ICNL

www.icnl.org
info@icnl.org

ОБЗОР

Цифровой кодекс Кыргызской Республики: понимание и соблюдение положений о защите персональных данных

Представленная информация носит исключительно общий информационный и образовательный характер. Она не предназначена и не должна рассматриваться как юридическая консультация. Ничто из содержащегося в этом обзоре не должно рассматриваться как основание для принятия решений без юридической консультации, основанной на конкретных фактах и обстоятельствах.

INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

1660 L Street NW #600
Вашингтон, округ Колумбия, 20036

Оглавление

Введение

Данный обзор предназначен для организаций гражданского общества (ОГО) в Кыргызстане, которые собирают, хранят, используют или передают персональные данные в ходе своей работы. К таким видам деятельности относятся, в частности, регистрация участников мероприятий, ведение списков рассылки, проведение опросов, учет кадров и волонтеров, использование фото- и видеоматериалов, а также предоставление отчётов донорам и партнёрам. Это лишь некоторые примеры; на практике большинство ОГО обрабатывают персональные данные в той или иной форме.

Система правового регулирования защиты персональных данных в Кыргызской Республике в настоящее время проходит важный переходный этап. С 23 ноября 2025 года организации, обрабатывающие персональные данные, включая ОГО, могут быть привлечены к ответственности в виде штрафов в соответствии с поправками к Кодексу о правонарушениях (статьи 413–2, 413–3, 413–4, 413–5). Между тем, 5 февраля 2026 года Закон 2008 года «Об информации персонального характера» утратил силу и заменен соответствующими положениями Цифрового кодекса. Одновременно вступили в силу новые составы правонарушений, предусмотренные Кодексом Кыргызской Республики о правонарушениях (статьи 228–3, 228–6 и 228–7). Таким образом, ОГО должны быть готовы к полному соблюдению как Цифрового кодекса, так и знать обновленные положения Кодекса о правонарушениях.

Для снижения правовых и операционных рисков организациям рекомендуется начать подготовку заранее. В частности, необходимо:

- провести инвентаризацию персональных данных, которые собираются организацией, и определить цели их обработки;
- обеспечить надлежащее получение и документирование согласия субъектов персональных данных;
- пересмотреть порядок хранения персональных данных и определить круг лиц, имеющих к ним доступ;
- установить, передаются ли персональные данные донорам или партнёрам либо осуществляются ли трансграничные передачи персональных данных;
- назначить ответственное лицо по вопросам обработки персональных данных в случаях, когда это требуется законодательством;
- разработать или обновить основные внутренние документы, включая уведомление о конфиденциальности, формы согласия и внутренние правила обращения с персональными данными.

Настоящий обзор направлен на содействие ОГО в понимании своих обязанностей и организации процесса приведения деятельности в соответствие с требованиями законодательства. Требования к защите персональных данных изложены в документе в простой и доступной форме.

Однако, пожалуйста, обратите внимание, что данный документ следует использовать только в качестве справочного материала в образовательных целях. Ничто из содержащегося здесь не должно рассматриваться как юридическая консультация по конкретным ситуациям без консультации с квалифицированным юристом.

Краткий обзор требований к защите персональных данных

1. ЗНАЙТЕ, КАКИЕ ДАННЫЕ ВЫ ОБРАБАТЫВАЕТЕ

Начните с определения того, какие персональные данные обрабатывает ваша организация. Часть информации относится к специальным категориям персональных данных (например, данные о состоянии здоровья, этнической принадлежности, религиозных убеждениях, политических взглядах). Избегайте сбора специальных категорий данных, если только не применяется одно из прямо предусмотренных законом исключений и не обеспечены усиленные меры защиты.

2. ПРЕЖДЕ ЧЕМ СОБИРАТЬ ДАННЫЕ, УБЕДИТЕСЬ, ЧТО У ВАС ЕСТЬ ЗАКОННОЕ ОСНОВАНИЕ

Вы можете обрабатывать персональные данные только при наличии законного основания. Если ни одно из законных оснований не применимо, вы должны получить согласие, прежде чем собирать или использовать персональные данные. Для большинства видов деятельности ОГО согласие остается наиболее безопасным и юридически обоснованным основанием для сбора данных.

3. ПОЛУЧИТЕ СОГЛАСИЕ НАДЛЕЖАЩИМ ОБРАЗОМ

В согласии должно быть четко указано, кто собирает данные; какие данные собираются; зачем они собираются и как будут использоваться; кто их получит; как долго они будут храниться; как можно отозвать согласие. Согласие должно быть задокументировано, и ОГО должна иметь возможность доказать, что оно было получено.

4. СОБИРАЙТЕ ТОЛЬКО ТО, ЧТО ВАМ ДЕЙСТВИТЕЛЬНО НУЖНО

Применяйте принцип минимизации данных: собирайте только информацию, необходимую для достижения конкретной цели; не запрашивайте дополнительные данные или данные «на всякий случай»; избегайте сбора конфиденциальных данных. Если цель может быть достигнута с меньшим количеством данных, собирайте меньше.

5. ЗАЩИТИТЕ ДАННЫЕ

Примите практические меры безопасности для защиты персональных данных. Уровень защиты должен соответствовать риску и степени конфиденциальности обрабатываемых вами данных.

6. НЕ ХРАНИТЕ ДАННЫЕ ДОЛЬШЕ, ЧЕМ ЭТО НЕОБХОДИМО

Персональные данные должны храниться только до тех пор, пока это необходимо для достижения заявленной цели. Отдельные документы подлежат обязательному хранению в течение установленных сроков в соответствии с другими нормативными правовыми актами (например, кадровые документы). Такие случаи должны быть обоснованы и документированы.

7. БУДЬТЕ ОСТОРОЖНЫ ПРИ ПЕРЕДАЧЕ ДАННЫХ ДРУГИМ ЛИЦАМ

Если вы передаете персональные данные другим лицам, вы по-прежнему несете юридическую ответственность за соблюдение законодательства. Обработчики данных

должны действовать только по вашим указаниям и на основании письменного соглашения.

8. РАССМАТРИВАЙТЕ ТРАНСГРАНИЧНУЮ ПЕРЕДАЧУ ДАННЫХ КАК ЗОНУ ПОВЫШЕННОГО РИСКА

До опубликования официального перечня государств, обеспечивающих надлежащий уровень защиты, четко информируйте субъектов персональных данных о возможной трансграничной передаче; получайте согласие на такую передачу; документируйте применяемые меры защиты.

9. УВАЖАЙТЕ ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Лица, чьи данные вы обрабатываете, имеют право знать, как используются их данные, получать к ним доступ, исправлять неточности, отзывать согласие, возражать против определенных видов обработки и запрашивать удаление данных в случаях, когда это разрешено законом. Оперативно и в письменной форме отвечайте на такие запросы и возражения.

10. БУДЬТЕ ГОТОВЫ ПОДТВЕРДИТЬ СОБЛЮДЕНИЕ ТРЕБОВАНИЙ

Цифровой кодекс требует подотчетности. Добросовестное соблюдение требований, четкая документация и прозрачность значительно снижают правовые и операционные риски.

На кого распространяется действие закона?

Цифровой кодекс различает тех, чьи данные защищены (обладателей прав), и тех, кто обязаны соблюдать правила обработки (лиц, несущих ответственность).

КТО ЗАЩИЩЕН ЗАКОНОМ?

- **Субъект персональных данных**. Субъектом персональных данных является физическое лицо , чьи персональные данные собираются или используются. Сюда входят бенефициары, сотрудники, волонтеры, партнеры или доноры, чьи имена, контактные данные, фотографии или другая личная информация хранятся в ОГО. Система защиты персональных данных существует прежде всего для защиты прав и интересов этого лица.
- **Принципал данных (записей)** — это субъект правоотношений в цифровой среде, к которому относятся цифровые данные или цифровые записи (то есть они содержат информацию о нём). По Цифровому кодексу принципалом данных может быть физическое лицо, юридическое лицо или государственный орган. Если данные относятся к физическому лицу, оно является одновременно принципалом данных и субъектом персональных данных. Если данные относятся к организации или государственному органу, эта организация/орган является принципалом данных. Однако правила защиты персональных данных применяются для защиты именно физических лиц.

КТО НЕСЕТ ОБЯЗАТЕЛЬСТВА ПО ЗАКОНУ?

- **Владелец персональных записей** — это лицо [1] или организация, которые определяют, зачем и как обрабатываются персональные данные. Проще говоря, это тот, кто определяет: цель обработки (например, ведение списка бенефициаров, рассылка новостей, хранение кадровых документов); и способы обработки (какие инструменты используются, где хранятся данные, кому они передаются). Для ОГО обычно владельцем персональных записей является сама организация. Именно владелец персональных записей несёт основную юридическую ответственность за соблюдение требований по защите персональных данных.
- **Обработчик** — это подрядчик или поставщик услуг, который обрабатывает персональные данные от имени владельца и только в соответствии с его инструкциями. Обработчики не определяют, для чего обрабатываются персональные данные. Он выполняет технические или операционные задачи, например: хостинг баз данных или облачного хранилища; администрирование онлайн-регистраций; обработка данных опросов; оказание ИТ- и иных

[1]Согласно Закону «Об информации персонального характера» владельцем (или держателем) персональных данных могло быть только юридическое лицо. Однако Цифровой кодекс расширяет это понятие, и теперь он применяется ко всем типам организаций — физическим лицам, индивидуальным предпринимателям и организациям.

цифровых услуг. Обработчик действует на основании договора или правового акта и не имеет самостоятельного права использовать данные для собственных целей.

- **Собственник материальных носителей с информацией персонального характера** — это лицо или организация, которым принадлежат материальные носители, содержащие персональную информацию в нецифровой форме: регистрационные листы, папки с договорами, блокноты, USB-накопители и т. п. На практике ОГО может одновременно быть и владельцем персональных записей, и собственником материальных носителей, но по закону это разные роли.

КЕЙС: КТО ЕСТЬ КТО В СФЕРЕ ВЗАИМОДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ?

Гражданская инициатива «Бирге» (ГИБ) готовит национальный молодёжный форум и должна организовать регистрацию, коммуникацию с участниками и логистику мероприятия. Для регистрации заявители заполняют онлайн-форму, которую ГИБ создала с использованием Google Формы. Форма собирает: ФИО, номер телефона, адрес электронной почты и регион проживания каждого заявителя. Все ответы автоматически сохраняются в Google Диске ГИБ; доступ к ним имеют только программный менеджер и ассистент проекта.

Чтобы цифровые системы работали стабильно, ГИБ заключает договор с местной ИТ-компанией Айкын Tech. Компания помогает администрировать облачное хранилище ГИБ, настраивает права доступа при приёме или увольнении сотрудников и оказывает техническую поддержку при сбоях. Айкын Tech не использует информацию об участниках для собственных целей и действует строго в соответствии с письменными инструкциями ГИБ.

На мероприятии ГИБ распечатывает список участников с именами и номерами телефонов, чтобы организовать регистрацию на стойке. После завершения форума распечатанный список собирают и помещают под замок в шкаф для документов в кабинете административного сотрудника. Участники форума — молодые лидеры, которые добровольно предоставили свои персональные данные при подаче заявки.

ВОПРОСЫ

Исходя из этой истории, определите, кто является:

1. владельцем персональных записей;
2. обработчиком;
3. принципалами данных / субъектами персональных данных;
4. собственником материальных носителей с информацией персонального характера.

Сделайте паузу и подумайте, прежде чем смотреть ответы.

ОТВЕТЫ

1. **Владелец персональных записей — ГИБ.** ГИБ определяет, зачем собираются данные участников и как они будут использоваться, выбирает цифровые инструменты, управляет доступом и несёт юридическую ответственность.
2. **Обработчик — Айкын Tech**. Айкын Tech оказывает техническую поддержку по договору, администрирует настройки облачного хранилища и действует по инструкциям ГИБ. Компания не определяет цели обработки данных.
3. **Субъекты персональных данных** — участники молодёжного форума. Собранная информация напрямую относится к физическим лицам, подающим заявку на участие.
4. **Собственник материальных носителей** — ГИБ. Распечатанный список участников является материальным носителем, содержащим информацию персонального характера. Организация, которой принадлежит и которая контролирует этот документ, является собственником материального носителя; в данном случае — ГИБ, представленная административным сотрудником.

Что такое персональные данные?

> Цифровой кодекс:
>
> Статья 1(21) *информация персонального характера*
>
> Статья 1(42) *персональные данные*
>
> Порядок обезличивания персональных данных для проведения статистических, социологических, исторических, медицинских и других научных и практических исследований

В Цифровом кодексе используются два взаимосвязанных определения для объяснения того, что считается персональными данными.

Информация персонального характера — это любая информация о физическом лице, которое может быть идентифицировано прямо или косвенно: либо на основании самой этой информации, либо на основании этой информации в совокупности с другой информацией. К ней относятся, например: ФИО, адрес проживания, паспортные данные и персональный идентификационный номер, видео- или аудиозаписи, фотографии, отпечатки пальцев, адрес электронной почты, IP-адрес (уникальный номер устройства, подключающегося к интернету), генетические данные и любые иные сведения, «привязанные» к конкретному человеку.

Такая информация может быть:

- одним сведением, по которому человека можно определить напрямую; или
- набором сведений, которые в совокупности позволяют установить личность человека.

Проще говоря, если информация относится к реальному человеку и позволяет понять, кто именно это (сама по себе или вместе с другими данными), это информация персонального характера. Точность значения не имеет: даже ошибочные сведения остаются «информацией персонального характера», если относятся к идентифицируемому человеку.

Персональные данные – это уже цифровые данные, содержащие информацию персонального характера. То есть информация должна относиться к идентифицируемому человеку, и быть в цифровой форме. Если цифровая информация позволяет распознать конкретного человека, она считается персональными данными и охраняется законом.

Однако, если данные обезличены, они больше не считаются персональными данными. Обезличивание означает полное удаление и стирание всей идентифицирующей информации. Шифрование персональных данных или кодирование и хранение различных фрагментов данных отдельно не считается полным обезличиванием.

КЕЙС: КАК ОПРЕДЕЛИТЬ, ЧТО СЧИТАЕТСЯ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Гражданская инициатива «Бирге» (ГИБ) реализует программу наставничества для молодёжи. Сначала заявители заполняют бумажную анкету, где указывают ФИО, номер телефона и домашний адрес. Бумажные анкеты хранятся в папке на полке в офисе ГИБ. Позже ассистент программы переносит все сведения из бумажных анкет в онлайн-таблицу, размещённую в Google Диске ГИБ. Таблица содержит ФИО, контактные данные и регион проживания каждого заявителя. Для защиты информации ГИБ шифрует цифровой файл. Любой, кто пытается открыть его без ключа расшифровки, видит набор случайных символов вместо читаемого текста.

По завершении программы ГИБ готовит отчёт для донора. Вместо передачи имён и контактов отдельных участников ГИБ указывает только сводные данные: «подали заявки 120 молодых людей, отобраны 75», а также обезличенную статистику по полу и региональному распределению участников. В отчёте нет сведений, которые можно связать с конкретным человеком.

ВОПРОСЫ

По этой истории определите, какие данные являются:

1. информацией персонального характера;
2. персональными данными;
3. зашифрованными персональными данными;
4. обезличенными данными.

Сделайте паузу и подумайте, прежде чем смотреть ответы.

ОТВЕТЫ

1. **Информация персонального характера** — бумажные анкеты, заполненные заявителями.

ФИО, телефоны и домашние адреса явно относятся к идентифицируемым лицам. Хотя данные на бумаге и не являются цифровыми, это всё равно информация персонального характера, потому что она описывает конкретных людей.

2. **Персональные данные** — цифровая таблица, созданная на основе бумажных анкет.

После внесения тех же идентифицирующих сведений в цифровой файл они становятся персональными данными по Цифровому кодексу. Поскольку это цифровая информация, позволяющая идентифицировать конкретных лиц, она полностью подпадает под режим защиты персональных данных.

3. **Зашифрованные персональные данные** — зашифрованная таблица в Google Диске.

Хотя таблица зашифрована, после расшифровки она по-прежнему содержит идентифицирующие сведения. Шифрование защищает данные, но не устраняет возможность идентификации. Поэтому это остаётся персональными данными (в данном случае — зашифрованными).

4. **Обезличенные данные** — сводный отчёт для донора.

В отчёте есть только итоги и обезличенная статистика; в нём отсутствуют имена, телефоны и другие идентификаторы. Поскольку информацию невозможно связать с конкретным человеком, это обезличенные данные, и они больше не рассматриваются как персональные данные по Цифровому кодексу.

Что такое специальные категории персональных данных и как с ними обращаться

> Статья 80 Цифрового кодекса

Статья 80 Цифрового кодекса устанавливает строгие ограничения на обработку **специальных категорий персональных данных**. Это наиболее чувствительная информация о человеке, неправильное использование которой может привести к серьёзному вреду, дискриминации или нарушению прав. К специальным категориям персональных данных относятся сведения о расовой или этнической принадлежности; политических взглядах; религиозных или философских убеждениях; членстве в профессиональных союзах; генетических данных; биометрических данных, используемых для цифровой идентификации; состоянии здоровья; половой жизни или сексуальной ориентации.

Для ОГО это означает, что сбор и обработка специальных категорий персональных данных, как правило, запрещены. Цифровой кодекс допускает обработку таких данных только в строго определённых случаях и при наличии усиленных мер защиты. ОГО должны избегать обработки специальных категорий данных, если только не применяется одно из следующих исключений:

1. **Когда данные необходимы для заключения или исполнения договора**

Пример: ОГО заключает договор с психологом для работы в молодёжном лагере. Психолог добровольно предоставляет справку о состоянии здоровья, подтверждающую возможность работы с несовершеннолетними. Поскольку информация представлена в рамках договора, ОГО вправе её обработать.

2. **Когда обязанность сбора данных прямо предусмотрена законом**

Пример: Государственная программа требует предоставления медицинских или иных специальных сведений для подтверждения права участия в проекте социального заказа. Если требование установлено нормативным правовым актом, ОГО вправе обрабатывать такие данные.

3. **Когда это необходимо для защиты жизни или безопасности человека**

Пример: ОГО, оказывающая помощь пострадавшим от гендерного насилия, фиксирует критически важную медицинскую информацию для организации безопасного убежища или экстренной помощи.

4. **Когда лицо самостоятельно и явно сделало информацию публичной**

Пример: Человек публично размещает информацию о своём диагнозе на сайте. ОГО, готовящая аналитический материал о праве на охрану здоровья, может сослаться на эту информацию, поскольку она уже сделана общедоступной самим лицом.

5. **Когда обработка необходима в сфере общественного здравоохранения**

Специальные данные могут использоваться для предупреждения эпидемий, защиты населения или оказания гуманитарной помощи. Пример: во время пандемии COVID-19 горячая линия ОГО фиксировала результаты тестов и симптомы заявителей для определения необходимости срочного медицинского направления.

6. **Когда объединения обрабатывают специальные данные о своих членах**

Общественные объединения и религиозные организации вправе обрабатывать специальные категории данных своих членов, если это делается законно и в рамках целей, указанных в учредительных документах. Пример: Религиозная организация ведёт список членов и сведения об их участии в религиозной деятельности.

7. **Когда это необходимо для судебного разбирательства**

Пример: ОГО, помогающая бенефициару подать иск, может собрать чувствительные сведения о состоянии здоровья или личной жизни, если они требуются судом.

8. **Когда данные используются в научных целях — только в полностью обезличенной форме**

Пример: ОГО, изучающая доступ к медицинской помощи, использует обезличенные медицинские записи партнёрской клиники без указания имён и иных идентификаторов.

Существуют и иные исключения (например, для целей национальной безопасности, правоохранительной деятельности, официальной статистики или деятельности

лицензированных медицинских работников), однако они, как правило, не применимы к ОГО.

НА ЗАМЕТКУ ОГО

- √ Всегда задавайте вопрос: действительно ли нам необходима эта чувствительная информация для достижения цели? Если нет — не собирайте её.
- √ Если ОГО планирует собирать, хранить, использовать или передавать специальные категории персональных данных, необходимо проверить наличие одного из оснований, предусмотренных статьёй 80. Если ни одно основание не применяется, обработка запрещена — даже при наличии согласия.
- √ Согласие само по себе не является достаточным основанием, если оно не подпадает под одно из перечисленных исключений.
- √ Даже если исключение применяется, необходимо усилить меры защиты:
  - ограничить доступ строго кругом лиц, которым это необходимо;
  - хранить такие данные отдельно от других записей;
  - использовать шифрование и защиту паролем;
  - обезличивать данные при использовании в исследовательских целях (и, по возможности, в иных случаях);
  - минимизировать объём собираемой информации;
  - удалять данные сразу после утраты необходимости.

КЕЙС: ОБРАБОТКА СПЕЦИАЛЬНЫХ КАТЕГОРИЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

КЕЙС 1: Гражданская инициатива «Бирге» (ГИБ) организует двухдневный тренинг в конференц-зале. В онлайн-форме регистрации участников просят указать вид инвалидности и медицинский диагноз «для целей планирования».

ВОПРОС: Допустимо ли это?

ОТВЕТ: Нет. Планирование мероприятия и общая логистика не являются основанием для сбора медицинских данных в соответствии со статьёй 80. ГИБ должна задавать только нейтральные вопросы об обеспечении доступности, например: «Требуются ли вам условия доступности (например, доступ для инвалидной коляски, специальные места для сидения, сурдоперевод)?». ГИБ не вправе запрашивать диагнозы, вид инвалидности или сведения о лечении для обычного планирования мероприятия.

КЕЙС 2: ГИБ организует многодневный молодёжный лагерь на природе, включающий пешие маршруты, ночёвки и мероприятия в удалённых районах. Поскольку экстренная медицинская помощь может быть затруднена, ГИБ (на добровольной основе) просит участников указать критически важные медицинские состояния, тяжёлые аллергии и контактные данные для экстренной связи. Доступ к этим сведениям имеют только два подготовленных сотрудника по безопасности. Все чувствительные данные удаляются сразу после завершения лагеря. После мероприятия ГИБ рассматривает возможность

использования собранной медицинской информации для анализа потребностей доступности и подготовки отчёта донору.

ВОПРОС 1: Допустим ли сбор такой медицинской информации до начала лагеря?

ОТВЕТ: Да, но при строгом соблюдении условий. Статья 80 допускает обработку специальных категорий персональных данных, если это необходимо для защиты жизни или безопасности. Поскольку лагерь связан с реальными физическими рисками, ГИБ вправе собирать только минимально необходимую информацию для экстренного реагирования. ГИБ не должна запрашивать полные диагнозы или подробную медицинскую историю – только сведения, без которых невозможно предотвратить угрозу жизни или здоровью.

ВОПРОС 2: Может ли ГИБ использовать эти данные после лагеря для отчётности, оценки или анализа для донора?

ОТВЕТ: Нет. Исключение, связанное с защитой жизни и безопасности, применяется только к обработке в целях безопасности. Оно не позволяет использовать те же чувствительные данные для отчётности, мониторинга, оценки проекта или внутреннего анализа. Для таких целей допускается использование только в соответствии с пунктом 8 статьи 80 – в полностью обезличенной форме, когда невозможно установить личность участников.

Что такое обработка данных?

> Статья 1(35) Цифрового кодекса

В соответствии с Цифровым кодексом, обработка данных означает любое действие, которое вы совершаете с цифровыми данными. Это очень широкое понятие. Если ОГО совершает любое действие с цифровой информацией (собирает её, просматривает, хранит, изменяет или удаляет) это считается обработкой данных.

Проще говоря, если организация каким-либо образом работает с цифровыми данными (с момента их сбора до момента удаления), она осуществляет их обработку, и на такую деятельность распространяются требования Цифрового кодекса. Такое широкое определение введено намеренно, чтобы обеспечить ответственность за весь жизненный цикл персональных данных.

ПРИМЕР

ОГО осуществляет обработку персональных данных, когда:

- собирает имена и контактные данные при регистрации на мероприятие;
- хранит скан-копии паспортов для организации поездки;
- обновляет список рассылки, добавляя новые электронные адреса или номера телефонов;
- группирует бенефициаров по возрасту, полу или региону для подготовки проектного отчёта;

- ограничивает доступ к чувствительным файлам с помощью паролей;
- удаляет устаревшие регистрационные формы;
- уничтожает старые бумажные документы, содержащие информацию персонального характера.

Если ОГО выполняет любые из перечисленных действий (или иные сопоставимые действия), оно осуществляет обработку персональных данных и обязано соблюдать требования законодательства.

Как могут обрабатываться персональные данные детей

> Статья 81 Цифрового кодекса

Цифровой кодекс обеспечивает особую защиту персональных данных детей. Обработка таких данных возможна только в том случае, если это отвечает наилучшим интересам ребенка и при применении надежных мер защиты.

Персональные данные детей могут обрабатываться только в следующих случаях:

- обработка осуществляется на основании закона, прямо предусматривающего необходимость обработки персональных данных детей и определяющего цели их обработки;
- для защиты жизни или безопасности ребёнка либо безопасности другого лица или группы лиц;
- в медицинских целях (диагностика или лечение), но исключительно лицензированными медицинскими работниками, обязанными соблюдать врачебную тайну;
- в целях общественного здравоохранения (например, при реагировании на эпидемии или оказании гуманитарной помощи);
- для судебного разбирательства;
- в целях национальной безопасности, обороны, общественной безопасности или расследования преступлений (как правило, уполномоченными государственными органами);
- для проведения научных исследований или статистических целей — при условии применения надлежащих мер защиты либо в полностью обезличенной форме.

Если ни одно из перечисленных оснований не применяется, персональные данные ребёнка могут обрабатываться только с согласия его законного представителя. Дети, достигшие 14-летнего возраста, вправе самостоятельно давать согласие в пределах своей гражданской дееспособности. Любое согласие должно быть изложено простым и понятным языком, доступным для понимания ребёнком.

Фотографии, сделанные в общественных местах: применение норм Гражданского и Цифрового кодексов

> Статья 4 Цифрового кодекса
>
> Статья 19 Гражданского кодекса

Статья 19 Гражданского кодекса устанавливает общее правило, согласно которому изображение человека (картина, фотография, кинофильм и т. п.) не может быть опубликовано или распространено без согласия этого человека. Одновременно Гражданский кодекс предусматривает исключение: согласие не требуется, если изображение получено в общественном месте, а также в иных случаях, прямо предусмотренных законом. Такое регулирование традиционно направлено на обеспечение баланса между правом на неприкосновенность частной жизни и свободой получения и распространения информации в общественных местах. Однако данный подход не полностью соответствует правовому режиму, установленному Цифровым кодексом.

В цифровой среде изображения человека квалифицируются как персональные данные, поскольку позволяют прямо или косвенно идентифицировать физическое лицо. Следовательно, сбор, хранение, публикация и распространение фотографий и видеоматериалов в цифровой форме подпадают под действие законодательства о защите персональных данных. Согласно статье 4 Цифрового кодекса, при регулировании отношений в цифровой среде приоритет имеет Цифровой кодекс. Если нормы других законов затрагивают цифровую деятельность и создают противоречие, применяется Цифровой кодекс. Это означает, что исключение, предусмотренное статьёй 19 Гражданского кодекса для изображений, сделанных в общественных местах, не может автоматически применяться, если такие изображения обрабатываются или публикуются в цифровой форме.

Для ОГО это имеет важное значение:

- Сам факт того, что фотография сделана в общественном месте, не освобождает ОГО от соблюдения требований законодательства о защите персональных данных, если изображение впоследствии публикуется или распространяется в цифровом формате.
- Даже если в рамках Гражданского кодекса согласие может предполагаться ввиду публичного характера мероприятия, рекомендуется получать явное и информированное согласие на публикацию и дальнейшее использование цифровых материалов.
- Согласие на участие в мероприятии или нахождение в общественном месте не означает автоматического согласия на размещение изображения на веб-сайте, в отчётах или в социальных сетях.

Когда нормы Цифрового кодекса о персональных данных не применяются

> Статья 77(2) Цифрового кодекса

Цифровой кодекс распространяется практически на все случаи обработки персональных данных — независимо от того, осуществляется ли такая обработка организацией, государственным органом или физическим лицом. Если организация собирает, хранит, использует или передаёт персональные данные в цифровой форме, применяется Цифровой кодекс. Если информация находится на бумажных или иных материальных носителях, отдельные требования по защите информации персонального характера также продолжают действовать.

Однако существует одно важное исключение: закон не применяется, когда физическое лицо обрабатывает персональные данные исключительно в личных, семейных или бытовых целях, если при этом не нарушаются права других лиц. Это исключение не распространяется на организации. Как только персональные данные обрабатываются в рамках организационной, профессиональной или общественной деятельности, Кодекс применяется в полном объеме. Когда ОГО собирает или использует персональные данные в рамках своей организационной деятельности, например, в проектах, услугах или мероприятиях, Цифровой кодекс применяется, даже если данные обрабатываются только одним сотрудником или в небольших масштабах. ОГО *не может* ссылаться на исключение для «личного использования».

ПРИМЕР ИЗ ПРАКТИКИ: В КАКИХ СЛУЧАЯХ ПРИМЕНЯЕТСЯ ЦИФРОВОЙ КОДЕКС?

Жена исполнительного директора Гражданской инициативы «Бирге» (ГИБ) посещает корпоративное мероприятие и делает групповую фотографию. Она распечатывает снимок и размещает его дома в рамке. Исполнительный директор видит фотографию и решает разместить её на главной странице веб-сайта ГИБ.

ВОПРОС: РАСПРОСТРАНЯЮТСЯ ЛИ ТРЕБОВАНИЯ ЦИФРОВОГО КОДЕКСА О ПЕРСОНАЛЬНЫХ ДАННЫХ НА ДАННУЮ ФОТОГРАФИЮ?

ОТВЕТ: Если фотография распечатана и хранится дома для личных целей, это подпадает под исключение для личного использования, и положения Цифрового кодекса не применяются. Однако если фотография размещается на веб-сайте организации, она становится объектом обработки в цифровой среде в рамках организационной деятельности. В этом случае применяется Цифровой кодекс. Следовательно, размещение фотографии в интернете допустимо только после получения согласия всех лиц, изображённых на снимке.

Основные принципы защиты персональных данных

> Статья 78 Цифрового кодекса

В соответствии со статьей 78 Цифрового кодекса, ОГО должны соблюдать ряд ключевых принципов при обработке персональных данных:

1. *Законность, добросовестность и прозрачность.* Персональные данные должны обрабатываться на законных основаниях, добросовестно и прозрачно по отношению к субъекту персональных данных. До начала обработки ОГО должно убедиться, что имеется законное основание для обработки и организация готова соблюдать требования и процедуры, установленные законодательством. Люди должны понимать зачем собираются их данные, как они будут использоваться, какие права у них есть. Скрывать цели обработки или вводить бенефициаров в заблуждение запрещено.

2. *Ограничение цели обработки.* Персональные данные могут собираться только для конкретных, чётко определённых и законных целей. Изменение или расширение целей без согласия лица не допускается, если иное прямо не предусмотрено законом. Например, если данные собирались для регистрации на мероприятие, их нельзя использовать для рассылки фандрайзинговых писем без отдельного согласия.

3. *Минимизация данных.* ОГО обязано собирать минимально необходимый объём данных, достаточный для достижения заявленной цели. Если для регистрации достаточно имени и электронной почты, запрашивать номер телефона не следует.

4. *Достоверность.* Персональные данные должны быть точными и актуальными. Субъект персональных данных имеет право требовать исправления неточных сведений. Этот принцип особенно важен, если неточность может привести к негативным последствиям. Например, ОГО обязано обеспечивать корректность и регулярное обновление кадровых данных сотрудников. Ошибки в ИНН или адресе могут повлиять на выплаты или оформление налоговых документов. Первичные данные должны быть точными и при необходимости обновляться.

5. *Ограничение срока хранения.* Персональные данные должны храниться только в течение срока, необходимого для достижения цели обработки. После достижения цели данные подлежат безопасному уничтожению[2]. ОГО не следует бессрочно хранить устаревшие списки участников, заявки или аналогичные документы. Если проект завершён и данные более не требуются, они должны быть надлежащим образом уничтожены.

   Исключение: Некоторые документы подлежат обязательному хранению в течение установленных законом сроков. Например, кадровые документы, подтверждающие трудовую деятельность (приказы о приёме и увольнении, трудовые договоры, расчётные ведомости), должны храниться 60 лет. Для определения сроков хранения следует руководствоваться Перечнем типовых

[2] «Безопасное уничтожение» означает обеспечение невозможности восстановления или повторного прочтения персональных данных после утраты необходимости в их хранении. Для бумажных документов это, как правило, означает измельчение или сжигание. Для электронных файлов — использование программного обеспечения, которое обеспечивает безвозвратное удаление данных (а не просто перемещение файла в корзину), либо при необходимости физическое уничтожение носителя информации. Цель безопасного уничтожения — исключить возможность последующего восстановления, несанкционированного доступа или неправомерного использования данных.

управленческих архивных документов, образующихся в процессе деятельности государственных и негосударственных организаций, с указанием сроков их хранения.

6. *Целостность и конфиденциальность.* Персональные данные должны храниться безопасно и быть защищены от несанкционированного доступа, незаконного изменения, удаления, утраты. ОГО должно применять защиту паролями, безопасное хранение (в физической или цифровой форме), разграничение прав доступа. Доступ к персональным данным должен иметь только уполномоченный персонал.

7. *Ответственность.* Владелец персональных записей несёт ответственность за соблюдение всех указанных принципов и обязан быть способен подтвердить выполнение требований законодательства. ОГО должно иметь внутренние политики, инструкции, процедуры и практики, которые демонстрируют соблюдение Цифрового кодекса.

Когда допускается обработка персональных данных без согласия

> Статья 79(1) Цифрового кодекса

Статья 79 перечисляет правовые основания, позволяющие организации обрабатывать персональные данные [3]. Перед сбором или использованием персональных данных должно существовать как минимум одно из следующих оснований:

1. *Договор.* Обработка допускается, если она необходима для заключения или исполнения договора с лицом (или с лицом, действующим от его имени), а также для совершения действий по просьбе лица до заключения договора. Пример: сбор банковских реквизитов консультанта для выплаты вознаграждения по договору оказания услуг.

2. *Юридическая обязанность.* Обработка допускается, если она требуется законом или иным нормативным правовым актом. Это включает обязанности по отчётности, требования по соблюдению законодательства и обязательства в рамках государственных программ. Такие действия являются обязательными по закону, поэтому согласие не требуется. Пример: обработка персональных данных сотрудников (размер заработной платы, ИНН, паспортные данные) для исполнения требований налогового и трудового законодательства.

3. *Защита жизненно важных интересов.* Обработка допускается, если она необходима для защиты жизни, здоровья или безопасности лица. Пример: передача информации о бенефициаре службам экстренной помощи во время кризисной ситуации.

[3] Даже при наличии законных оснований для обработки некоторых видов персональных данных может потребоваться согласие, если это прямо предусмотрено законом.

4. *Выполнение задач в общественных или социально значимых интересах.* Обработка допускается, если она действительно необходима для осуществления деятельности в общественных интересах или социально значимых задач (например, гуманитарная, экологическая деятельность или защита сообщества). Пример: сбор данных участников для гуманитарной помощи после стихийного бедствия.
5. *Законные интересы.* Обработка допускается, если она необходима для защиты законных интересов организации или третьего лица при условии, что такие интересы не нарушают права и интересы субъекта персональных данных. Пример: хранение минимальных контактных данных для предотвращения повторной подачи заявок на участие в стипендиальной программе. Это отвечает законным интересам организации и оказывает минимальное влияние на права лица.

Некоторые законные основания сформулированы достаточно широко. Несмотря на их признание законом, их применение требует осторожности и надлежащего документирования. На практике основания «законные интересы» и «выполнение задач в общественных или социально значимых интересах» являются наиболее неопределёнными и могут толковаться по-разному, что создаёт риск произвольного применения и привлечения к ответственности. В связи с этим ОГО рекомендуется документировать в письменной форме обоснование применения соответствующего основания и по возможности получать согласие даже в тех случаях, когда теоретически может применяться иное законное основание.

Получение согласия обеспечивает большую правовую определённость, повышает прозрачность деятельности и снижает риски несоблюдения законодательства. Для большинства видов деятельности ОГО согласие остаётся наиболее безопасным и юридически устойчивым основанием обработки персональных данных.

Когда необходимо получить согласие на сбор или обработку персональных данных

> Статья 79(2) Цифрового кодекса

Прежде чем собирать или использовать персональные данные, необходимо иметь законное основание – договор, юридическая обязанность, защита жизненно важных интересов, выполнение задач в общественных интересах либо законные интересы. Если ни одно из этих оснований не применимо, необходимо получить ясное, понятное и добровольное согласие.

Согласие является одним из основных законных оснований, позволяющих организации осуществлять обработку персональных данных на законных основаниях. Получив согласие, ОГО вправе обрабатывать персональные данные без необходимости доказывать применимость других оснований, предусмотренных законом. В следующем разделе рассматриваются требования и порядок получения согласия.

Как получить согласие на сбор и обработку персональных данных

> Статья 79(2-6) Цифрового кодекса
>
> *См. также* Порядок получения согласия субъекта персональных данных на сбор и обработку его персональных данных, в том числе в форме электронного документа, включая цели предоставления государственных и муниципальных услуг (далее – Приказ № 27)

Часть 4 статьи 79 Цифрового кодекса устанавливает четыре условия действительности согласия. Все четыре условия должны соблюдаться одновременно. Если хотя бы одно из них отсутствует, согласие может быть оспорено и признано недействительным.

1. *Добровольность.* Согласие должно быть дано свободно, без давления, принуждения или скрытых негативных последствий. Лицо должно иметь реальную возможность выбрать — согласиться или отказаться. Отказ от согласия не должен приводить к исключению из мероприятия или к неблагоприятным последствиям, если соответствующие данные не являются строго необходимыми для участия. Пример: Участник должен иметь возможность зарегистрироваться на мероприятие без обязательного согласия на получение рассылки или публикацию фотографий. Если персональные данные не являются строго необходимыми для участия, отказ от их предоставления не может служить основанием для отказа в доступе к мероприятию.
2. *Конкретность.* Согласие должно быть связано с чётко определёнными и ограниченными целями. Недопустимо получать одно общее или «рамочное» согласие на все возможные действия. Для каждой отдельной цели требуется отдельное согласие, и каждая цель должна быть описана отдельно. Человек должен иметь возможность согласиться с некоторыми целями и отказаться от других.
3. *Информированность.* Согласие действительно только тогда, когда лицо ясно понимает, что будет происходить с его данными. Сложные юридические формулировки или технические термины нарушают принцип информированности. Информация должна быть изложена простым и понятным языком. Следует избегать длинных текстов, скопированных из закона, а также размытых формулировок вроде «для операционных нужд». Лицу должно быть разъяснено:
   - кто собирает данные (наименование ОГО, адрес, контактные данные);
   - какие данные собираются (например, ФИО, номер телефона, фотография, адрес электронной почты);
   - цель сбора (регистрация, рассылка, оказание услуги, отчётность донору и т. д.);
   - предполагаемые способы использования (хранение, размещение в социальных сетях, проверка третьими лицами и т. п.);

- какие третьи лица получат данные (конкретные доноры, партнёры, государственные органы, поставщики услуг; недопустимы формулировки «другие партнёры»);
- срок действия согласия (конкретная дата, период или иные чёткие критерии).

Если срок согласия различается по разным целям, он должен быть указан отдельно по каждой цели.

4. *Осознанность.* Согласие должно выражаться через активное и осознанное действие. Молчание или бездействие не считаются согласием. Человек должен четко выразить свое согласие, например, подписав форму, поставив галочку, нажав «Я согласен» или отправив подтверждающее электронное письмо. Это означает, что вы не должны автоматически добавлять людей в списки рассылки или использовать их личные данные только потому, что они поделились с вами своими контактными данными.

Цифровой кодекс позволяет давать согласие в любой форме, включая бумажные формы, электронные документы, онлайн-формы с галочками, электронные письма и т. д. Ключевое правило заключается в том, что организация должна иметь возможность доказать факт получения согласия. В случае возникновения спора бремя доказывания лежит на организации, а не на субъекте персональных данных. Поэтому ОГО следует хранить подписанные бумажные формы, электронные подтверждения и иметь возможность связать согласие с конкретным лицом и целью обработки. Человек может отозвать свое согласие в любое время. Процедура отзыва не должна быть сложнее, чем предоставление согласия (статья 79(5)).

Когда согласие недействительно

Согласие автоматически становится ничтожным, если оно было получено любым из следующих способов (статья 79(3)):

1. *Скрыто среди других запросов***.** Согласие считается недействительным, если оно не представлено четко как запрос на согласие. Пример: Положение о согласии «скрыто» внутри длинного договора, регистрационной формы или пользовательского соглашения без чёткого указания, что лицо просят дать согласие на обработку персональных данных. Согласие должно быть выделено и сформулировано ясно, а не маскироваться среди других условий.
2. *Неясная формулировка.* Согласие недействительно, если запрос изложен таким образом, что лицо не может понять его содержание. Пример: Использование сложного юридического языка, абстрактных или расплывчатых формулировок либо предоставление информации на языке, который человек не понимает. Если лицо не понимает, на что именно оно соглашается, такое согласие не является действительным.
3. *Запрос согласия при наличии иного законного основания.* Согласие недействительно, если оно запрашивается в ситуации, когда у организации уже имеется иное законное основание для обработки персональных данных без

согласия. Пример: Запрос согласия на обработку персональных данных сотрудников, которые обязаны обрабатываться в силу требований трудового или налогового законодательства; либо запрос согласия на действия, необходимые для исполнения договора. В таких случаях согласие не только не требуется, но и не имеет юридической силы.

Проверочный список: как получить действительное согласие

- √ Используйте чёткую и отдельную форму согласия (в бумажной или электронной форме) при сборе персональных данных.
- √ Явно отделяйте запрос согласия от договоров, регистрационных форм и иных документов.
- √ Используйте простой и понятный язык, доступный для лиц без юридической подготовки.
- √ В форме согласия чётко указывайте: кто осуществляет сбор персональных данных; какие персональные данные собираются; для каких целей они собираются и как будут использоваться; кому будут переданы персональные данные; срок действия согласия.
- √ Получайте отдельное согласие по каждой цели обработки и избегайте «общего» или рамочного согласия.
- √ Обеспечивайте свободу выбора: лицо должно иметь возможность согласиться на одни цели и отказаться от других.
- √ Храните надёжные доказательства получения согласия на протяжении всего срока использования данных (подписанные бумажные формы, электронные подтверждения, журналы регистрации, реестры и т. п.).
- √ Удаляйте записи о согласии, когда они более не требуются.
- √ Информируйте лиц об их правах, включая право отозвать согласие.
- √ Обеспечьте простой и понятный механизм отзыва согласия — процедура отзыва не должна быть сложнее, чем процедура его предоставления.

Практические примеры согласия

РЕГИСТРАЦИЯ НА МЕРОПРИЯТИЕ

Используйте регистрационную форму для сбора только тех персональных данных, которые действительно необходимы для организации мероприятия (например, ФИО и контактные данные). Участие в мероприятии не должно ставиться в зависимость от согласия на дополнительные (необязательные) виды обработки. Любая необязательная обработка (рассылка, фото- и видеосъёмка, передача данных партнёрам и т. д.) должна оформляться отдельными пунктами с возможностью выбора. В противном случае согласие не будет считаться добровольным и может быть признано недействительным.

Примерная формулировка:

☐ *Я приму участие в мероприятии. Я понимаю, что предоставление моих данных необходимо для регистрации на мероприятие и будет использовано для рассылки уведомлений о мероприятии.*

☐ *Я хотел(а) бы получать новостные рассылки и обновления от [Название организации]*

☐ *Я согласен(на) на фото- и/или видеосъемку во время мероприятия.*

ОНЛАЙН-ФОРМЫ

При получении согласия онлайн необходимо обеспечить, чтобы участник указал свои контактные данные; ознакомился с кратким и понятным уведомлением о конфиденциальности; выразил согласие активным действием (например, нажатием кнопки «Согласен»). Обязательно сохраняйте отметку времени или системную запись как доказательство получения согласия.

Примерная формулировка:

☐ *«Нажимая “Согласен”, я подтверждаю, что ознакомился(лась) с уведомлением о конфиденциальности и даю согласие [Название организации] на обработку моих персональных данных для выбранных выше целей».*

Обратите внимание: многие онлайн-сервисы автоматически собирают IP-адреса. Если IP-адреса не требуются для достижения цели обработки, отключите их сбор или удаляйте такие данные незамедлительно. Если IP-адреса используются для конкретной цели, необходимо прямо информировать участников и объяснить, зачем они нужны.

ФОТОГРАФИИ И ВИДЕО

Согласие на использование фотографий или видеоматериалов всегда следует получать отдельно, поскольку оно не является обязательным для участия в большинстве мероприятий.

Примерная формулировка:

Я даю согласие на использование моего фото и/или видео [Название организации] в публикациях, отчётах, на веб-сайте и в социальных сетях. Я понимаю, что изображение не будет использоваться в коммерческих целях и что я могу отозвать согласие в любое время.

☐ *Согласен(на)*

☐ *Не согласен(на)*

ПЕРЕДАЧА ДАННЫХ ДОНОРАМ

Если персональные данные планируется передавать донору или партнёру, это должно быть прямо указано в форме согласия и оформлено отдельным пунктом.

Примерная формулировка:

Ваше имя, название организации и адрес электронной почты будут переданы нашему донору, [Имя донора], с целью демонстрации результатов проекта и обеспечения прозрачности. Ваши данные не будут использоваться ни для каких других целей.

☐ *Я согласен(на) на передачу моих данных [Имя донора]*

☐ *Я не согласен(на) на передачу моих данных [Имя донора]*

РЕСУРСЫ И ШАБЛОНЫ

Образец формы согласия (в разработке): Государственное агентство по защите персональных данных готовит стандартную форму согласия. Следите за обновлениями на их официальном сайте: dpa.gov.kg.

Существующий шаблон: Приложение к приказу N27 содержит типовую форму согласия, обязательную для государственных и муниципальных органов. ОГО могут адаптировать этот шаблон для своих мероприятий и деятельности.

Обработка персональных данных повышенного риска и обязанность проведения оценки воздействия

> Статья 82 Цифрового кодекса

Статья 82 вводит обязанность проводить оценку воздействия на защиту персональных данных до начала отдельных видов обработки, связанных с повышенным риском. Такая оценка представляет собой предварительный анализ рисков, направленный на предотвращение возможного нарушения прав и законных интересов субъектов персональных данных. Большинство стандартных видов деятельности ОГО не требуют проведения оценки воздействия. Однако она обязательна в следующих случаях:

1. **Автоматизированное принятие решений , влияющее на людей** . Это относится к случаям, когда персональные данные используются для автоматической оценки людей (без участия человека), и принятое решение имеет последствия, затрагивающие жизнь человека. Пример: ОГО использует автоматизированную систему (ИИ), которая определяет, кто получит помощь или пособия.
2. **Обработка специальных категорий персональных данных более чем 1 000 лиц.** Оценка воздействия обязательна, если обрабатываются специальные категории персональных данных в отношении более 1 000 человек. Примеры: ОГО реализует крупный медицинский проект и собирает данные о состоянии здоровья более чем 1 000 бенефициаров; или ОГО проводит национальное исследование, в рамках которого собираются сведения о политических взглядах более 1 000 респондентов. Перед сбором специальных категорий данных необходимо тщательно оценить, действительно ли такие данные необходимы для достижения цели проекта. Если цель может быть достигнута без их сбора, их не следует запрашивать. По возможности, обезличьте и надежно уничтожьте персональные данные, когда они больше не нужны.
3. **Систематическое автоматизированное наблюдение в общественных местах.** Оценка воздействия требуется, если используются технические средства для

регулярного мониторинга общественных пространств, например: системы видеонаблюдения; технологии распознавания лиц; иные автоматизированные системы отслеживания. Разовые фотографии на мероприятиях не подпадают под данное требование.

Государственное агентство по защите персональных данных должно опубликовать два перечня операций – (1) которые всегда требуют проведения оценки воздействия и (2) которые такой оценки не требуют. До публикации соответствующих перечней ОГО следует руководствоваться положениями статьи 82 Цифрового кодекса.

Удаление персональных данных

> Статья 83 Цифрового кодекса

Персональные данные не должны храниться дольше, чем это необходимо для достижения целей обработки. Кроме того, субъект персональных данных вправе требовать их удаления в предусмотренных законом случаях. ОГО обязано удалить персональные данные без неоправданной задержки (в том числе по запросу лица), если имеется хотя бы одно из следующих оснований:

1. **Данные больше не нужны.** Если цель, для которой были собраны данные, достигнута, данные должны быть удалены. Пример: ОГО собрала контактные данные участников тренинга. Тренинг завершен, отчетность составлена и данные больше не нужны. Данные следует удалить.
2. **Прекращение законного основания обработки.** Если законное основание для обработки более не существует, персональные данные подлежат удалению. Это включает случаи, когда лицо отзывает согласие, и при этом отсутствуют иные законные основания (например, обязанность по закону) для дальнейшего хранения данных. Пример: Лицо отзывает согласие на получение рассылки. Если иных оснований для хранения его электронного адреса нет, адрес должен быть удалён из базы рассылки.
3. **Удовлетворение возражения против обработки.** Если лицо возражает против обработки его персональных данных, и после рассмотрения возражения организация приходит к выводу о необоснованности дальнейшей обработки, данные подлежат удалению. Пример: Бенефициар возражает против включения его данных в базу. После проверки ОГО признаёт, что дальнейшая обработка не требуется, и удаляет данные *(см. также статью 84 Цифрового кодекса)*.

Статья 83 предусматривает случаи, когда персональные данные могут быть сохранены, даже если формально имеются основания для их удаления. ОГО вправе продолжить хранение данных исключительно в следующих законных целях:

1. **Свобода выражения мнения.** Данные могут храниться, если это необходимо для осуществления права на свободу выражения мнения (например, в журналистской деятельности).

2. **Научные, исторические, статистические или архивные цели.** Данные могут храниться в законных исследовательских или архивных целях при условии наличия соответствующих мер защиты. Однако это не означает, что данные можно хранить неограниченно долго «на всякий случай». Цель должна быть реальной и юридически обоснованной.
3. **Предъявление или защита от правовых требований.** Данные могут храниться, если они необходимы для предъявления исковых требований; защиты от требований; защиты прав организации. Пример: Хранение кадровых документов в период трудового спора.
4. **Обязанность хранения по закону.** Если законодательство устанавливает обязательный срок хранения определённых документов, организация обязана соблюдать этот срок, даже при наличии запроса на удаление. Для определения сроков хранения следует руководствоваться *Перечнем типовых управленческих архивных документов, образующихся в деятельности государственных и негосударственных организаций, с указанием сроков их хранения*.

Таким образом, если персональные данные более не нужны либо лицо отзывает согласие и отсутствуют иные законные основания для их хранения, данные должны быть удалены. Сохранение допускается только в случаях, прямо предусмотренных законом (например, для исполнения юридической обязанности, научных целей или защиты прав).

Рассмотрение возражений против обработки персональных данных

> Статья 84 Цифрового кодекса

Субъект персональных данных вправе возразить против отдельных способов обработки его персональных данных (например, включения в автоматизированную базу данных) либо против определённых целей обработки (например, использования данных для анализа или отчётности). Организация обязана незамедлительно прекратить обработку в оспариваемом способе или для оспариваемой цели, если возражение касается следующих случаев:

1. **Автоматизированное принятие решений.** Если данные используются для автоматизированного принятия решений в отношении человека, этот человек имеет полное право возражать. Это относится к решениям, принимаемым без существенного участия человека, а также к автоматизированной оценке, ранжированию или исключению, которые затрагивают права этого человека, его доступ к услугам или другие возможности.
2. **Несправедливая или дискриминационная обработка.** Даже если обработка формально соответствует закону, она должна быть также добросовестной и недискриминационной. Если обработка носит несправедливый или дискриминационный характер, лицо вправе возразить против неё.

3. **Возражение, связанное с отказом от цифровых записей.** Лицо может возразить против обработки его персональных данных в цифровой форме, например отказаться от хранения или передачи данных в цифровом виде. По возможности организация должна предоставить нецифровой или ограниченный цифровой формат взаимодействия.
4. **Возражение в связи с уходом из цифрового сообщества.** Если человек покидает цифровое сообщество[4] (например, онлайн-платформу, сеть или систему), он может возражать против дальнейшей обработки своих данных, связанных с этим сообществом. После выхода человека дальнейшая обработка данных, связанная с этим сообществом, может утратить законное основание.
5. **Защита цифровой идентичности.** Цифровой кодекс закрепляет право лица определять, каким образом оно представлено и идентифицируется в цифровой среде, включая цифровые сообщества (например, онлайн-платформы, сети, базы данных проектов, администрируемые ОГО). Обработка должна быть прекращена, если она нарушает право лица самостоятельно определять свою цифровую идентичность, если иное прямо не предусмотрено законом. Это новое и значимое положение Цифрового кодекса, связывающее защиту персональных данных с правом на идентичность и автономию в цифровом пространстве.

При получении возражения ОГО обязана временно приостановить обработку соответствующих цифровых записей на период рассмотрения и провести оценку обоснованности возражения. В течение семи рабочих дней ОГО должна предоставить мотивированное письменное решение с указанием будет ли обработка прекращена или продолжена и правовых и фактических оснований принятого решения. Молчание или затягивание рассмотрения не допускаются. Если лицо не согласно с решением организации, оно вправе подать жалобу в Государственное агентство по защите персональных данных и обратиться в суд.

Обработчики персональных данных

> Статья 86 Цифрового кодекса

Если ОГО передаёт персональные данные подрядчикам или поставщикам услуг (например, IT-компаниям, бухгалтерам, консультантам, ивент-агентствам, платформам для опросов), она сохраняет полную ответственность за соблюдение требований Цифрового кодекса. Такие лица выступают в качестве обработчиков персональных данных и вправе осуществлять обработку исключительно по поручению ОГО; в соответствии с ее письменными инструкциями; для чётко определённых целей. Передача обработки на аутсорсинг не освобождает ОГО от юридической

[4] Статья 1(88) Цифрового кодекса: «цифровое сообщество - объединение субъектов правоотношений в цифровой среде независимо от наличия у него статуса юридического лица, созданное ими по их собственной инициативе и на началах добровольности для реализации задач его участников на основании общих правил по развитию и (или) использованию объектов правоотношений в цифровой среде».

ответственности. Обработчик не вправе привлекать субподрядчиков без предварительного письменного согласия ОГО.

Привлечение обработчика требует заключения *письменного договора* или иного *правового акта*, в котором должны быть чётко определены цель обработки, срок обработки, виды обрабатываемых персональных данных и категории субъектов персональных данных. Договор также должен предусматривать обязанность обработчика ограничивать доступ к персональным данным, действовать строго по письменным инструкциям ОГО, оказывать содействие в исправлении или удалении данных и вести учёт и хранить доказательства соблюдения требований законодательства.

Государственное агентство по защите персональных данных должно опубликовать рекомендуемые типовые формы договоров с обработчиками. ОГО рекомендуется использовать такие типовые формы либо привести существующие договоры в соответствие с ними для снижения правовых и операционных рисков.

Как ОГО должны обеспечивать защиту персональных данных

> Статья 88 Цифрового кодекса
>
> *См. также* : Постановление Правительства Кыргызской Республики от 21 ноября 2017 г. № 760 об утверждении требований по обеспечению безопасности и защиты персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных (Постановление № 760)

ОГО обязаны принимать практические технические и организационные меры для защиты персональных данных. Для соблюдения требований законодательства ОГО следует:

1. **Взять на себя ответственность за защиту данных.** Обеспечивать защиту персональных данных, баз данных и цифровых систем как при внутренней обработке, так и при передаче данных подрядчикам.
2. **Встраивать защиту данных в цифровые системы изначально.** При выборе цифровых решений необходимо использовать безопасные платформы; ограничивать доступ к персональным данным; собирать только необходимые данные; избегать хранения специальных категорий данных, если это не является необходимым; и по возможности применять шифрование и обезличивание.
3. **Вести учёт операций обработки.** Поддерживать базовые журналы или реестры, отражающие какие данные обрабатываются, с какой целью, кем осуществляется обработка.
4. **Назначить ответственное лицо.** Если в организации более десяти сотрудников, необходимо назначить сотрудника или привлечённого специалиста, ответственного за вопросы защиты персональных данных и контроль

соблюдения требований. Небольшим ОГО рекомендуется определить такое ответственное лицо, хотя это и не является обязательным требованием.

5. **Обучать сотрудников и партнёров.** Проводить практическое обучение по правилам защиты персональных данных, внутренним процедурам и распространённым рискам (фишинг, слабые пароли, случайное раскрытие информации).
6. **Соблюдать технические требования безопасности.** Необходимо учитывать и применять технические стандарты защиты, утверждённые Кабинетом Министров Кыргызской Республики, с учётом уровня чувствительности обрабатываемых данных (Постановление № 760).

Постановление № 760 устанавливает обязательные требования для всех организаций, обрабатывающих персональные данные в информационных системах, включая ОГО. Вводится система уровней защищённости в зависимости от степени угроз:

1. Синий уровень — минимальный риск (базовые организационные меры).
2. Зелёный уровень — средний риск (усиленные меры, включая шифрование).
3. Жёлтый уровень — высокий риск (централизованное управление, электронные журналы учёта, системы обнаружения вторжений).
4. Красный уровень — критический риск (максимальные меры защиты, защищённые каналы связи, сертифицированные средства защиты, ежегодные аудиты).

ОГО могут воспользоваться онлайн-модулем Государственного агентства по защите персональных данных для самооценки уровня риска: https://self-rating.dpa.gov.kg/. По результатам (синий–красный уровень) необходимо внедрить соответствующие меры защиты.

ПРИМЕЧАНИЕ ДЛЯ ОГО

Постановление N760 устанавливает стандарты надлежащей защиты, ожидаемые от всех, кто обрабатывает персональные данные в информационных системах. Это означает, что ОГО следует:

- √ Определить свой уровень риска в зависимости от характера обрабатываемых данных. Избегать сбора избыточных данных, которые могут повысить уровень риска (например, сведения о состоянии здоровья сотрудников или бенефициаров).
- √ Внедрить базовые меры безопасности (внутренние политики, назначение ответственного лица, контроль доступа, резервное копирование, шифрование).
- √ При обработке специальных категорий данных или больших массивов данных (например, сведения о здоровье, уязвимых группах) применять усиленные меры защиты.

Трансграничная передача персональных данных: что это значит и как соблюдать требования законодательства

> Статья 89 Цифрового кодекса

Многие ОГО в Кыргызстане работают с зарубежными партнерами, донорами и сетями. Это часто предполагает передачу персональных данных за пределы страны, например: направление списков участников донору за рубежом; использование облачных сервисов или программного обеспечения, серверы которых расположены в других государствах; передача паспортных данных или иных документов гостиницам и авиакомпаниям за пределами Кыргызской Республики; физическое перемещение документов, содержащих персональные данные, при выезде на конференции или мероприятия за границу.

Согласно статье 89, Государственное агентство по защите персональных данных утверждает и публикует перечень иностранных государств, обеспечивающих адекватный уровень защиты персональных данных, сопоставимый с требованиями Цифрового кодекса. Перед передачей персональных данных за границу ОГО обязана проверить, включено ли соответствующее государство в данный перечень. Если персональные данные передаются в страну, включённую в перечень:

- передача допускается в соответствии с Цифровым кодексом;
- такая передача не может быть запрещена или ограничена;
- при этом продолжают применяться общие принципы защиты персональных данных (ограничение цели, безопасность, минимизация и т. д.).

Если государство не включено в перечень стран с адекватным уровнем защиты, трансграничная передача допускается только в установленных законом случаях:

1. **С согласия субъекта персональных данных.** Пример: Участник мероприятия прямо соглашается на передачу его персональных данных иностранному донору или партнёру.
2. **Для целей договора.** Передача необходима для заключения или исполнения договора с участием лица. Пример: Передача данных в рамках участия в международной программе.
3. **Для защиты жизненно важных интересов.** Пример: Передача медицинской информации в чрезвычайной ситуации, когда невозможно получить согласие.
4. **На основании международных договоров или требований законодательства.** Если передача предусмотрена международными договорами, обязательными для Кыргызской Республики, либо требуется законодательством в целях защиты конституционного строя, обороны или безопасности.

5. **При наличии договорных гарантий защиты.** ОГО вправе передать персональные данные даже в государство, не обеспечивающее адекватный уровень защиты, при условии заключения договора, обеспечивающего надлежащую защиту прав субъектов персональных данных. На практике это означает, что ОГО может передавать персональные данные иностранному донору или поставщику услуг (обработчику), если заключён письменный договор и получатель обязуется обеспечивать защиту персональных данных в соответствии со стандартами Цифрового кодекса. Конкретные договорные положения, обеспечивающие «адекватную защиту», будут определены Государственным агентством по защите персональных данных. После их публикации ОГО следует привести в соответствие договоры с донорами, партнёрами и обработчиками.

ПРИМЕЧАНИЕ ДЛЯ ОГО

Практическая проблема заключается в том, что перечень государств с адекватным уровнем защиты пока не опубликован. До его утверждения ОГО не может самостоятельно точно определить, соответствует ли правовая система другого государства уровню защиты, установленному в Кыргызской Республике. В целях демонстрации добросовестности и соблюдения законодательства до публикации разъяснений рекомендуется прямо указывать в форме согласия возможность трансграничной передачи персональных данных, а также получать информированное согласие субъектов персональных данных на такую передачу.

Обращение с бумажными документами и нецифровой информацией персонального характера

> Статья 91 Цифрового кодекса

Бумажные документы тоже требуют надлежащего обращения. Если ОГО осуществляет обработку информации персонального характера без использования цифровых средств (например, ведёт рукописные записи, бумажные списки или хранит личные дела в папках), она всё равно обязана соблюдать основные принципы обработки персональных данных, установленные Цифровым кодексом, и иметь законное основание для такой обработки. Обработка на бумажных носителях не выводит организацию из сферы действия законодательства.

При этом ОГО не обязана применять к физическим документам полный комплекс цифровых мер безопасности, однако она должна ограничивать доступ к таким материалам; обеспечивать их хранение в безопасном месте; вести базовый учёт мест хранения и лиц, имеющих доступ к этим документам.

Уполномоченный орган по защите персональных данных

> Статья 90 Цифрового кодекса
>
> *См. также* Положение о Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики, утвержденное Постановлением Кабинета Министров Кыргызской Республики от 30 января 2026 года № 46.

Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики (уполномоченный орган по защите персональных данных) является специализированным государственным органом, осуществляющим регулирование и надзор в сфере защиты персональных данных.

Уполномоченный орган обеспечивает законность и безопасность сбора, хранения и использования персональных данных; осуществляет контроль за соблюдением требований Цифрового кодекса; рассматривает обращения и жалобы субъектов персональных данных; проводит проверки; выносит обязательные для исполнения предписания; требует исправления, блокирования или удаления незаконно обрабатываемых данных; применяет меры реагирования при выявлении нарушений. Он также публикует разъяснения, рекомендации и типовые формы; ведёт официальные реестры; взаимодействует с иностранными регуляторами; осуществляет просветительскую деятельность (отчёты, обучение, консультации).

Для ОГО уполномоченный орган выполняет двойную функцию: контрольную — вправе проводить проверки, рассматривать жалобы и выносить обязательные решения; методическую — является официальным источником разъяснений, рекомендаций и шаблонов, на которые ОГО может опираться при применении Цифрового кодекса. Также субъекты персональных данных вправе обращаться в уполномоченный орган с жалобами на действия ОГО.

Уполномоченный орган также ведёт публичный реестр, содержащий информацию об инцидентах в сфере персональных данных; проведённых проверках; вынесенных обязательных решениях; случаях привлечения к ответственности за нарушения законодательства. Данный реестр размещается на официальном сайте и повышает прозрачность. Это означает, что серьёзные нарушения со стороны организаций могут стать публично известными.

Для снижения правовых и репутационных рисков рекомендуется регулярно отслеживать информацию на официальном сайте уполномоченного органа; использовать опубликованные шаблоны и рекомендации; своевременно и добросовестно реагировать на запросы уполномоченного органа; рассматривать жалобы и обращения как официальные процедуры, требующие документирования и последующего контроля.

КОНТАКТЫ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Официальный сайт: https://dpa.gov.kg.

Консультационная поддержка по WhatsApp: +996 998 950 350.

Ответственность за нарушение законодательства о персональных данных

> Кодекс Кыргызской Республики о правонарушениях
>
> *Статья 228–3. Нарушение прав принципалов данных*

Применяется, если владелец персональных записей не соблюдает права лица в отношении его персональных или цифровых данных, и это причиняет вред его правам или законным интересам. Нарушениями признаются:

- отказ предоставить информацию об обработке персональных данных или отказ в доступе к ним;
- непринятие мер по исправлению неточных или неполных данных;
- неисполнение требования об удалении персональных данных или прекращении их обработки после законного запроса или возражения.

Штрафы: 2 000 сомов — для физических лиц; 5 000 сомов — для юридических лиц.

> Кодекс Кыргызской Республики о правонарушениях
>
> *Статья 228–6. Недобросовестные действия в цифровой среде (в контексте обработки персональных данных)*

Применяется при недобросовестной обработке персональных данных в нарушение Цифрового кодекса. Обработка признаётся недобросовестной, если она включает:

- принятие решений на основе неточных, неполных или устаревших данных;
- вмешательство в идентичность лица (например, указание национальности, религии, гендерной идентичности или политических взглядов без согласия или игнорирование предоставленной человеком информации);
- дискриминационное использование персональных данных;
- сбор избыточных данных сверх необходимого;
- принудительное или «связанное» согласие (обуславливание услуги несвязанной обработкой);
- отсутствие предварительного чёткого информирования о целях обработки.

Штрафы: 5 000 сомов — для физических лиц; 10 000 сомов — для юридических лиц. При повторном нарушении в течение года: 10 000 сомов и 25 000 сомов соответственно.

> Кодекс Кыргызской Республики о правонарушениях
>
> *Статья 228–7. Нарушение прав участников рассмотрения споров в цифровой среде*

Нарушение имеет место, если руководитель Государственного агентства по защите персональных данных не принимает решение по спору в установленный срок. Данная

норма касается бездействия регулятора и не устанавливает обязанностей для ОГО. Однако она важна для ОГО, подающих жалобы, поскольку гарантирует своевременное рассмотрение обращения.

Штраф: 10 000 сомов — для должностных лиц.

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

Применяется при нарушении установленных законодательством требований к сбору, хранению, обработке, защите, передаче или распространению персональных данных, если деяние не образует состава преступления. Нарушения включают:

- сбор или обработку персональных данных без законного основания (например, без действительного согласия);
- хранение данных без надлежащих мер защиты;
- передачу или распространение данных без правовых оснований;
- иное несоблюдение обязательных требований законодательства.

Штрафы: 7 500 сомов — для физических лиц; 10 000 сомов — для должностных лиц; 65 000 сомов — для юридических лиц. При повторном нарушении в течение года: 25 000 сомов; 30 000 сомов; 120 000 сомов соответственно.

Важно: В соответствии с Цифровым кодексом регистрация в реестре владельцев персональных данных больше не требуется. Соответственно, штрафы за отсутствие регистрации или ошибки в регистрации не применяются.

> Кодекс Кыргызской Республики о правонарушениях
>
> *Статья 413–3. Трансграничная передача персональных данных с нарушением установленного законодательством порядка*

Применяется при передаче персональных данных за пределы Кыргызской Республики с нарушением установленной процедуры, если деяние не образует состава преступления. Нарушения включают:

- передачу данных в страну без подтверждения адекватного уровня защиты;
- передачу без явного согласия субъекта либо иного законного основания;
- передачу без надлежащих гарантий и документального оформления.

Штрафы: 15 000 сомов — для физических лиц; 17 500 сомов — для должностных лиц; 65 000 сомов — для юридических лиц. При повторном нарушении в течение года: 30 000 сомов; 35 000 сомов; 100 000 сомов соответственно.

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

Применяется, если владелец персональных записей необоснованно отказывает субъекту в предоставлении информации об обработке его данных, за исключением случаев, прямо предусмотренных законом. На практике нарушение имеет место, если ОГО без законных оснований отказывает бенефициару, сотруднику, волонтёру или партнёру в доступе к его персональным данным. По данной статье ответственность несёт только юридическое лицо.

Штраф: 25 000 сомов — за первое нарушение; 45 000 сомов — при повторном нарушении в течение года.

> Кодекс Кыргызской Республики о правонарушениях
>
> *Статья 413–5. Неисполнение законных требований уполномоченного государственного органа по персональным данным*

Применяется, если организация или лицо не исполняет законные требования уполномоченного органа. Нарушение имеет место, если ОГО игнорирует, затягивает или отказывается выполнять обязательные предписания или запросы в пределах полномочий органа (например, об устранении нарушений или предоставлении информации).

Штрафы: 10 000 сомов — для физических лиц; 20 000 сомов — для должностных лиц; 30 000 сомов — для юридических лиц.

> Уголовный кодекс Кыргызской Республики
>
> *Статья 190. Нарушение неприкосновенности частной жизни*

Применяется при незаконном сборе, хранении, использовании или распространении сведений о частной жизни лица без его согласия, кроме случаев, установленных законом. Нарушениями признаются:

- незаконный сбор, хранение, использование или распространение конфиденциальной информации о частной жизни;
- разглашение личной или семейной тайны в СМИ, публичных выступлениях или иных публичных формах;
- совершение указанных действий с использованием служебного положения.

Данная статья обычно касается особо чувствительных сведений (о состоянии здоровья, семейной жизни, интимных отношениях и т. п.), особенно если их разглашение причинило существенный вред.

Санкция:

- за основной состав: общественные работы (40–100 часов), исправительные работы (2 месяца – 1 год) либо штраф 20 000–50 000 сомов;
- за квалифицированный состав (публичность, СМИ, злоупотребление должностью): исправительные работы (1–3 года), штраф 50 000–100 000 сомов либо лишение свободы до 5 лет с возможным лишением права занимать определённые должности.

Повышенный риск для ОГО может возникать при публикации историй, фотографий, видеоматериалов или описаний случаев, раскрывающих детали частной жизни без явного согласия или надлежащего обезличивания, особенно при работе с уязвимыми группами.

Нормативные правовые акты

При подготовке данного обзора были использованы следующие нормативные правовые акты:

- Цифровой кодекс Кыргызской Республики от 31 июля 2025 года №178 и вступил в силу 5 февраля 2026 года
- Кодекс Кыргызской Республики о правонарушениях от 28 октября 2021 года №128 (с поправками от 31 декабря 2025 года)
- Уголовный кодекс Кыргызской Республики от 28 октября 2021 года №127 (с поправками от 14 ноября 2025 года)
- Гражданский кодекс Кыргызской Республики от 8 мая 1996 года №15 (с поправками от 14 ноября 2025 года).
- 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 защищенности персональных данных
- Положение о Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики, утвержденное Постановлением Кабинета Министров Кыргызской Республики от 30 января 2026 года № 46
- Постановление Государственного органа по защите персональных данных при Кабинете Министров Кыргызской Республики об утверждении Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных, в том числе в форме электронного документа, включая цели предоставления государственных и муниципальных услуг от 15 апреля 2025 года № 27
- Приказ Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики «Об утверждении Порядка обезличивания персональных данных для проведения статистических,

социологических, исторических, медицинских и других научных и практических исследований» от 14 января 2025 года № 4

- Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных и негосударственных организаций, с указанием сроков их хранения, утвержден приказом Министерства цифрового развития Кыргызской Республики от 1 сентября 2024 года № 3-д