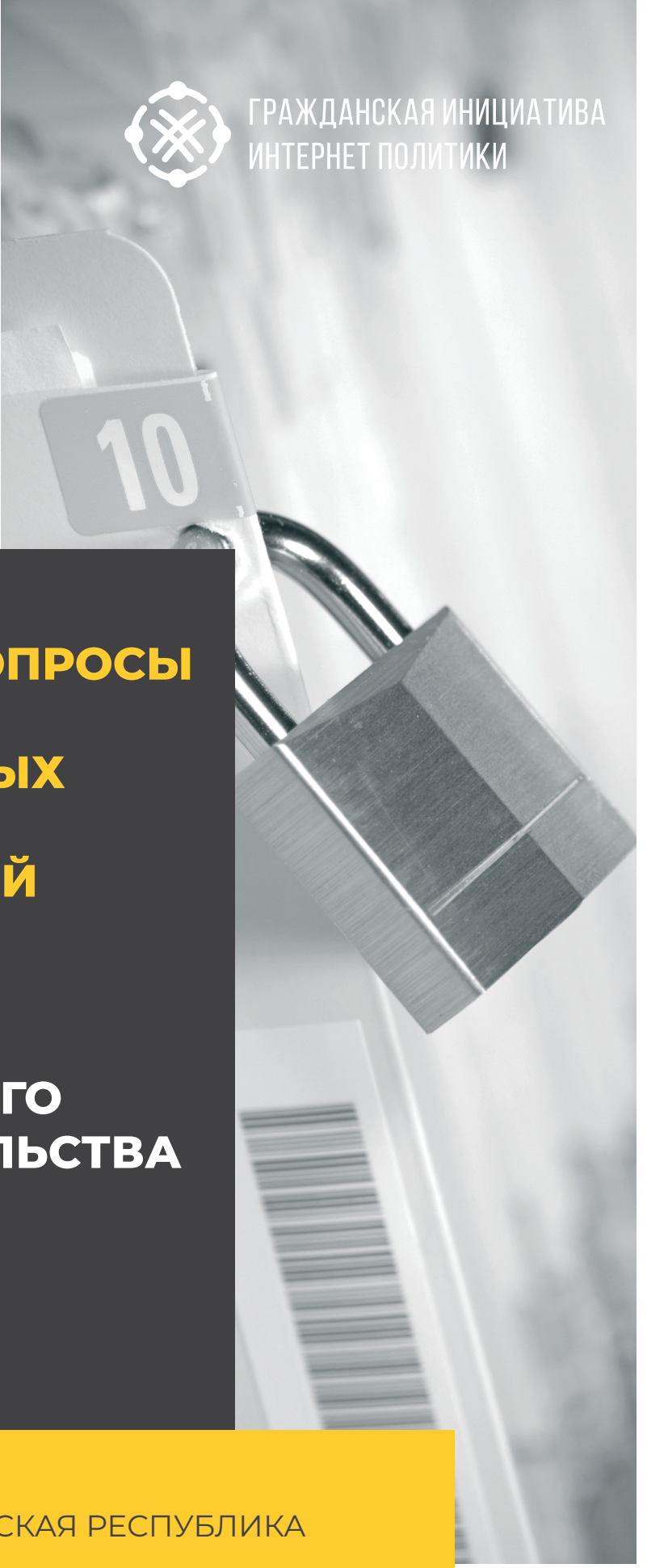
ГРАЖДАНСКАЯ ИНИЦИАТИВА
ИНТЕРНЕТ ПОЛИТИКИ




# ПРАВОВЫЕ ВОПРОСЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ:

## АНАЛИЗ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА

2023 / БИШКЕК / КЫРГЫЗСКАЯ РЕСПУБЛИКА

# ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

Право на неприкосновенность частной жизни или право на приватность определяет как самостоятельную ценность личное пространство каждого человека (личную и семейную жизнь, честь, репутацию, имя, облик, корреспонденцию, жилище, и др.), и его защиту от любого необоснованного вторжения или огласки. Это право настолько значимо для всего мира, что оно закреплено во Всеобщей декларации прав человека, статья 12 которой гласит: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

Идеи приватности – неприкосновенности частной жизни, стали правом, нарушать которое нельзя никому, ни частным лицам, ни государству. Содержащиеся во Всеобщей декларации прав человека формулировки (они сформулированы в негативном ключе – «никто не может», а не в позитивном – «у каждого есть право на приватность») о правовой охране частной жизни и запрете любого произвольного вмешательства в нее, определили суть и место данного института в системе прав человека, провозгласив тезисы о невмешательстве в частную жизнь и о жилище как неприкосновенном пространстве личности. Вслед за Всеобщей декларацией прав человека неприкосновенность частной жизни получила свое закрепление в других основополагающих документах: в статье 17 Международного пакта о гражданских и политических правах, в статье 8 Европейской конвенции по правам человека, в конституциях практически всех стран мира, как и в Конституции Кыргызской Республики (право каждого человека на неприкосновенность частной жизни, на защиту чести и достоинства[1] установлено статьей 29). Приверженность к защите частной жизни от произвольного вмешательства сохранена и в более поздних международных документах: Хартия Европейского союза по правам человека, принятая в 2000 году, в статье 7 дословно воспроизводит формулу статьи 8 Европейской конвенции по правам человека.

С правом на приватность тесно связан институт защиты персональных данных. По сути, защита персональных данных осуществляется в соответствии с правом на неприкосновенность частной жизни. Эта защита

[1] Статья 29 Конституции Кыргызской Республики от 11 апреля 2021 года (выдержки): «1. Каждый имеет право на неприкосновенность частной жизни, защиту чести и достоинства. Человеческое достоинство в Кыргызской Республике абсолютно и неприкосновенно.... 4. Не допускается сбор, хранение, использование и распространение конфиденциальной информации, информации о частной жизни человека без его согласия, кроме случаев, установленных законом. 5. Каждому гарантируется защита, в том числе судебная, от неправомерного сбора, хранения, распространения конфиденциальной информации и информации о частной жизни человека, а также гарантируется право на возмещение материального и морального вреда, причиненного неправомерными действиями».

распространяется на сбор и обработку персональных данных, потому что «право на неприкосновенность частной жизни затрагивается не только в ходе анализа или использования информации о физическом лице человеком или алгоритмом..., но и... самим фактом подготовки и сбора данных, касающихся личности, семьи и жизни конкретного человека...»[2] . Даже простое генерирование и сбор данных, касающихся личности, семьи или жизни человека, уже затрагивает право на неприкосновенность частной жизни, поскольку в результате этих действий человек теряет некоторый контроль над информацией, которая может поставить под угрозу его или ее частную жизнь. Кроме того, само существование наблюдения/анализа персональных из разных источников равносильно вмешательству в право на неприкосновенность частной жизни.

Если институт неприкосновенность частной жизни защищает интересы личности от противоправного вмешательства со стороны государства или бизнеса, то законодательное регулирование защиты персональных данных исходит из возможности оборота персональных данных с выстраиванием обеспечения принципов и условий их обработки. Данные – это необходимый актив цифровой экономики, обмен данными является неотъемлемой основой информационного общества, цифрового рынка.

В условиях цифровой трансформации, появления цифровых услуг масштаб сбора и обмена персональными данными существенно увеличивается. Технологии позволяют частным компаниям и органам государственной власти в рамках осуществления своей деятельности использовать персональные данные в беспрецедентном масштабе. Это требует наличия надежной правовой базы в области защиты данных, опирающейся на строгое исполнение, так как это имеет существенное значение для создания атмосферы доверия, которая позволит развиваться цифровой экономике. Необходимо повысить уровень правовой определенности и практической достоверности в отношении легального обмена своими данными для физических лиц, субъектов экономической деятельности и органов государственной власти.

Поэтому совершенствование законодательства в сфере защиты персональных данных, создание надлежащих надзорных органов, обладающих сильными полномочиями для пресечения нарушений, является важной задачей для КР.

Представленный анализ основан на исследовании действующего законодательства КР, а также европейского права, нормативных документах правовой системы ЕС. Формально-логический, технико-юридический, сравнительно-правовой методы, специальные юридические методы являются методологической основой при подготовке настоящего обзора.

[2] United Nations High Commissioner for Human Rights “The Right to Privacy in the Digital Age”, A/HRC/39/29, пункт 7

# ДЕЙСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО

Законодательство КР в сфере защиты персональных данных вытекает из статьи 29 Конституции КР от 11 апреля 2021 года, где закреплено право каждого человека на неприкосновенность частной жизни, на защиту чести и достоинства.

Текущее регулирование сферы защиты персональных данных представлено следующим законодательством:

- Закон КР «Об информации персонального характера» от 14 апреля 2008 года № 58;

- Порядок получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядок и форма уведомления субъектов персональных данных о передаче их персональных данных третьей стороне (постановление Правительства КР от 21 ноября 2017 года № 759);

- Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных (постановление Правительства КР от 21 ноября 2017 года № 760);

- Положение о Государственном агентстве по защите персональных данных при Кабинете Министров КР (постановление Кабинета Министров КР от 22 декабря 2021 года № 325);

- Закон КР «О биометрической регистрации граждан Кыргызской Республики» от 14 июля 2014 года.

**Закон КР «Об информации персонального характера»**

**от 14 апреля 2008 года № 58**

Специальный Закон КР «Об информации персонального характера» был принят 2008 году (далее – Закон). В целях обеспечения защиты прав и свобод человека и гражданина, Закон направлен на правовое регулирование работы с персональными данными на основе общепринятых международных принципов, связанных со сбором, обработкой и использованием персональных данных.

**Понятие персональных данных, закрепленное в Законе:**

**Информация персонального характера (персональные данные) -** зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности.

К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном положении, финансовом положении, состоянии здоровья и прочее.

Как видно из приведенного определения, перечень информации, относящейся к персональным данным, не носит исчерпывающего характера, к персональным данным относится любая информация о конкретном человеке, с помощью которой его можно идентифицировать, и которая относится к такому человеку прямо или косвенно **(см. рисунок 1).**

**Рисунок 1. Персональные данные**

**Закон КР «Об информации персонального характера»** в целом отвечает основным международным стандартам защиты персональных данных, в том числе (Страсбургской) Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (ETS N 108) от 28 января 1981 г. Установленные им правила и процедуры сбора и обработки персональных данных, при условии их соблюдения и соответствующей имплементации, позволяют держателям и обработчикам персональных данных соблюдать права субъектов, а последним – держать под своим контролем любые операции со своими данными.

В 2017 году в Закон были внесены изменения (в связи с принятием законов «Об электронном управлении» и «Об электронной подписи»), согласно которым:

- установлена компетенция Правительства КР по изданию нормативных правовых актов, регулирующих сферу персональных данных, включая вопросы безопасности;
- детализированы вопросы, касающиеся формы согласия субъекта на обработку его персональных данных, установлена возможность получения согласия в форме электронного документа;
- введена отдельная статья, касающаяся статуса и функций уполномоченного органа по защите персональных данных.

Указанные изменения позволили принять в ноябре 2017 года ряд нормативных правовых актов на уровне Правительства КР, уточняющих вопросы защиты персональных данных при их обработке в информационных системах.

**Порядок получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядок и форма уведомления субъектов персональных данных о передаче их персональных данных третьей стороне**
Указанный документ утвержден постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 759. Он устанавливает форму и процедуру получения согласия субъекта персональных данных (далее субъект), в том числе в форме электронного документа, на сбор и обработку его персональных данных в соответствии с Законом Кыргызской Республики "Об информации персонального характера", а также обязательные процедуры уведомления субъекта о факте передачи его персональных данных третьей стороне. Приложением к документу утверждена Типовая форма согласия субъекта на сбор и обработку его персональных данных.

Держатель (обладатель) массива персональных данных (далее держатель) обязан в недельный срок с момента передачи персональных данных информировать субъекта об осуществленной передаче его персональных данных третьей стороне. Форму уведомления (по телефону, смс-сообщением, письмом, сообщением электронной почты) держатель выбирает по согласованию с субъектом, исходя из способа связи с ним. Если держатель на основании имеющихся у него данных не может уведомить субъект о передаче его персональных данных, он обязан сообщить об этом в уполномоченный государственный орган по персональным данным (далее уполномоченный орган), предоставив данные, позволяющие идентифицировать субъект в случае обращения его в уполномоченный орган, а также сведения о предпринятых попытках информировать такого субъекта о

передаче его персональных данных. В целях информирования субъекта об осуществлении передачи его персональных данных третьей стороне уполномоченным органом организуется добровольная регистрация субъекта и хранится контактная информация, предоставленная субъектом.

**Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.**

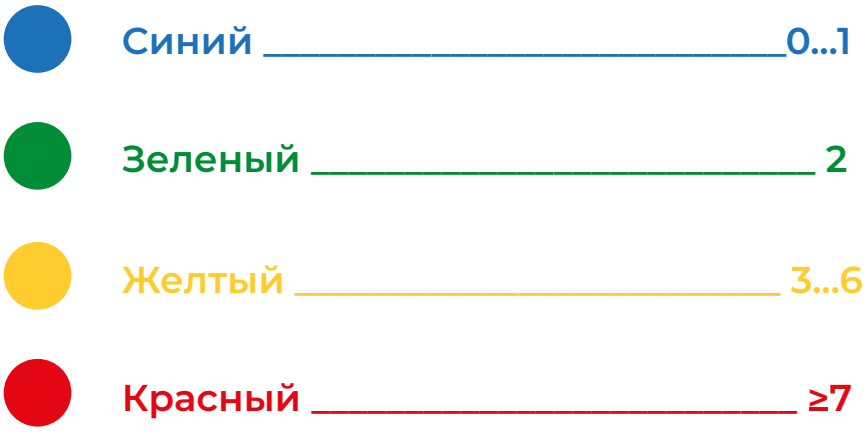
Также в 2017 году Правительством Кыргызской Республики[3] утверждены «Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных».

[3] Постановление Правительства Кыргызской Республики от 21 ноября 2017 года № 760

В документе, обязательном для исполнения всеми держателями и обработчиками персональных данных, как государственными, так и частными, предусмотрены 4 уровня защищенности персональных данных при их обработке в информационных системах (от меньшего к большему, **см. рисунок 2):**

1) синий;
2) зеленый;
3) желтый;
4) красный

**Рисунок 2. Уровни защищенности персональных данных**



Выбор уровня защищенности персональных данных, обеспечение которого необходимо при их обработке в конкретной информационной системе персональных данных, осуществляется самим держателем на основе рейтинга угроз в зависимости от определенных критериев – от размера вреда, который может быть причинен в результате реализации угрозы, до содержания персональных данных и продолжительности их обработки (всего установлено 5 таких критериев). Рейтинг угрозы безопасности персональных данных определяется как произведение баллов по каждому из утвержденных Правительством критериев

Установленные уровни защищенности персональных данных (от синего до красного) обеспечиваются выполнением определенных для каждого уровня требований (например, применение шифровальных (криптографических) средств защиты информации; установлением системы контроля помещений, в которых установлена информационная система; обеспечение резервирования; ведением журнала «логов»; назначением лица, ответственного за обеспечение безопасности – так называемого «офицера по защите данных»; проведением ежегодного аудита информационной системы, и т.п. – в зависимости от уровня защиты).

Кроме того, разработаны[4] Методические рекомендации по организации безопасности персональных данных в соответствии с требованиями Закона КР «Об информации персонального характера», которые должны помочь всем держателям определить уровень защиты и принять соответствующие меры. Документ рекомендован к применению со стороны регулятора на тот момент - Государственного комитета информационных технологий и связи (ныне – МЦР).

[4] Разработаны Общественным фондом «ГИИП»

**Положение о Государственном агентстве по защите персональных данных при Кабинете Министров КР**

Согласно Закону «Об информации персонального характера» уже с 2008 года предусматривалось что Правительством определяется уполномоченный государственный орган по защите персональных данных. Однако это случилось только в конце 2021 года, когда на основании решения Кабмина появилось Агентство в качестве государственного органа при Кабинете министров КР, специально уполномоченного осуществлять функции и полномочия по обеспечению соответствия обработки персональных данных требованиям Закона, защите прав субъектов персональных данных.

**Рисунок 3. Требования к защите в зависимости от уровня**

| № | Требования | | | |
|---|---|---|---|---|
| | 0...1 | 2 | 3...6 | ≥ 7 |
| 1 | Разработка политики по управлению ИПХ | Разработка политики по управлению ИПХ | Разработка политики по управлению ИПХ | Разработка политики по управлению ИПХ |
| 2 | Доведение до сотрудников и контрагентов содержания политики | Доведение до сотрудников и контрагентов содержания политики | Доведение до сотрудников и контрагентов содержания политики | Доведение до сотрудников и контрагентов содержания политики |
| 3 | Назначение ответственных лиц за безопасность ИПХ | Назначение ответственных лиц за безопасность ИПХ | Назначение ответственных лиц за безопасность ИПХ | Назначение ответственных лиц за безопасность ИПХ |
| 4 | Включение в трудовые договора, должностные инструкций обязанностей в отношении ИПХ | Включение в трудовые договора, должностные инструкций обязанностей в отношении ИПХ | Включение в трудовые договора, должностные инструкций обязанностей в отношении ИПХ | Включение в трудовые договора, должностные инструкций обязанностей в отношении ИПХ |
| 5 | Осуществление контроля соответствия Управления ИПХ | Осуществление контроля соответствия Управления ИПХ | Осуществление контроля соответствия Управления ИПХ | Осуществление контроля соответствия Управления ИПХ |
| 6 | Ведение журнала учёта носителей ИПХ и списка лиц с доступом к ИПХ | Ведение журнала учёта носителей ИПХ и списка лиц с доступом к ИПХ | Ведение журнала учёта носителей ИПХ и списка лиц с доступом к ИПХ | Ведение журнала учёта носителей ИПХ и списка лиц с доступом к ИПХ |
| 7 | Логгирование действий при работе с ИПХ: лицо, операция, дата, время. | Логгирование действий при работе с ИПХ: лицо, операция, дата, время. | Логгирование действий при работе с ИПХ: лицо, операция, дата, время. | Логгирование действий при работе с ИПХ: лицо, операция, дата, время. |
| 8 | Ежедневное резервирование | Ежедневное резервирование | Ежедневное резервирование | Ежедневное резервирование |
| 9 | | Проектирование ИС с учётом требований ИПХ | Проектирование ИС с учётом требований ИПХ | Проектирование ИС с учётом требований ИПХ |
| 10 | | Аудит и оценка эффективности ИС до ввода в эксплуатацию или перед глобальным обновлением | Аудит и оценка эффективности ИС до ввода в эксплуатацию или перед глобальным обновлением | Аудит и оценка эффективности ИС до ввода в эксплуатацию или перед глобальным обновлением |
| 11 | | Применение средств криптографической защиты информации | Применение средств криптографической защиты информации | Применение средств криптографической защиты информации |
| 12 | | | Централизованное управление системой защиты ИПХ, вплоть до выделенного Департамента | Централизованное управление системой защиты ИПХ, вплоть до выделенного Департамента |
| 13 | | | Контроль и защита физического доступа в помещения обработки ИПХ | Контроль и защита физического доступа в помещения обработки ИПХ |
| 14 | | | Нефальсифицируемое логгирование всех событий с ИПХ | Нефальсифицируемое логгирование всех событий с ИПХ |
| 15 | | | Обеспечение высокой доступности ИС ИПХ в режиме реального времени | Обеспечение высокой доступности ИС ИПХ в режиме реального времени |
| 16 | | | Наличие системы обнаружения и предотвращения НСД | Наличие системы обнаружения и предотвращения НСД |
| 17 | | | | Использование только защищённых каналов связи |
| 18 | | | | Защита ИПХ от утечек по техническим каналам |
| 19 | | | | Применение сертифицированных С(К)ЗИ |
| 20 | | | | Ежегодный аудит ИС ИПХ |

Постановлением Кабинета министров КР 22 декабря 2021 года № 325 было утверждено **Положение о Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики** (ГАЗПД)[5] в качестве государственного органа исполнительной власти, разрабатывающего и реализующего единую государственную политику в сфере информации персонального характера, осуществляющего функции по обеспечению защиты прав субъектов персональных данных (субъектов), регистрации держателей (обладателей) массивов персональных данных, ведению Реестра держателей массивов персональных данных.

В соответствии с положением, целью деятельности Агентства является обеспечение защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных, независимо от применяемых средств обработки этой информации, включая использование информационных технологий.

**Рисунок 4. Задачи ГАЗПД**


[5] С изменениями, внесенными постановлением Кабинета Министров КР от 4 марта 2022 года № 103

**Таблица 1. Функции и права ГАЗПД**[6]

| Функции Агентства | Права Агентства |
|---|---|
| **1) в сфере отраслевой политики:**<br><br>- содействие развитию и реализации государственной политики в области персональных данных в пределах своей компетенции;<br>- разработка единой государственной политики в области защиты персональных данных;<br>- осуществление функции государственного заказчика научно-технических и инвестиционных программ и проектов в области защиты персональных данных;<br>- обеспечение выполнения обязательств, принятых в рамках международных договоров в сфере персональных данных, вступивших в силу в соответствии с законодательством Кыргызской Республики;<br>- обеспечение согласованности деятельности государственных органов по вопросам реализации и защиты прав субъектов персональных данных, в том числе безопасности, при обработке персональных данных;<br>- разработка проектов нормативных правовых актов и решений Кабинета Министров Кыргызской Республики в области правового регулирования работы с персональными данными, защиты прав субъектов персональных данных, обеспечения безопасной обработки персональных данных, | **1)** в пределах своей компетенции принимать в установленном порядке ведомственные акты, обязательные для исполнения работниками Агентства;<br><br>**2)** реализовывать национальные стратегии и программы в информационной сфере в целях создания условий для эффективной реализации и защиты прав субъектов персональных данных, обеспечения безопасной обработки персональных данных;<br><br>**3)** осуществлять анализ и обобщение практики применения национального законодательства в сфере информации персонального характера;<br><br>**3-1)** подготовка заключения с замечаниями и рекомендациями по результатам проводимых проверок;<br><br>**4)** осуществлять сотрудничество с органами, уполномоченными в сфере защиты персональных данных, иностранных государств, а также международными организациями по вопросам, связанным с защитой персональных данных;<br><br>**5)** организовывать и проводить конференции, семинары и другие мероприятия, направленные на реализацию и защиту прав субъектов персональных данных, обеспечение безопасной обработки |

[6] Из Положения о Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики

отраслевых стандартов, технических условий, инструкций в сфере персональных данных, а также технических актов по регулированию деятельности в области персональных данных;

**2) в сфере регулирования, координации, надзора и контроля:**

- осуществление контроля путем проведения проверок за соблюдением требований законодательства Кыргызской Республики по защите персональных данных и прав субъектов персональных данных;
- ведение учета и регистрации массивов персональных данных и их держателей (обладателей);
- формирование и ведение Реестра держателей (обладателей) массивов персональных данных;
- согласование перечней персональных данных держателей (обладателей) массивов персональных данных;
- осуществление контроля за использованием персональных данных, полученных государственными органами, местными государственными администрациями и органами местного самоуправления от других государственных держателей (обладателей) персональных данных;
- координация использования государственными органами, местными государственными администрациями и органами местного самоуправления в своей деятельности персональных данных, находящихся у других держателей (обладателей) персональных данных;
- дача рекомендаций по спорным персональных данных, обмен опытом по указанным вопросам;

**6)** организовывать проведение научных и иных исследований по вопросам эффективной реализации и защиты прав субъектов персональных данных, обеспечения безопасной обработки персональных данных;

**7)** заключать договоры с юридическими и/или физическими лицами в соответствии с гражданским законодательством Кыргызской Республики;

**8)** создавать в установленном порядке и принимать участие в работе советов, комиссий, технических комитетов и рабочих групп для решения вопросов, отнесенных к компетенции Агентства, с привлечением необходимых специалистов и экспертов, работников государственных органов и органов местного самоуправления (по согласованию);

**9)** запрашивать от держателей (обладателей) массивов персональных данных необходимую информацию в соответствии с Законом Кыргызской Республики "Об информации персонального характера" для исполнения своих полномочий;

**9-1)** требовать от держателей (обладателей) персональных данных уточнения, блокировки или уничтожения недостоверных или полученных незаконным путем персональных данных, принятия надлежащих мер к обеспечению защиты и безопасности персональных данных;

вопросам, возникающим между участниками информационного взаимодействия при обработке, хранении и передаче персональных данных, в том числе с использованием элементов электронного управления;
- осуществление контроля за обеспечением исполнения требований законодательства Кыргызской Республики по содержанию и обработке персональных данных в информационных системах персональных данных, а также защите персональных данных;
- осуществление мониторинга практики обеспечения безопасности персональных данных при их обработке, обобщение и публикация лучших практик и стандартов обеспечения безопасности персональных данных при их обработке;
- оказание содействия субъектам персональных данных в реализации и защите их прав;
- рассмотрение обращений субъектов персональных данных о нарушениях законодательства в сфере персональных данных и вынесение заключений;
- направление в правоохранительные органы материалов, связанных с нарушением прав субъектов персональных данных, предусмотренных законодательством Кыргызской Республики в сфере персональных данных, для принятия соответствующих мер по исполнению законодательства Кыргызской Республики;
- осуществление методической помощи по организации защиты персональных данных.

**10)** представлять интересы Агентства в судебных органах, государственных органах Кыргызской Республики и иных организациях;

**11)** осуществлять иные права, вытекающие из законодательства Кыргызской Республики в сфере информации персонального характера.

**Рисунок 5. Состав полномочий ГАЗПД**

# АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА

Несмотря на наличие достаточно большой разноуровневой (от закона до актов на уровне Кабинета министров и рекомендаций от регулятора для держателей) нормативной правовой базы, существующее законодательство уже достаточно устарело и не отвечает современным реалиям технологического развития страны, и имеет ряд пробелов и недостатков.

Закон «Об информации персонального характера» разрабатывался и принимался почти 15 лет назад – еще в «до-технологическую» эпоху, он объективно не учитывает уровень цифрового развития – например, появление алгоритмов искусственного интеллекта, возможность автоматического (не человеком) принятия решений в отношении субъекта, появление новых способов идентификации субъектов в цифровом пространстве с использованием их данных, в том числе биометрических, а также вызовы для обработки персональных данных, в том числе трансграничные, появившиеся в связи с пандемией COVID-19.

С момента принятия Закона в 2008 году, в Кыргызской Республике, как и во всем мире, произошли глобальные технологические и правовые изменения. Изменился не только подход к сбору личной информации, но и отношение общества и самих субъектов персональных данных к этой проблематике. Поэтому назрела необходимость зафиксировать в законодательстве современный уровень развития цифровых технологий и дать ответ на актуальные вызовы и угрозы, обусловленные постоянно расширяющимися возможностями их использования, идущих в том числе во вред субъектов персональных данных. Также необходимо закрепить новые права субъектов данных, новые основания для их обработки, и другие актуальные вопросы. Важно убедиться, что базовое законодательство отвечает современным потребностям правового регулирования в данной области и эффективно достигает своей заявленной цели - обеспечение защиты прав граждан, связанных со сбором, обработкой и использованием их персональных данных в различных целях.

В качестве ориентира лучшей международной практики предлагается рассматривать Общий Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных) (General Data Protection Regulation) (GDPR). Подходы к правовому регулированию сферы защиты персональных данных, которые демонстрирует Евросоюз, имеют в настоящее время большое практическое значение для многих государств. Развитие регулирования этой сферы в Евросоюзе свидетельствует о последовательном, системном и комплексном формировании правовых норм, развитии и совершенствовании соответствующих институциональных основ в

интересах субъектов данных, что отвечает стремлениям и интересам Кыргызской Республики в этой сфере – а именно правового регулирования работы с персональными данными на основе общепринятых международных принципов и норм[7].

Руководствуясь такого рода лучшей мировой практикой, при дальнейшей работе над совершенствованием законодательства в этой сфере предлагаем необходимым **устранить нижеследующие пробелы и недостатки.**

[7] Из преамбулы Закона Кыргызской Республики «Об информации персонального характера»

### Термины и определения

Законожательство необходимо дополнить новыми терминами и определениями, как «биометрические персональные данные», «псевдонимизация», «профилирование», что позволит не только ввести в правовое регулирование новую терминологию, но и что более важно - выстроить эффективные меры по защите персональных данных (с помощью псевдонимизации или запрета профилирования), в том числе особо чувствительных. К последним необходимо отнести собственно биометрические персональные данные, не выводя их регулирование за пределы законодательства в сфере защиты персональных данных, включая поднадзорность их обработки отраслевому регулятору - ГАЗПД.

Важно также установить, что использование биометрических персональных данных допускается только в целях аутентификации лица (когда сверяется соответствие один к одному – представляемых конкретным лицом биометрических данных с данными этого же лица, имеющимися в эталонной базе биометрии), а не в целях идентификации (когда сверяется один ко всему множеству – представляемых конкретным лицом биометрических данных со всеми биометрическими данными, имеющимися в базе биометрии). Указанный принцип прямо закреплен в Общем Регламенте о защите персональных данных, который прямо запрещает обработку генетических данных, биометрических данных в целях однозначной идентификации физического лица[8].

Предлагаются следующие определения перечисленным терминам[9]:

- **«Биометрические данные»** — это персональные данные, полученные в результате специальной технической обработки, которые касаются физических, физиологических или поведенческих черт физического лица, а также позволяют произвести или подтверждают однозначную идентификацию этого физического лица, например, изображение лица или дактилоскопические данные;

- **«Профилирование»** — это любая форма автоматической обработки персональных данных, заключающаяся в использовании персональных данных для оценки определенных личных аспектов физического лица, в частности, для анализа или предугадывания аспектов его результативности в работе, его экономического положения, здоровья, личных предпочтений, интересов, надежности, поведения и перемещений;

[8] Из статьи 9 Общего регламента защиты персональных данных (GDPR) Европейского союза

[9] Из Общего регламента защиты персональных данных (GDPR) Европейского союза

• **«Псевдонимизация»** — это обработка персональных данных таким образом, что их больше невозможно отнести к конкретному субъекту данных без использования дополнительной информации, при условии, что такая дополнительная информация хранится отдельно, и в отношении нее приняты технические и организационные меры, предотвращающие ее отнесение идентифицированному или идентифицируемому физическому лицу.

Исключение правового регулирования биометрических персональных данных отдельным законодательством и отнесение таких данных к специальным категориям персональных данных (в статье 8), фактически вытекает не только из логики законодательства, но и из Решения Конституционной палаты от 14 сентября 2015 года N 11-р, в котором указано, что «Биометрические данные являются особо чувствительной категорией персональных данных, незаконное использование которых создает угрозу и может нанести существенный вред правам и законным интересам субъектов этих данных.».

**Соответствие международным стандартам прав субъектов персональных данных**

Закон не учитывает в полном объеме права субъектов персональных данных, содержащихся в международных стандартах, что влияет на возможности их защиты, в том числе таких как:

- Право на удаление данных ("право быть забытым");[10]
- Обязанность уведомления относительно изменения или уничтожения персональных данных или ограничения обработки;
- Право на переносимость данных;
- Право на возражение (против профилирования, прямого маркетинга);
- Право не подвергаться решению, которое может включать в себя конкретные меры, оценивающему характеристики личности, основанному исключительно на автоматизированной обработке и влекущему правовые последствия;[11]
- Право на получение информации о нарушении безопасности персональных данных (обязанность уведомления субъекта данных о нарушении безопасности персональных данных).

Дополнение законодательства соответствующими правами субъектов данных и корреспондирующими им обязанностями держателей персональных данных позволит улучшить их защиту, повысить информированность субъектов и обеспечить контроль над своими данными, обеспечить соответствие законодательства международным стандартам.

[10] Всякое применение «право на забвение» должно быть строго ограничено, поскольку необходимо обеспечить соблюдение определенных минимальных требований, чтобы такое право не противоречило праву на свободу выражения мнений, как в смысле содержания, так и в процессуальном смысле. В частности, субъектами «права на забвение» должны быть частные лица, «право на забвение» должно применяться только к поисковым системам (в качестве операторов персональных данных), а не к хостинговым сервисам и контент-провайдерам. Всякие меры правовой защиты должны прямо ссылаться на свободу выражения мнений как основополагающее право, с которым такие меры защиты должны быть уравновешены)

[11] Как, например, автоматический отказ в онлайн-форме заявки на кредит или онлайн-рекрутинга без какого-либо человеческого посредничества; подобная обработка должна подлежать соответствующим мерам защиты, которые должны включать в себя специфическую информацию о субъекте данных и право требовать людского вмешательства, для выражения своей точки зрения, требования объяснения решения, принятого в результате такой оценки, и для изменения решения. Данная мера не должна относиться к ребенку.

**«Проектируемая защита» и «защита по умолчанию»**

Закон не устанавливает в качестве обязательных технических и организационных мер к защите персональных данных как «проектируемая защита» и «защита по умолчанию» **(data protection by design and by default).**[12]

Введение принципов защиты данных уже на стадии проектирования информационных систем, или обсуждения технических заданий на их разработку позволит отраслевому регулятору (ГАЗПД) обеспечить контроль за соответствием законодательства уже на стадии закупки и/или разработки технологических систем, что в конечном счете будет способствовать реализации необходимых мер по защите персональных данных. Такие меры являются необходимыми, принимая во внимание текущий уровень цифровизации, затраты на внедрение технологических (информационных) систем для обработки данных, характер, масштаб, контекст и цель обработки, а также риски, связанные с той или иной вероятностью и серьезностью нарушения прав и свобод физических лиц, вызванные обработкой.

В результате держатели персональных данных, как во время определения средств обработки, так и во время самой обработки, будут обязан внедрять надлежащие технические и организационные меры, например, **псевдонимизацию,** предназначенные для эффективного внедрения принципов защиты персональных данных, таких как **минимизация данных,** а также **для интеграции необходимых гарантий в обработку** с целью соблюдения требований законодательства в данной сфере.

**Использование цифровых способов для юридически значимого согласия**

Одним из недостатков действующего Закона является требование к форме согласия на обработку персональных данных – в письменной (офлайн) или в электронной (онлайн) форме, подписанное электронной подписью.

Действующий закон не признает выражение лицом своей воли с помощью электронных или иных технических средств (например, при заполнении формы согласия на сайте или в приложении, установленном в смартфоне, при нажатии клавиши ОК и проставлении специальной отметки («галочки») в чек-боксе) для полноценного юридически значимого волеизъявления на обработку своих персональных данных. Это серьезно затрудняет реализацию права на управление своими данными. Кроме того, остро стоит вопрос создания общегосударственной онлайн-платформы управления полученными или выраженными согласиями граждан на обработку данных.

Предоставлением согласия на обработку персональных данных может являться проставление соответствующего «флажка» или нажатие кнопки «Отправить» при регистрации (подаче электронного заявления) на сайте держателя/обработчика, или в соответствующим приложении, установленном на устройстве субъекта персональных данных.
Идентификация должна включать в себя цифровую идентификацию субъекта данных, например, посредством механизма аутентификации на основе учетных данных, которые используются субъектом данных для входа под своим логином в

[12] Обязательство внедрять надлежащие технические и организационные меры, например, псевдонимизацию, предназначенные для эффективного внедрения принципов защиты персональных данных, таких как минимизация данных, а также для интеграции необходимых гарантий в обработку с целью соблюдения требований.

онлайновую службу, предоставляемую держателем/обработчиком данных. Держатель (обработчик) может использовать все приемлемые способы для того, чтобы проверить и подтвердить личность субъекта данных, который запрашивает доступ, в частности, в контексте онлайновых служб и онлайновых идентификаторов.

В связи с чем предлагается дополнить законодательство такими формулировками:

• Согласие на обработку персональных данных должно быть добровольным, конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в **любой позволяющей подтвердить факт его получения форме,** если иное не установлено законодательством.

• **Согласие субъекта на обработку его данных допускается при отсутствии иных оснований для обработки (договор, закон, защита жизни и т.п.), и запрос согласия на обработку персональных данных не допускается при наличии других оснований** обработки персональных данных в целях, на которые запрашивается согласие.

**Форма (язык изложения) согласия**

Одним из недостатков закона является отсутствие в нем требований к изложению самого согласия в понятной и легко доступной форме, чтобы использовался понятный и простой язык, в нем не содержалось несправедливых условий, например, чтобы выполнение договора (в том числе исполнение услуги) не обуславливалось дачей согласия на обработку персональных данных, которые не нужны для выполнения договора. Согласие на сбор данных не должно быть условием для выполнения или продолжения исполнения договора.

Цель состоит не в том, чтобы получить согласие любой ценой, а в том, чтобы четко проинформировать лицо о предмете данного им согласия, его сфере и значении.

Также необходимо определить в законодательстве, что использование предварительно отмеченных полей (предустановленных «галочек» в чек-боксе формы согласия) является недействительным, ровно так же, как и молчание или бездействие со стороны субъекта данных, а также простое обращение к услуге (совершение так называемых «конклюдентных» действий при выражении согласия) - не могут рассматриваться как дача согласия на обработку.

**Возможность отзыва согласия**

Закон не предусматривает возможность **отзыва согласия в любое время и в том же порядке/форме, что и выражение согласия.**

Согласно общепринятой международной практике, субъект данных имеет право в любое время отозвать свое согласие. Отзыв согласия не влияет на законность обработки, которая была основана на согласии до его отзыва. Субъект данных должен быть проинформирован об этом перед тем, как он выразил согласие. Отзыв согласия должен быть столь же прост и доступен, как и его выражение, как правило - через один и тот же интерфейс, будь то приложение, веб-сайт или электронная почта (например, продавец не может получить согласие через онлайн-форму и

попросить пользователей позвонить по номеру телефона в рабочее время, чтобы отозвать его).

Кроме того, не должно быть никакой платы, связанной с требованием отозвать согласие, и лицо должно быть в состоянии отказать или отозвать согласие без каких-либо негативных последствий. Отзыв согласия лица не влияет на правомерность процессов, основанных на ее / его согласии. Они остаются действительными в том случае, если они выполнялись с соблюдением условий, предусмотренных законодательством.

Еще одним обязательством, вытекающим из положения о праве на отзыв согласия на обработку, является обязательство держателя удалить все данные, связанные с этим конкретным согласием.

**Рисунок 6. Форма согласия субъекта**

**Согласие субъекта персональных данных на сбор и обработку его персональных данных**

г. Бишкек 25 декабря 2019 г.

Я, Козубеков Эрнек Бактыбекович
(фамилия, имя, отчество)

проживающий по адресу: г. Бишкек, ул. Ю. Абдрахманова, д. 1 «а», кв. 13

Документ, удостоверяющий личность: ID-паспорт (вид документа) серия AN № 1234567

выдан 15/10/2012 (дата выдачи) МКК 50-55 (кем выдан)

свободно, осознанно, по своей воле даю согласие ЗАГС Октябрьского р-на ДРНАГС ГРС при ПКР
(наименование, адрес собственника или владельца информационной системы, ФИО обработчика)

- на обработку (любая операция или набор операций, выполняемых независимо от способов держателем (обладателем) персональных данных либо по его поручению, автоматическими средствами или без таковых, в целях сбора, записи, хранения, актуализации, группировки, блокирования, стирания и разрушения персональных данных),

а также на:

- передачу персональных данных (предоставление держателем (обладателем) персональных данных третьим лицам в соответствии с Законом Кыргызской Республики "Об информации персонального характера" и международными договорами;
- с трансграничную передачу персональных данных (передача держателем (обладателем) персональных данных держателям, находящимся под юрисдикцией других государств) следующих персональных данных:

1. Фамилия, Имя и Отчество
2. Дата и место рождения
3. Сведения о гражданстве
4. Номер контактного телефона
5. Номер паспорта
6. Персональный идентификационный номер
7. Личная фотография
8. Семейное положение и состав семьи

Вышеуказанные персональные данные предоставляю для обработки в целях предоставления мне государственной (муниципальной) услуги Регистрация рождения
(указать наименование услуги)

Я ознакомлен(а) с тем, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока предоставления мне государственной (муниципальной) услуги и хранения данных об оказанной услуге в соответствии с законодательством Кыргызской Республики;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных обработка моих персональных данных полностью или частично может быть продолжена в соответствии со статьями 5 и 15 Закона Кыргызской Республики «Об информации персонального характера».

Дата начала обработки персональных данных: 25 декабря 2019 года
(число, месяц, год)

"25" декабря 2019 г.

Э.Б.Козубеков — Подпись

Козубеков Э. Б. — ФИО

**Правовые основания для обработки персональных данных**

В законе не указаны все признаваемые международными актами юридические основания для работы с персональными данными, такие как наличие договора. Это приводит к тому, что банки, операторы связи, или компании для заключения договора на услуги, или трудового договора – вынуждены отбирать согласие на обработку ПД, что нивелирует саму суть института согласия как свободного волеизъявления, которое тем самым ставится под условие получения или неполучения определенной услуги (банковской, услуги связи и т.п.).

Не уточнены исключения на получение согласия для законной обработки данных, например, для школ. Поскольку школы не являются государственными органами, на них не распространяется исключение на получение согласия при исполнении своих функций.

Представляется, что необходимы дополнения законодательства новыми правовыми основаниями для обработки ПД:
- если их обработка **необходима для заключения или исполнения договора,** в котором субъект персональных данных является стороной, представителем или иным лицом, действующим от имени стороны по договору, или выгодоприобретателем, либо для принятия мер по требованию субъекта до заключения договора;
- обработка необходима для выполнения держателем обязанностей (полномочий), установленных законом или принятыми в соответствии с ним нормативными правовыми актами, **или осуществляется на основании закона** Кыргызской Республики, прямо предусматривающего необходимость обработки персональных данных, и определяющего цели их обработки;

**Обработка специальных категорий персональных данных**

В действующем законе не учтены все **случаи исключений, когда допускается обработка особо чувствительных (специальных категорий) данных.**

Например:

- обработка персональных данных, которые субъект данных явным образом сделал общедоступными;
- обработка осуществляется на основании закона Кыргызской Республики, прямо предусматривающего необходимость обработки таких персональных данных, и определяющего цели их обработки;
- обработка осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством сохранять врачебную тайну;
- обработка осуществляется для защиты существенных интересов в области общественного здравоохранения, в том числе, для мониторинга и защиты от опасной для жизни эпидемии и ее распространения, или в целях гуманитарной помощи;
- обработка необходима в связи с осуществлением правосудия, в том числе в рамках третейского производства;
- обработка осуществляется для защиты национальной безопасности,

обороны, общественной безопасности или предотвращения, расследования и судебного преследования уголовных преступлений и исполнения уголовных наказаний;
• обработка осуществляется в научных, статистических или иных исследовательских целях, при условии обезличивания персональных записей.

Представляется, что дополнение законодательства в сфере защиты персональных данных подобными положениями с одновременным установлением правил и процедур обезличивания данных, существенно облегчит правоприменительную практику, исключит правовую неопределенность в этих вопросах.

**Особенности обработки персональных данных детей**

Развитие технологий означает расширение возможностей для сбора и использования персональных данных, не только взрослых, но и детей. Статистика свидетельствует[13] , что почти 5 млрд. человек (62,5% населения Земли) проводят в сети 7 часов в день (более 40 % времени бодрствования), используя интернет на всех устройствах. В социальных сетях «добавляется» в среднем более 1 млн. новых пользователей каждый день, или почти 13 новых пользователей каждую секунду. По данным Всемирного банка, 90% людей в возрасте 10 лет и старше будет использовать интернет к 2030 году.
50% пользователей интернета во всем мире составляют молодые люди в возрасте от 18 до 24 лет; 90% из них являются активными пользователями социальных сетей

[13] Данные приведены из отчетов, представленных на ресурсе https://datareportal.com/ на основе сбора данных из множества цифровых источников

Фактически каждый день дети ежедневно взаимодействуют в сети со множеством сервисов – игровые платформы, социальные сети, приложения, мессенджеры. Они постоянно идентифицируются в разнообразных системах, оставляя свои данные – идентификаторы, которые неразрывно связаны с личностью. Часто дети представлены в сети сразу несколькими аккаунтами – в социальных сетях Tik Tok, Instagram, Telegram, стриминговых и видео сервисах (Netflix, YouTube, Steam).

Международные стандарты в этой сфере устанавливают, что дети заслуживают особой защиты в отношении своих личных данных, поскольку они могут быть менее осведомлены о рисках, последствиях, гарантиях и их правах в отношении обработки персональных данных. Конкретная защита должна применяться к использованию персональных данных детей в целях маркетинга или создания профилей пользователей и сбора персональных данных детей при использовании услуг, предоставляемых непосредственно ребенку.

Поэтому **законодательство также необходимо дополнить нормами об особенностях обработки персональных данных детей,** установив следующие пункты:
• основания для такой обработки;
• при отсутствии таких оснований - обработка персональных данных ребенка допускается только при условии получения согласия законного представителя ребенка на обработку персональных данных ребенка и только для тех целей обработки, в отношении которых было получено согласие;
• дети, достигшие четырнадцатилетнего возраста, вправе самостоятельно давать согласие на обработку своих персональных данных в целях, соответствующих их возрастным интересам;

• требования к форме согласия - запрос согласия на обработку персональных данных детей и любая связанная с обработкой персональных данных детей информация должны быть изложены ясным и простым языком, который ребенок сможет понять.

**Политика держателя (обладателя) массива персональных данных в отношении обработки персональных данных**

Пробелом является и отсутствие **требований об обязательном опубликовании (в том числе на сайте) документа, определяющего политику держателя** (обладателя) массива персональных данных в отношении обработки персональных данных (так называемых Privacy Policy – политик конфиденциальности/обработки ПД). Сейчас предусмотрено только доведение содержания данного документа до работников и контрагентов держателя (обладателя) массива персональных данных. Указанный пробел представляется целесообразным восполнить в законодательстве.

**Права на получение информации о несанкционированном доступе**

В общем контексте современных подходов к защите прав граждан на неприкосновенность частной жизни также применимы такие нормы как право на получение информации о несанкционированном доступе третьих лиц к их персональным данным, право заявить о своем несогласии, и независимо от места жительства получать квалифицированную правовую защиту, в том числе и от уполномоченного органа.

Отсутствие подобных норм в законодательстве негативно влияет на состояние защиты персональных данных и права субъектов в связи с обработкой их данных.

**Обязательная регистрация держателей**

Устаревшей нормой, а также коррупционным риском из-за возможности для применения карательных санкций, является наличие в ст. 30 Закона обязанности по обязательной регистрации массивов персональных данных и держателей (обладатели) этих массивов, и функций уполномоченного органа по ведению реестра держателей (обладателей) массива персональных данных. В результате существует риск применения карательных санкций в отношении любых юридических лиц за формальное несоблюдение этого требования (не постановка на учет в качестве держателя).

При этом закон не устанавливает процедур, например, максимально простой уведомительной онлайн регистрации держателей персданных только в целях их учета и понимания целей обработки персональных данных, или когда обработка может привести к возникновению высокой степени риска.

Представляется необходимым внести соответствующие изменения в законодательство с установлением, например, добровольной регистрации с максимально простой процедурой такой регистрации, что может служить своего рода «преференцией» - свидетельством добросовестности такого держателя.

**Меры ответственности за правонарушения и преступления Необходимость совершенствования процессуальных норм**

В действующем законодательстве не определены меры ответственности за правонарушения (административная ответственность) и преступления с

персональными данными (уголовная ответственность).
В связи с чем, необходимы релевантные дополнения в Кодекс о правонарушениях[14], и Уголовный кодекс[15].

Определяющими факторами при этом должны стать вопросы не столько наказаний за допущенные нарушения, сколько восстановления нарушенных прав субъектов и причиненного им вреда в результате незаконных/ противоправных действий с их данными.

На уровне процессуального законодательства не закреплены методы и средств цифровой криминалистики (компьютерной форензики), фиксации цифровых доказательств о нарушениях с персональными данными в целях расследования, их исследования в суде. Указанные пробелы также негативно влияют на возможности расследования, исследования в суде доказательств, привлечения к ответственности виновных лиц. В связи с чем, необходимы соответствующие изменения в уголовно-процессуальное и гражданско-процессуальное законодательства, разработка соответствующих актов на уровне Кабинета министров (инструкций для следователей, экспертов), а также включение в образовательные программы подготовки юристов, криминалистов соответствующих дисциплин.

**Утечки персональных данных**

Существует правовой пробел, который касается обязанности держателей персональных данных **уведомлять граждан об об утечках их персональных данных** (с рекомендациями по принятию надлежащих мер к минимизации последствий таких утечек – смене паролей, адресов электронной почты, и т.п.).

В перспективе необходимо ставить вопрос **о создании data-cert,** который будет отслеживать и реагировать на факты утечки персональных данных.

**Вопросы обработки и трансграничной передачи данных**

В качестве мер реагирования на вызовы, появившиеся во время пандемии COVID-19, необходимо решить правовые вопросы, связанные с обработкой и передачей персональных данных в условиях чрезвычайной ситуации, трансграничной передачей персональных данных, когда невозможно или затруднительно получение согласия на это субъекта, а также вопросы правомерного доступа к чувствительным (специальным категориям) медицинским данным.

Режим трансграничных потоков данных также является вызовом в рамках интеграции Кыргызстана в Евразийском экономическом союзе, в цифровой повестке которого создание общего для ЕАЭС рынка и оборота (свободного перемещения) персональных данных граждан, сближения правового регулирования, законодательных подходов к защите данных.

[14] В Кодексе о правонарушениях от 28.10.2021 г., имеется одна статья - 228-1. Нарушение требований по защите информации персонального и коммерческого характера (Нарушение требований по организации защиты электронных документов, информации персонального и коммерческого характера, а равно неправомерное использование, обеспечение доступа и передача третьим лицам такой информации - влекут наложение штрафа на физических лиц в размере 200 расчетных показателей.).

[15] Уголовным кодексом от 28.10.2021 г., предусмотрено наказание за нарушение неприкосновенности частной жизни (ст. 190 УК), нарушение тайны переписки (ст. 193), несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи (ст. 319).

**Полномочия и компетенция регулятора по защите персональных данных**

Установленные Законом и Положением о ГАЗПД функции и полномочия регулятора по защите персональных данных не в полной мере **соответствуют стандартам самостоятельности, независимости, компетенциям**, задачам и полномочиям надзорных органов в этой сфере, как это установлено международными стандартами[16]. Наличие «сильных» компетенций и независимости от регулируемых субъектов являются существенным и необходимым компонентом защиты физических лиц в отношении обработки их персональных данных.

Несоблюдение принципов независимости и самостоятельности при создании института регулятора по защите персональных данных, в отсутствие установленных в законе полномочий такого органа и утвержденных и опубликованных стандартов его работы, чревато негативными последствиями для соблюдения прав человека в процессе такой реформы, созданием очередной правительственной структуры с карательными функциями. Это особенно тревожно на фоне громких журналистских расследований о коррупции, утечек персональных данных с камер «Безопасного города», установки и использования камер с функцией распознавания лиц, что было сделано в отсутствие необходимой правовой базы и общественных обсуждений с экспертным сообществом. Также это касается таких вопросов, как применение методов цифровой слежки по данным о геолокации, обработка цифрового фото и видео изображения, передача телеметрических данных о состоянии здоровья по каналам связи,  перевод государственных услуг в цифровой формат с требованием однозначной идентификации/подтверждения личности с получением и хранением в цифровой среде персональных данных, включая биометрические.

Кроме того, функции в сфере регулирования, координации, надзора и контроля не распространяются на персональные данные, полученные в результате деятельности органов прокуратуры Кыргызской Республики, правоохранительных органов и органов, осуществляющих оперативно-розыскную, разведывательную и контрразведывательную деятельность, производство официальной статистики.[17]  Это является существенным и необоснованным ограничением в предмете надзора в сфере защиты персональных данных.

Бизнес высказывает необходимость придания должной юридической значимости разъяснениям и заключениям, которые делает регулятор по обращениям граждан и самих держателей. Безусловно, придание большей юридической силы разъяснениям правоприменительной практики по вопросам защиты персональных данных, исходящих от отраслевого регулятора (ГАЗПД) будет способствовать созданию правовой определенности и надлежащих практик при обработке и защите ПД.

[16] В качестве главного ориентира в этой сфере предлагается рассматривать Общий регламент защиты персональных данных (GDPR) Европейского союза; стандарты деятельности надзорных органов предусмотрены статьями 51-59 GDPR.

[17] П.10 Положения

## Регулирование сбора и обработки биометрических персональных данных

Пробелом в надлежащем регулировании сферы персональных данных является наличие еще одного специального Закона – «О биометрической регистрации граждан Кыргызской Республики» от 14 июля 2014 года.

Данный Закон самостоятельно, отличными от Закона об информации персонального характера способами регулирует отношения, возникающие при осуществлении сбора, обработки, хранения и использования биометрических данных граждан КР, актуализации и защите базы биометрических данных. Исходя из приведенных в Законе формулировок, биометрические данные выведены из-под регулирования закона об информации персонального характера, хотя по сути являются чувствительными персональными данными – специальной категорией персональных данных согласно ст. 8 Закона об информации персонального характера.

Процедуры в отношении биометрических данных, указанные в Законе о биометрической регистрации, не синхронизированы с процедурами, предусмотренными Законом об информации персонального характера, и не соответствуют европейским стандартам защиты сенситивных (чувствительных) данных.[18]

Для обязательной биометрической регистрации в Законе не делается никаких исключений, в том числе, для малолетних граждан, граждан, страдающих психическими расстройствами, граждан, постоянно проживающих за границей, лиц, чьи убеждения не позволяют им предоставлять биометрические данные. С обязательностью регистрации связаны основные трудности Закона: как в части противоречия его актам высшей юридической силы, так и в части реализации положений Закона.

Установление обязательной биометрической регистрации требует, во-первых, крайне конкретного определения целей, в которых используются собранные биометрические данные, во-вторых, наличия обоснованного перечня исключений из обязательной регистрации. Законом ни того, ни другого не предусмотрено: цели использования собранной биометрической информации определены расплывчато (ст.2 и ст.7), а перечня исключений никак не предусмотрено.

Указанные обстоятельства были предметом рассмотрения Конституционной палаты Верховного суда КР, которая по ходатайству экспертов рассмотрела соответствие указанного Закона нормам Конституции. Приложение 1 содержит сведения об итогах рассмотрения.

[18] Для обязательной биометрической регистрации в Законе не делается никаких исключений, в том числе, для малолетних граждан, граждан, страдающих психическими расстройствами, граждан, постоянно проживающих за границей, лиц, чьи убеждения не позволяют им предоставлять биометрические данные. С обязательностью регистрации связаны основные трудности Закона: как в части противоречия его актам высшей юридической силы, так и в части реализации положений Закона. Установление обязательной биометрической регистрации требует, во-первых, крайне конкретного определения целей, в которых используются собранные биометрические данные, во-вторых, наличия обоснованного перечня исключений из обязательной регистрации. Законом ни того, ни другого не предусмотрено: цели использования собранной биометрической информации определены крайне расплывчато (ст.2 и ст.7), а перечня исключений совсем не предусмотрено.

Предлагается исключить двойственность и правовую неопределенность в регулировании вопросов обработки и защиты персональных данных, как биометрических, геномных, иных специальных категорий, так и иных, создав общик правовые подходы к этому институту в едином нормативном правовом акте, основанном на общепризнанной международной практике. При таком подходе действующий закон о биометрической регистрации подлежит подаче на утрату.

**Риски нарушений во время глобальной пандемии**

Одним из серьезных вызовов праву на неприкосновенность частной жизни и законности обработки персональных данных стала пандемия коронавируса COVID-19. Власти многих стран прибегли к беспрецедентным мерам, которые имели потенциальные риски нарушения гражданских прав с опасностью продолжения вмешательства в частную жизнь и после конца пандемии. В практике КР также были разработаны и применены цифровые сервисы и приложения, с нарушениями законодательства в сфере персональных данных (Приложение 2).

Например, не запрашивалось согласие в электронном виде (подписанное электронной подписью), не были заявлены и указаны цели сбора и обработки персональных данных, не отмечена возможность передачи третьим лицам, не были указаны сроки обработки данных, периоды хранения, срок и способы уничтожения данных и их анонимизации.  В целом не были обговорены условия введения и прекращения ограничений гражданских прав во время чрезвычайной ситуации. Также не было уточнено, как соблюдены требования кибербезопасности в отношении персональных данных и информационных систем, в которых они обрабатываются, как они защищены от утечек, по каким открытым или зашифрованным протоколам передаются данные.

В то же время, законодательством КР не регламентировано проведение телеметрических наблюдений, отсутствует Закон о телемедицине с установлением возможности применения телемедицинских технологий и сервисов цифрового благополучия. В отсутствии законодательства, определяющего права, обязанности и полномочия государственных органов в сфере телемедицины и цифрового благополучия, действия, направленные на сбор, накопление, хранение и использование особо чувствительных персональных данных с помощью телеметрии не соответствовали требованиям закона КР «Об информации персонального характера» ни по форме, ни по содержанию в части процедур получения согласия на обработку персональных данных, обеспечения безопасности такой обработки и иных требований.

Данная практика и опыт КР выявила ряд пробелов в законодательстве, имеющем отношение к чрезвычайным мерам реагирования на последствия глобальной пандемии.

# ЗАКЛЮЧЕНИЕ

Защита физических лиц в отношении обработки персональных данных является и остается фундаментальным правом. Несмотря на в целом прогрессивный характер законодательства Кыргызской Республики в сфере обработки и защиты персональных данных, его глобальное соответствие существующим международным стандартам в сфере приватности, Закон «Об информации персонального характера» от 2008 года существенно устарел и нуждается в обновлении.

С учетом быстрого развития технологий, на основе правового анализа законодательства о условиях обработки и защиты персональных данных, необходимо вести постоянную деятельность по выявлению и устранению пробелов и недостатков в правовом регулировании данной сферы. Соответствующая работа должна быть проведена с учетом новых вызовов и угроз, связанных с автоматизированным сбором и обработкой персональных данных с помощью цифровых технологий, включая растущее применение технологий искусственного интеллекта, аналитики больших данных, наличие возможности автоматического (не человеком) принятия решений и взаимодействия с технологиями.

При этом, практическое соблюдение Закона держателями начинается не с закупки необходимых технических средств для такой защиты, а с разработки документов и постановки соответствующих организационных и организационно-технических процессов управления. Держателям необходимо понимать не только какие конкретные меры необходимы для защиты данных соответствующими техническими средствами, но также обеспечивать правовые условия для сбора и обработки персональных данных граждан. Ключевыми для практического уровня соблюдения законодательства для держателей являются ответы на вопросы:

- С какой целью организация собирает персональные данные граждан?
- Соответствует ли заявленная цель реальным потребностям организации?
- Не собирает ли организация персональных данных больше, чем это требуется для её цели?
- Существует ли политика обработки информации персонального характера, насколько она исполняется и соответствует требованиям Закона и декларируемым целям обработки?
- Определены ли сроки хранения персональных данных, насколько они объективны?
- Имеется ли согласие субъектов о сборе, обработке, хранении, на трансграничную передачу, на обработку третьими лицами?

Соблюдение законодательства по защите персональных данных — это, в первую очередь, внедрение и соблюдение определенных процессов, правил и процедур, которые должны быть ясны и понятны, как тем, кто собирает персональные данные, так и самим субъектам, которые должны иметь возможность их контролировать и защищать.

# ПРИЛОЖЕНИЕ 1

## Решение Конституционной палаты Верховного суда КР о соответствии Закона КР "О биометрической регистрации граждан Кыргызской Республики" нормам Конституции

Конституционная палата Верховного суда КР по ходатайству экспертов рассмотрела соответствие указанного Закона нормам Конституции. Решением Конституционной палаты от 14 сентября 2015 года N 11-р положения рассматриваемого Закона признаны не противоречащими Конституции. Вместе с тем, в мотивировочной части решения Конституционной палаты указано, что **«Биометрические данные являются особо чувствительной категорией персональных данных, незаконное использование которых создает угрозу и может нанести существенный вред правам и законным интересам субъектов этих данных».** А также, по сути, соответствующим Конституции признаны только 2 задачи, указанные в статье 2 Закона: составление актуализированного списка избирателей; своевременная регистрация граждан и выдача идентификационных документов.

Иные задачи, определенные в оспариваемой норме (часть 2 статьи 2 Закона), несмотря на их государственную и социальную значимость, носят недопустимо обобщенный характер, что является неприемлемым при ограничении прав и свобод человека и гражданина, гарантированных Конституцией КР. Указанные задачи, по своей сути, являются целями оспариваемого Закона, достижение которых предполагается посредством создания актуализированной базы данных граждан КР с использованием биометрических данных:

- Определение качественного и количественного состава граждан Кыргызской Республики, проживающих на территории Кыргызской Республики и за ее пределами;
- Эффективная борьба с преступностью, нелегальной миграцией, терроризмом и торговлей людьми;
- Своевременное и качественное предоставление услуг населению не раскрывают в полной мере намерений государства, не содержат детальных положений, определяющих порядок использования базы биометрических данных для достижения задач (целей) Закона, установленных частью 2 статьи 2 Закона.

В этой связи Конституционная палата указала, что законодателю следует внести соответствующие изменения в Закон КР "О биометрической регистрации граждан Кыргызской Республики", определяющие точные и ясные цели данного Закона, а также механизмы их достижения. При этом законодателю необходимо правильно использовать юридическую терминологию в законотворческом процессе, чтобы исключить двусмысленность и неоднозначное понимание норм Закона.

Также в решении указано, что при создании государственных информационных систем должны соблюдаться следующие условия: фиксирование биометрических

данных граждан без унижения достоинства личности и причинения вреда здоровью; исключение возможности незаконного воспроизведения, использования и распространения биометрических данных граждан; обеспечение конфиденциальности и безопасности информации, содержащейся в государственной информационной системе, и ограничение этой информации только теми сведениями, которые необходимы для проверки подлинности идентификационных документов нового поколения.

Согласно Решению Конституционной палаты, Жогорку Кенешу КР внести в Закон КР "О биометрической регистрации граждан Кыргызской Республики" соответствующие изменения и дополнения, вытекающие из мотивировочной части настоящего Решения.[19]

[19] Только сейчас Жогорку Кенешем Кыргызской Республики рассматриваются соответствующие изменения в данный Закон, подготовленные Кабинетом министров Кыргызской Республики для исполнения решения Конституционной палаты.

# ПРИЛОЖЕНИЕ 2

## Цифровые инструменты, разработанные в КР в рамках противодействия глобальной пандемии

| Цифровой продукт | Описание |
|---|---|
| Электронное разрешение (пропуск) транспортному средству на передвижение во время комендантского часа и дневной электронный пропуск для транспортных средств | Для подачи заявки необходимо заполнить представленную на ресурсе электронную форму с указанием своих персональных данных (ФИО, ПИН, номер телефона, адрес места жительства, номер автотранспортного средства), целей получения и периода, а также вложить необходимые документы. Если определенная деятельность требует регулярного передвижения на транспортном средстве помимо водителя еще и дополнительного пассажира, на ресурсе необходимо вписать также данные пассажира. После одобрения заявителю необходимо распечатать свое разрешение с QR-кодом и наклеить на лобовое стекло транспорта, на которое было выдано разрешение (или иметь при себе). |
| Электронный маршрутный лист (обязательный документ онлайн или офлайн формы для возможности передвижения по городу) | Представляет собой электронную форму для предоставления своих персональных данных с точным указанием своих персональных данных – ФИО, ПИН, номер телефона, адреса места жительства/регистрации, адреса направления. |
| Смарт система учета эпидемиологических данных | Разработана электронная автоматизированная система управления в помощь службе санитарно-эпидемиологического надзора. Цифровая система обрабатывает и анализирует следующие виды документов:<br>• временная анкета о подтвержденных и вероятных случаях инфицирования новым коронавирусом (2019-nCoV); |

Мобильное приложение «Stop COVID-19 KG», размещенное на маркетплэйсе Google Play[20]

[20] https://play.google.com/-store/apps/details?id=kg.cdt.stop-covid19

- анкета для сбора персональных данных о контактном лице с пациентом с коронавирусом;
- форма для пассажиров с их персональными данными, прибывающих в Кыргызскую Республику;
- данные по результатам анализа.

Приложение позволяет уполномоченным государственным органам, отдельным уполномоченным лицам контролировать местонахождение зараженного человека (либо с подозрением на заражение коронавирусной инфекцией COVID-19) и отслеживать перемещение на карте.
Для контроля и отслеживания на карте используется технология GPS. А также система позволяет сохранять историю перемещений. Приложение имеет доступ к данным о местоположении (approximate location (net-work-based), precise location (GPS and net-work-based), номеру телефона, фото/ мультимедиа/ файлам, хранилищу, камере (делать фото и видео), микрофону (для записи аудио), данным о подключении по Wi-Fi, имеет разрешение предотвращения засыпания устройства, и другие. Лицам, находящимся на карантине по подозрению о возможности заражения COVID-19, органы местного самоуправления подписания документа под названием «Обязательство о соблюдении правил карантина и принятии ограничений» (на русском/кыргызском языках), обязательной установки мобильного приложения «Stop COVID-19 KG» и отправке отчета о такой установке в виде скриншота экрана телефона на приложение Вотсап (WhatsApp). В обязательстве указана обязанность дать согласие на проведение телеметрических наблюдений посредством аудио/видено сессий, установить указанное приложение, обеспечить работоспособность мобильного устройства для работы приложений, поддерживать надлежащий уровень заряда батареи мобильного устройства, а также подключения к сети интернет.

ГРАЖДАНСКАЯ ИНИЦИАТИВА
ИНТЕРНЕТ ПОЛИТИКИ

ул. Рыскулова, 79-Б, 3 этаж, офис № 13
+996 312 54 04 40 / +996 770 700 300
info@gipi.kg
@internet_policy

www.internetpolicy.kg