье 25 Закона о персональных данных, ОГО может передавать персональные данные в другую страну только при условии, что в этой стране действуют строгие правила защиты данных («адекватный уровень защиты»). Если в стране, куда вы хотите отправить данные, отсутствуют адекватные законы о защите данных, передача данных допускается только в особых случаях:

- С согласия лица — например, если участник письменно соглашается, что его данные могут быть переданы иностранному партнеру.
- Для защиты интересов человека — например, при предоставлении медицинской информации в экстренной ситуации.
- Если данные уже являются общедоступными — например, имена и контакты, указанные в общедоступном каталоге или на общедоступном веб-сайте.

НА ЗАМЕТКУ ОГО

Практической проблемой является отсутствие официальных рекомендаций о том, какие страны соответствуют стандарту «адекватной защиты». Агентство по защите данных планирует опубликовать список таких стран, однако этот список пока не опубликован. До выхода официального списка ОГО не могут самостоятельно достоверно определить, соответствует ли правовая система другой страны уровню защиты, установленному в Кыргызстане.

Поэтому, чтобы подтвердить добросовестное соблюдение закона в ожидании официальных инструкций от Агентства по защите данных, организациям следует всегда указывать в формах согласия информацию о возможной трансграничной передаче персональных данных и получать информированное согласие субъектов на такую передачу.

Когда персональные данные являются конфиденциальными и когда они могут быть обнародованы?

> Статьи 6, 7 и 26 Закона о персональной информации
>
> *См. также:* Приказ Государственного агентства по защите персональных данных при Кабинете Министров КР «Об утверждении Порядка обезличивания персональных данных для целей проведения статистических, социологических, исторических, медицинских и иных научно-практических исследований» от 14 января 2025 года № 4.

Персональные данные считаются конфиденциальной информацией, если законом не установлено иное. Это означает, что ОГО должны обращаться с ними осторожно, не раскрывать их и защищать от неправомерного использования. Если ваша организация собирает имена, адреса, номера телефонов или иные персональные сведения о бенефициарах, сотрудниках или партнёрах, вы обязаны относиться к этой информации как к конфиденциальной. Необходимо обеспечивать защиту от несанкционированного доступа, незаконного блокирования, неправомерной передачи, случайного или несанкционированного уничтожения, изменения или утраты.

Правила конфиденциальности отменяются в следующих трех ситуациях:

1. *Анонимизация.* При анонимизации персональных данных они становятся «обезличенными». Все идентифицирующие данные удаляются, поэтому их невозможно связать с конкретным лицом. Пример: публикация результатов опроса в виде групповой статистики без имён и контактных данных. Анонимизация должна проводиться с осторожностью, чтобы исключить возможность повторной идентификации человека, даже косвенной, по уникальным признакам или редким деталям.
2. *По запросу пользователя.* Субъект данных может по своему усмотрению сделать свои данные публичными. Например, он может попросить включить его в каталог проекта или опубликовать свою контактную информацию в публичном отчёте.
3. *Общедоступные наборы данных.* Справочники, телефонные или адресные книги могут существовать, но только с письменного согласия лица, чьи данные включены в них. Несмотря на то, что такие данные не считаются конфиденциальными, для их включения требуется согласие.

НА ЗАМЕТКУ ОГО

- √ Никогда не включайте людей в публичные списки (например, опубликованный отчёт, каталог членов, контакт-лист на сайте) без их письменного согласия.
- √ Если человек позже попросит удалить его данные, необходимо оперативно выполнить этот запрос.
- √ Даже если данные обезличены или сделаны публичными по согласию, организация обязана обращаться с ними этично и уважать выбор людей.

Какие ещё обязанности возникают у держателя (обладателя) массива персональных данных и у обработчика данных?

> Статьи 17–21 Закона о персональной информации
>
> *См. также* : Постановление Правительства КР от 21 ноября 2017 года N760 «Об утверждении Требований к обеспечению безопасности и защиты персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» (Постановление № 760).

Быть держателем (обладателем) массива персональных данных (организацией, которая решает, зачем и каким образом обрабатываются данные) или обработчиком персональных данных (организацией или лицом, которое обрабатывает данные от имени держателя) означает наличие ряда важных обязанностей по закону. Эти обязанности направлены на защиту прав субъектов персональных данных и обеспечение ответственного сбора, использования и хранения информации.

Постановление № 760 устанавливает обязательные требования безопасности для всех организаций в Кыргызстане, которые обрабатывают персональные данные в информационных системах, включая ОГО. Оно основано на статье 21 Закона о персональной информации. В документе вводится система уровней защищённости персональных данных и определяются меры, которые организации обязаны предпринимать в зависимости от уровня риска.

В зависимости от серьезности угроз существует четыре уровня защиты данных:

- Синий уровень — минимальный риск (требуются базовые организационные меры защиты).
- Зелёный уровень — средний риск (дополнительные меры, например, использование средств криптографической защиты).

- Жёлтый уровень — высокий риск (необходимы централизованное администрирование, ведение электронных журналов событий, внедрение систем обнаружения вторжений).
- Красный уровень — критический риск (применение наиболее строгих мер: использование сертифицированных средств защиты, защищённых каналов связи, проведение регулярных аудитов безопасности).

Для самооценки уровня защищённости персональных данных ОГО могут использовать онлайн-модуль Агентства по защите данных: https://self-rating.dpa.gov.kg/. В зависимости от результата (синий–красный уровень) необходимо реализовать соответствующие меры защиты.

НА ЗАМЕТКУ ОГО

Постановление № 760 закрепляет минимальные требования и стандарты безопасности, которые обязан соблюдать каждый, кто обрабатывает персональные данные в информационных системах. Для ОГО это означает необходимость:

√ Определить уровень угроз в зависимости от характера и объёма обрабатываемых персональных данных. Избегайте сбора лишних сведений (например, информации о состоянии здоровья), которые могут автоматически повысить ваш уровень защищённости и привести к более строгим требованиям.

√ Обеспечить реализацию базовых мер: разработку локальных актов, назначение ответственного за защиту персональных данных, установку средств контроля доступа, резервное копирование, использование шифрования.

√ Если обрабатываются специальные категории персональных данных (например, информация о здоровье или уязвимых группах) или большие массивы данных, применять меры, соответствующие более высокому уровню защищённости.

Нужно ли регистрироваться в качестве держателя персональных данных? Как это сделать?

> Статьи 16 и 30 Закона о персональной информации

Согласно Закону о персональной информации, любое юридическое лицо, работающее с персональными данными, обязано предварительно зарегистрироваться в качестве держателя массива персональных данных в

Агентстве по защите данных. Без регистрации организация не имеет законного права обрабатывать персональные данные.

Если ваша организация собирает или использует персональные данные (например, базы данных бенефициаров, кадровые документы сотрудников, реестры волонтёров, фотографии участников), вы считаетесь держателем массива персональных данных и обязаны пройти регистрацию в Агентстве по защите данных. Исключение составляют только массивы, содержащие сведения, отнесённые к государственной тайне в соответствии с Законом «О государственной тайне», который не распространяется на ОГО.

При регистрации вам необходимо предоставить информацию о ваших наборах данных, включая:

- √ наименование массива (например, «База данных бенефициаров»);
- √ данные об организации (адрес, форма собственности, руководитель, контактная информация);
- √ цель и способы сбора и использования персональных данных;
- √ срок хранения данных;
- √ перечень персональных данных, которые вы собираете (например, имена, телефоны, электронные адреса);
- √ категории субъектов персональных данных (например, бенефициары, сотрудники, волонтёры);
- √ источники данных (например, анкеты, опросы);
- √ порядок информирования субъектов о сборе и возможной передаче данных;
- √ меры защиты для обеспечения безопасности и конфиденциальности;
- √ ответственного за обработку персональных данных в вашей организации;
- √ лиц или организаций, которым могут передаваться данные (партнёры, доноры);
- √ планы по трансграничной передаче данных (если такие имеются).

Агентство по защите данных ведёт Реестр держателей массивов персональных данных. Ежегодно Агентство публикует этот Реестр в СМИ, чтобы общественность знала, какие организации официально имеют право работать с персональными данными. Регистрация даёт вашей организации право обрабатывать персональные данные и защищает от штрафов за обработку данных

без регистрации *(подробнее см. раздел «Какие штрафы предусмотрены за нарушение законодательства о персональных данных?»)*.

Дополнительная информация о процессе регистрации доступна в видеоматериале Агентства: https://dpa.gov.kg/ru/register/help/5. Для консультаций и справки вы можете связаться с Агентством через WhatsApp: +996 998 950 350.

НА ЗАМЕТКУ ОГО

31 июля 2025 года Президент подписал новый Цифровой кодекс КР. Кодекс вводит обновлённые правила работы с персональными данными и отменяет требование о регистрации в качестве держателя персональных данных. Однако Кодекс вступает в силу только через шесть месяцев после его официального опубликования, то есть 8 февраля 2026 года. При этом важно отметить, что положения Кодекса о правонарушениях вступают в силу раньше – 23 ноября 2025 года.

Таким образом, возникает переходный период с 23 ноября 2025 года до 8 февраля 2026 года, в течение которого Агентство по защите данных всё ещё вправе накладывать штрафы за обработку персональных данных без регистрации, хотя обязанность регистрации в будущем будет отменена.

В переходный период:

- √ Проверьте, зарегистрированы ли вы в качестве держателя персональных данных в Агентстве.
- √ Если вы еще не зарегистрированы, рассмотрите возможность завершить регистрацию до 23 ноября 2025 года, чтобы избежать штрафов.
- √ Соблюдайте все прочие требования по защите данных (согласие, меры безопасности, конфиденциальность и т. д.).
- √ Следите за обновлениями от Агентства о том, как на практике будет осуществляться поэтапный отказ от регистрации.
- √ Планируйте заранее: даже после отмены требования о регистрации с 8 февраля 2026 года ОГО обязаны будут соблюдать требования Цифрового кодекса в части обработки персональных данных.

Кто обеспечивает исполнение закона?

> Статья 3, 29 [1] Закона о персональной информации
>
> *См. также* Положение о Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики, утвержденное

> Постановлением Кабинета Министров Кыргызской Республики от 22 декабря 2021 года №325.

В Кыргызстане ответственность за обеспечение защиты персональных данных возложена на Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики (далее – Агентство по защите данных).

Закон о персональной информации, принятый в 2008 году, установил основные правила сбора, обработки и защиты персональных данных. Однако до 2021 года в Кыргызстане не было специального уполномоченного органа в сфере защиты персональных данных. Это означало, что отсутствовал механизм надзора, процедуры обжалования незаконных действий держателей массивов персональных данных, а также санкции за нарушения. Для того чтобы обеспечить исполнение правил в сфере защиты данных, в 2021 году было создано Агентство по защите данных.

Агентство по защите данных отвечает за то, чтобы персональные данные в Кыргызстане собирались, хранились и использовались законно и безопасно. В его полномочия входит:

- контроль за соблюдением законодательства в сфере персональных данных;
- регистрация организаций в качестве держателей массивов персональных данных и ведение официального Реестра;
- рассмотрение обращений граждан и предоставление организациям разъяснений и консультаций;
- выдача обязательных для исполнения предписаний, предупреждений или направление материалов в правоохранительные органы при выявлении нарушений;
- требование внесения изменений, блокирования или уничтожения недостоверных либо незаконно полученных данных.

Помимо контрольных функций, Агентство также разрабатывает национальную политику и нормативные акты, утверждает стандарты безопасной обработки данных, сотрудничает с зарубежными органами по защите данных и повышает уровень осведомлённости через отчёты, тренинги и исследования. Иными словами, Агентство по защите данных не только обеспечивает исполнение закона, но и помогает организациям улучшать свою практику работы с персональными данными.

КОНТАКТЫ АГЕНТСТВА ПО ЗАЩИТЕ ДАННЫХ

Официальная информация, инструменты и обновления: https://dpa.gov.kg

Для консультаций и поддержки: WhatsApp: +996 998 950 350

Какие штрафы предусмотрены за нарушение законодательства о персональных данных?

> Кодекс Кыргызской Республики о правонарушениях
>
> *«Статья 413 [2]. Нарушение требований о защите персональных данных*

Статья 413[2] Кодекса о правонарушениях устанавливает штрафы для организаций и физических лиц, которые не соблюдают установленные законодательством правила защиты персональных данных в Кыргызской Республике. Это означает, что если ваша организация собирает, хранит или использует персональные данные (например, списки бенефициаров, регистрационные формы участников мероприятий или фотографии участников), вы обязаны соблюдать закон. В противном случае вы рискуете быть оштрафованными.

Если ОГО неправильно обрабатывает персональные данные — например, собирает их без надлежащего согласия, хранит ненадлежащим образом или передает третьим лицам без разрешения, — законом предусмотрены следующие штрафы за первое нарушение:

- Физические лица (например, сотрудники): 7 500 сомов
- Должностные лица (например, директора, менеджеры): 10 000 сомов
- Юридические лица (сама ОГО): 65 000 сомов

Если такое же нарушение совершается повторно в течение одного года после применения взыскания, штрафы значительно возрастают:

- Физические лица: 25 000 сомов
- Должностные лица: 30 000 сомов
- Юридические лица: 120 000 сомов

Кроме того, организации подлежат штрафу, если они не зарегистрировались в качестве держателя (обладателя) массива персональных данных. Внесение неполной или недостоверной информации в Реестр либо сбор и обработка персональных данных без регистрации также является нарушением и влечет штраф в размере 45 000 сомов.

НА ЗАМЕТКУ ОГО

- √ Собирайте и используйте персональные данные только на законных основаниях. Всегда обеспечивайте согласие субъекта данных или наличие иного законного основания.
- √ Зарегистрируйтесь как держатель массива персональных данных, если ваша организация подпадает под это требование.
  - Посмотрите видеоинструкцию по заполнению реестра держателей персональных данных.
  - Зарегистрируйтесь через официальный сайт: https://dpa.gov.kg/ru.
- √ Пересмотрите и обновите ваши внутренние политики защиты данных, чтобы предотвратить нарушения. Вы можете воспользоваться генератором политик конфиденциальности Агентства по защите данных, чтобы создать политику для вашей организации.
- √ Обучите своих сотрудников правильному обращению с персональными данными. Помните: ошибки сотрудников могут привести к штрафам для вашей организации.

> Кодекс Кыргызской Республики о правонарушениях
>
> *«Статья 413³. Трансграничная передача персональных данных с нарушением установленного законодательством порядка»*

Многие ОГО регулярно обмениваются данными с международными донорами, партнёрами или сетями. Такая деятельность квалифицируется как «трансграничная передача данных». Важно отметить, что даже использование таких цифровых инструментов, как Google Forms, Google Drive или Microsoft OneDrive, подразумевает трансграничную передачу данных, поскольку данные хранятся на серверах за пределами Кыргызстана.

Перед передачей данных за границу ОГО обязаны обеспечить соблюдение законодательства Кыргызстана. Как правило, для этого требуется либо подтверждение того, что принимающая страна обеспечивает адекватный уровень защиты данных, либо получение явного согласия субъекта данных. *Подробнее о требованиях законодательства см. в разделе «Трансграничная передача персональных данных» выше.*

Несоблюдение этих правил (даже непреднамеренное) может повлечь за собой значительные штрафы. Если ОГО передает персональные данные за границу без соблюдения установленной законом процедуры (например, в страну, не обеспечивающую адекватную защиту данных), применяются следующие штрафы за первое нарушение:

- Физические лица (например, сотрудники): 15 000 сомов
- Должностные лица (например, директора, менеджеры): 17 500 сомов
- Юридические лица (сама ОГО): 65 000 сомов

Если то же самое нарушение совершено повторно в течение года после наложения штрафа, санкции значительно увеличиваются:

- Физические лица: 30 000 сомов
- Чиновники: 35 000 сомов
- Юридические лица: 100 000 сомов

ПРИМЕР

Инициатива «Бирге» собирает имена, номера телефонов и адреса электронной почты участников тренинга. Впоследствии организация по электронной почте передает полный список участников международному донору, находящемуся в Канаде. Поскольку донор находится за пределами Кыргызстана, это считается трансграничной передачей персональных данных. Если организация не получила явного согласия участников на такую передачу или если Канада не обеспечивает адекватную защиту данных, она нарушает статью 413[3]. Даже если передача была непреднамеренной (например, сотрудник посчитал отправку списка безвредной), Инициатива «Бирге» всё равно может быть оштрафована.

НА ЗАМЕТКУ ОГО

√ Всегда проверяйте, содержат ли данные, которыми вы делитесь с международными партнерами, персональные данные.

√ Получите четкое и информированное согласие от людей, прежде чем передавать их данные за границу, если только не имеется иного правового основания.

√ Проверьте, обеспечивает ли принимающая страна адекватную правовую защиту персональных данных.

√ Ведите надлежащую документацию — фиксируйте, как было получено согласие и цель передачи.

> Кодекс Кыргызской Республики о правонарушениях
>
> *«Статья 413[4]. Необоснованный отказ держателем (обладателем) массива персональных данных в предоставлении субъекту его персональных данных»*

Согласно законодательству Кыргызстана, каждый человек (субъект данных) имеет право знать, как собираются, хранятся и используются его персональные данные.

Это означает, что бенефициары, сотрудники или партнёры могут запросить доступ к своим персональным данным, хранящимся в вашей организации (например, анкетам, контактным данным или фотографиям). Отказ вашей организации в удовлетворении такого запроса без достаточных правовых оснований будет считаться нарушением. Важно отметить, что согласно этой статье, штраф может быть наложен только на организацию (юридическое лицо), а не на отдельных сотрудников.

- Штраф за первое нарушение: 25 000 сомов.
- Штраф за повторное нарушение в течение года: 45 000 сомов.

НА ЗАМЕТКУ ОГО

- √ Разработайте простую процедуру обработки запросов на доступ к данным от бенефициаров, сотрудников или партнеров.
- √ Обучите персонал тому, когда необходимо предоставлять информацию, а когда может применяться исключение.
- √ Ведите чёткий учёт того, какие персональные данные собирает ваша ОГО и как они обрабатываются. Это упростит реагирование на запросы.
- √ Помните: отказ в доступе без достаточных правовых оснований может повлечь за собой штрафные санкции для организации.

> Кодекс Кыргызской Республики о правонарушениях
>
> *«Статья 413⁵. Неисполнение законных требований уполномоченного государственного органа по персональным данным»*

Уполномоченный государственный орган по защите персональных данных (Агентство по защите данных) отвечает за надзор за соблюдением законодательства о защите персональных данных в Кыргызстане. Он имеет законные полномочия запрашивать информацию, проводить проверки и выдавать обязательные к исполнению предписания организациям, обрабатывающим персональные данные *(подробнее см. в разделе «Кто обеспечивает исполнение закона»)*. Например, Агентство может потребовать от вас устранения пробелов в вашей практике защиты данных – зарегистрировать массивы персональных данных или обновить политику конфиденциальности. Игнорирование этих предписаний или несвоевременный ответ может привести к штрафам как для физических лиц, так и для организации.

Невыполнение ОГО законного требования или распоряжения Агентства считается нарушением статьи 413⁵. Установлены следующие штрафы:

- Физические лица (например, сотрудники): 10 000 сомов
- Должностные лица (например, директора, менеджеры): 20 000 сомов
- Юридические лица (сама ОГО): 30 000 сомов

НА ЗАМЕТКУ ОГО

√ Всегда реагируйте на запросы Агентства своевременно.

√ Храните все необходимые документы в порядке, чтобы их можно было быстро предоставить при необходимости.

√ Если вы не уверены, как выполнить предписание, запросите разъяснение в письменной форме у Агентства.

√ Помните: за невыполнение требований могут быть оштрафованы сама организация, ее руководители и сотрудники.

Нормативные правовые акты

При подготовке настоящего практического руководства были использованы следующие нормативные правовые акты:

- Закон Кыргызской Республики от 14 апреля 2008 года № 58 «Об информации персонального характера»
- Кодекс Кыргызской Республики о правонарушениях: статьи 413^{2}–413^{5} (нарушения в сфере персональных данных)
- Постановление Правительства Кыргызской Республики от 21 ноября 2017 года № 760 «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищённости персональных данных»
- Постановление Кабинета Министров Кыргызской Республики от 22 декабря 2021 года № 325 «О Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики»
- Приказ Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики от 15 апреля 2025 года № 27 «Об утверждении Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных, в том числе в виде электронного документа, в том числе в целях предоставления государственных и муниципальных услуг»

- Приказ Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики от 14 января 2025 года № 4 «Об утверждении Порядка обезличивания персональных данных для проведения статистических, социологических, исторических, медицинских и других научных и практических исследований»
- Цифровой кодекс Кыргызской Республики (принят 31 июля 2025 года, вступает в силу 8 февраля 2026 года)