АНАЛИТИЧЕСКАЯ ЗАПИСКА

Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики

«УТВЕРЖДАЮ»

И.о. директора
Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики
А.Б. Касымбеков

_____

«_____» _____ 2023 г.

Анализ регулятивного воздействия к проекту Закона Кыргызской Республики «О защите персональных данных»

Основания для разработки:

Приказ Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики «О создании рабочей группы по проведению Анализа регулятивного воздействия проекта Закона Кыргызской Республики «О защите персональных данных» от «23» октября 2023 года № 47-п.

Сроки проведения АРВ: 23 октября – 15 декабря 2023 года

Руководитель рабочей группы:

Т.К. Мамбетакунова – заведующая отделом законодательной экспертизы защиты персональных данных Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики

_____

Члены рабочей группы:

К.С. Омельченко – заместитель министра цифрового развития Кыргызской Республики

_____

М.М. Бостонкулов – специалист управления развития цифровых решений Министерства цифрового развития Кыргызской Республики

_____

Ж.Ч. Тегизбекова – кандидат юридических наук, эксперт, преподаватель по цифровому праву

_____

А.М. Токтосунова – директор Учебного центра Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики

_____

В.В. Ткачев – директор по IT-аудиту ОсОО «Бейкер Тилли Бишкек»

_____

Г.Т. Ускенбаева, Президент ОЮЛ «Ассоциация поставщиков (производителей и дистрибьюторов)»

_____

Ж.К. Коноева – главный инспектор отдела методологии надзора управления методологии надзора Национального Банка Кыргызской Республики

_____

Ж.С. Кыдыралиев – начальник сектора правовой поддержки головного офиса Юридического отдела ЗАО «Демир Кыргыз Интернешнл Банк»

_____

Эркинбек уулу С. – юрист юридического департамента ОАО «РСК Банк»

_____

Б.Т. Давлетбекова – начальник управления развития продуктов ОАО «Халык Банк Кыргызстан»

_____

М.Т. Осмоналиев – главный инспектор Управления по защите информационных ресурсов ОАО «Халык Банк Кыргызстан»

_____

Э.С. Бексултанов – заместитель начальника Управления информационной безопасности ОАО «Оптима Банк»

_____

Д. Бозгорпоев – ведущий юрист ОЮЛ «Ассоциация операторов связи»

_____

С.С. Тагаева – главный инспектор отдела законодательной экспертизы защиты персональных данных Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики, секретарь рабочей группы

_____

Контактные данные ответственного лица:
С.С. Тагаева, телефон 0312 641019, e-mail: tagaeva@dpa.gov.kg, адрес: 720071, г. Бишкек, пр. Чуй, 265а, здание Национальной Академии наук, 2 этаж, западное крыло, Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики.

I. Проблемы и основания для изменения регулирования

1. Описание проблемы

Кыргызская Республика, понимая значение, роль и преимущества информационно-телекоммуникационных технологий в вопросах модернизации системы государственного управления, активно внедряет цифровые технологии практически во все сферы системы государственного управления и общественной жизни. Цифровая среда, обладая значительным потенциалом для реализации прав и свобод граждан, является при этом сложной системой, которая подвержена быстрой эволюции, и во многих отношениях, оказывая влияние на жизнь простых граждан, может привести к возникновению рисков нарушения их прав.

В 2008 году был принят Закон Кыргызской Республики «Об информации персонального характера» (далее – Закон), который регулирует вопросы, связанные с работой с персональными данными в целях обеспечения защиты прав и свобод человека и гражданина при сборе, обработке и использовании его персональных данных.

С 2008 года в Закон были внесены некоторые изменения (в редакции Законов от 20 июля 2017 года № 129, 29 ноября 2021 года № 142, 30 июня 2022 года № 53, 12 июля 2022 года № 61), при этом Закон не обновлялся ключевым образом в течении пятнадцати лет, в связи с чем, назрела острая необходимость модернизации законодательной базы в области защиты персональных данных. В частности, существует необходимость упрощения процедур получения согласия на сбор и обработку персональных данных, и его отзыв, включения норм по защите персональных данных детей, более четкого установления функций уполномоченного органа, расширения прав субъекта персональных данных и конкретного разграничения прав и обязанностей держателей и обработчиков массивов персональных данных.

Так, в соответствии со статьей 9 действующего Закона согласие субъекта должно быть выражено в письменной форме на бумажном носителе, либо в форме электронного документа, подписанного в соответствии с законодательством Кыргызской Республики электронной подписью. Учитывая, что существующий порядок получения согласия является сложным и устаревшим, проектом Закона предлагается упростить существующий порядок получения согласия субъекта персональных данных путем установления порядка получения согласия в добровольном, конкретном, информированном и однозначном волеизъявлении, в котором субъект персональных данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных, в форме, позволяющей подтвердить факт его получения. Кроме того, включаются нормы о необходимости получения согласия субъекта персональных данных только в письменной форме или в виде цифрового документа иными законодательными актами.

Действующим законодательством не предусмотрено право субъекта на отзыв своего согласия на обработку его персональных данных, который ограничивает права субъектов персональных данных, в связи с чем, предусматривается ввести статью «Отзыв согласия субъектом персональных данных», который может являться основанием для уничтожения его персональных данных, собранных, обрабатываемых и хранящихся у держателя, в том числе тех данных, которые переданы обработчикам и третьим лицам.

Проектом предусматривается определение биометрических персональных данных и генетических персональных данных, как части специальных категорий персональных данных и их правового режима, а также вводятся понятия профилирования и псевдонимизации.

В настоящее время развитие искусственного интеллекта стремительно прогрессирует. Современные системы искусственного интеллекта повсеместно используются для сбора и обработки как явных данных о человеке, таких как имя, место жительства и т.д., так и неявных сведений. Примером тому являются, социальные сети, где пользователь предоставляет свои персональные данные для регистрации на том или ином сайте (Facebook, Instagram, Одноклассники.ru и др.), а также других целей, а владельцы того или иного сайта в целях трекинга обрабатывают эти данные, в том числе используя технологии на базе искусственного интеллекта.

В связи с вышеизложенным, предлагается ввести статью «Использование автоматизированной обработки персональных данных, влекущее правовые последствия для субъекта персональных данных», которая устанавливает порядок обработки персональных данных субъектов искусственным интеллектом.

Кроме этого, предлагается предусмотреть право возражения субъектом по вопросам обработки его персональных данных, в том числе отказ от обработки для целей прямого маркетинга, а также предусмотреть полномочия уполномоченного государственного органа по персональным данным рассматривать заявления субъекта персональных данных о прекращении обработки излишних персональных данных, а также персональных данных, которые используются в целях прямого маркетинга или рассылки уведомлений, а также незаконной передачи третьим лицам.

Предлагаемым проектом планируется внедрить в качестве права субъекта получать компенсации за причиненный ущерб и моральный вред из средств, поступающих от взысканий, применяемых к держателям в соответствии с Кодексом Кыргызской Республики о правонарушениях.

При этом, предполагается еще несколько уровней, дающих право на получение компенсаций, в их числе медиация и арбитраж. Предполагается создание при Уполномоченном государственном органе независимого арбитража по рассмотрению споров, касающихся компенсации причиненного ущерба и морального вреда, после не урегулирования вопросов, связанных с

компенсацией причиненного ущерба и морального вреда посредством привлечения медиатора.

В свою очередь решения арбитража могут быть пересмотрены в судебном порядке по заявлению держателя, также субъект персональных данных, имеет право на возмещение причиненного ущерба и на компенсацию морального вреда в судебном порядке.

Обеспечение защиты персональных данных детей является одной из важнейших задач в области защиты данных. Дети в интернете сталкиваются с множеством угроз, таких как онлайн-хулиганство, кибербуллинг, недопустимый контент и другие риски. Для того, чтобы предотвратить эти угрозы, необходимо обеспечить эффективную защиту их персональных данных. Данная проблема является важной еще и из-за стремительного развития цифровых технологий и интернет-сервисов. Регулирование сбора, хранения и использования персональных данных детей урегулировано недостаточно четко законодательством Кыргызской Республики. В связи с чем, необходимы предлагаемые изменения, которые подробно регулируют особенности обработки персональных данных детей.

Глава 4 Закона регулирует права и обязанности держателя и обработчика по работе с массивами персональных данных.

В соответствии с частью 2 статьи 16 действующего Закона Кыргызской Республики «Об информации персонального характера» юридические лица имеют право на работу с персональными данными после регистрации в Уполномоченном государственном органе в качестве держателя (обладателя) массива персональных данных. Однако, проектом Закона должны быть предусмотрены положения, упрощающие данную норму, а именно предусматривающие, что юридические и физические лица, имеющие массивы персональных данных с данными более 10000 субъектов персональных данных, а также специальные категории персональных данных, вне зависимости от их количества собираемые для реализации целей, не закрепленных нормативными правовыми актами в качестве обязательных, образовательные и социальные организации, а также все государственные и муниципальные органы должны проходить регистрацию в вышеназванном реестре.

Предлагается дополнить организационные и технические меры защиты персональных данных и обязать держателей и обработчика принять правила внутреннего распорядка и внедрить меры, которые, в частности, отвечают принципам проектируемой защиты данных и защиты данных по умолчанию.

В связи с тем, что норма об обязательном информировании субъектов персональных данных об осуществленной передаче его персональных данных третьей стороне в любой форме в недельный срок не исполняется большинством держателей персональных данных, необходимо упростить порядок информирования субъектов персональных данных об

осуществленной передаче его персональных данных третьей стороне, за исключением трансграничной передачи персональных данных.

Кроме того, закрепить за Уполномоченным государственным органом по персональным данным определение порядка оценки адекватности применяемых мер защиты персональных данных и законодательства иностранных государств для включения в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных и за держателями ответственность в удостоверении в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

Проектом планируется предусмотреть регламентацию обеспечения соблюдения законодательства в области информации персонального характера и обязать держателей массивов персональных данных не позднее, чем через 72 часа после обнаружения нарушения безопасности персональных данных уведомить Уполномоченный государственный орган по персональным данным об инциденте, а также документировать любые нарушения безопасности персональных данных, в том числе их обстоятельства, последствия и меры, принятые для исправления ситуации, также, назначить ответственное лицо по защите персональных данных и предусмотреть правовые основания деятельности ответственного лица по защите персональных данных.

Проектом закона также должно быть предусмотрено право Уполномоченного государственного органа по персональным данным помимо самостоятельного контроля за соблюдением закона в сфере защиты персональных данных, право привлекать сторонние организации осуществляющие контрольные функции в отношении держателей, после прохождения аккредитации в Уполномоченном государственном органе по персональным данным.

Предлагаемые изменения упростят вопросы регистрации в реестре и получения согласия на сбор и обработку персональных данных субъектов и его отзыв, а также будут введены новые положения с учетом внедрения современных технологий.

Существующие и потенциальные угрозы в сфере пер относятся к числу наиболее серьезных вызовов XXI века. Эти угрозы от широкого круга источников проявляются в подрывных действиях, направленных как против физических лиц, бизнеса, государственных органов, так и против правительства. Их последствия несут в себе существенный риск для общественной безопасности, безопасности государств и стабильности глобально связанного между собой международного сообщества как единого целого».

Особенно это актуализируется в условиях, когда государственные органы и частные структуры используют биометрические данные граждан для обеспечения эффективной цифровой трансформации. В перспективе предусматривается активное использование информационно-коммуникационных технологий для достижения целей модернизации государственного управления, экономики и социальной сферы посредством инновационных технологий, где основным идентификатором гражданина будут выступать только его персональные данные.

Результаты анализа мнений заинтересованных лиц относительно существующего регулирования

Заинтересованные лица:

- Уполномоченный орган – Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики считает, что модернизация Закона Кыргызской Республики «Об информации персонального характера» необходима из-за стремительного развития цифровых технологий и интернет-сервисов и должны быть предусмотрены нормы, которые определяют не только порядок обработки персональных данных детей, но и субъектов персональных данных при использовании искусственного интеллекта. Также необходимо предусмотреть нормы, обеспечивающие эффективную защиту персональных данных детей.
- Субъекты предпринимательства считают, что должны быть внедрены справедливые меры защиты прав не только граждан, но и субъектов предпринимательства, которые в полной мере бы обеспечивали не только неотвратимость наказания, в случаях нарушения прав граждан в области защиты их персональных данных, но и применять упрощенные меры при для получения согласия субъектов персональных данных, их уведомления, поскольку действующее регулирования в части уведомления субъектов накладывает дополнительное бремя для субъектов предпринимательства.

2. Масштаб проблемы

Разработанным проектом затрагиваются все юридические и физические лица, которые осуществляют хранение и обработку персональных данных не для личных, семейных или хозяйственных целей физического лица.

Вследствие динамичной эволюции новейших информационных технологий перед правоприменителями возникают вопросы в области защиты персональных данных, до настоящего времени не урегулированных на законодательном уровне.

Так, масштаб возникшей проблемы охватывает различные спектры деятельности любого субъекта, так или иначе взаимодействующих с институтом «персональных данных».

В экономическом измерении

Экономические потери в случае отказа во внедрении представленных новшеств будут значительными и могут затронуть различные стороны экономики государства, в частности:

1. Рост числа цифрового мошенничества в интернет-среде вследствие ухода киберпреступности в виртуальную реальность может стать серьезным ударом по бизнесу, независимо от направления деятельности компании, а также по деятельности банковских, финансовых структур.

К примеру мошеннические манипуляции с безналичными денежными средствами на банковских счетах, жертвами которых становится широкие слои населения Кыргызстана, происходят вследствие правовой неграмотности последних, а также наличия пробелов в законодательствах, непосредственно регулирующих данную отрасль права. Так как в банковских системах содержатся большое число персональных данных о клиентах, сотрудниках и партнерах, то их безопасность должна строго контролироваться государством и самими владельцами банковских и финансовых структур в целях пресечения цифрового мошенничества и последующих за ним экономических последствий.

Представленная проблема может привести к дополнительным финансовым потерям как отдельного субъекта, так и банковской, финансовой структуры в целом.

2. Возникновение недоверительного отношения к финансовым и банковским структурам со стороны населения, что повлечет печальные последствия для репутации на национальном рынке соответственно окажет негативное влияние на деловые отношения.

3. Поскольку потребитель формирует мнение о деловой репутации организации/фирмы путем оценки качества предоставляемых услуг, их спектром, отношения сотрудников к клиентам, то несовершенства законодательства послужат причиной ослабления моральной составляющей самих сотрудников, влекущего массовые увольнения и соответственно образования безработицы в стране.

4. Отсутствие профилактики правонарушений и преступлений среди населения путем устранения пробелов в законодательстве, проведения массовых кампаний и повышения уровня правовой осведомленности повлечет увеличение значительной доли правонарушений и преступлений экономической направленности.

5. Постепенные выявляющиеся противоправные случаи в сфере персональных данных личности приведет к увеличению числа судебных разбирательств, соответственно повышению излишних судебных расходов, то есть несовершенство законодательства может вызвать споры между

субъектом персональных данных, держателем (обладателем) массива персональных данных и обработчиком относительно манипуляций в отношении персональных данных.

В социальном измерении.

Непринятие представленного проекта в дополнение затронут и социальные аспекты общества, в частности:

1. Со стремительным развитием информационных технологий так же стремительно учащаются случаи утечки персональных данных, в результате чего злоумышленники получают доступ к личным персональным данным субъекта. Полученную информацию злоумышленник может использовать в различных неправомерных целях, итог которого отразится на субъекте чрезвычайно негативно, что обусловит возникновение массовой волны обеспокоенного населения относительно защиты своих персональных данных (к примеру, взлом банковских счетов, кража, вымогательства, шантажи, угрозы, распространение данных жертвы в целях подрыва репутации и т.п.).

Полностью предотвратить утечки персональных данных довольно трудоемкая задача, однако консолидация усилий, комплексное регулирование, соблюдение правил цифровой гигиены и бережного отношения к своим персональным данным поможет свести риск неблагоприятных последствий к минимуму.

В территориальном измерении.

Данная проблема распространяется абсолютно на всю территорию Кыргызской Республики, поскольку персональные данные используются во всех сферах деятельности человека, выступая уязвимым институтом, а также риск возникновения неправомерных деяний повсеместно сохраняется на непрочной планке.

Для решения всех вышеперечисленных проблем необходимы предлагаемые изменения, которые способствуют в полном объеме реализовать Закон Кыргызской Республики «О защите персональных данных».

3. Основания для изменения регулирования, актуальность решения проблемы

Экономические основания для изменения регулирования.

Защита персональных данных имеет большое значение как для общества, так и для экономики страны. С постоянным развитием технологии хозяйствующим субъектам открывается возможность выходить на международной рынок, предлагать и поставлять свои товары и услуги широкому кругу потребителей. Однако для того, чтобы функционировать на международном рынке, предприятиям необходим непрерывный доступ к данным, где бы такая информация ни находилась, предполагающий в свою очередь свободную трансграничную передачу данных, которая

способствует развитию экономики каждой отдельной страны и мировой экономики в целом. Данный факт является причиной тому, что настоящий вопрос поднимается на международном уровне, обсуждается хозяйствующими субъектами, и многие страны начинают проводить реформы в законодательстве, поскольку современные реалии демонстрируют явные признаки устаревания законодательства и несоответствия современным тенденциям.

Правовые основания для изменения регулирования.

Стремительные изменения общественной жизни, многообразие общественных отношений и моделей их развития и реализации способствуют возникновению пробелов в праве, поскольку субъект правотворчества не поспевает за тенденциями развития общественных отношений.

Так, необходима законодательная проработка вопроса контроля в сфере защиты конфиденциальной информации, повышение правовой грамотности населения в сфере персональных данных и квалификации держателей (обладателей) массива персональных данных и обработчиков. Очевидные проблемы в сфере персональных данных в современных реалиях свидетельствуют о том, что действующее законодательство нуждается в существенной доработке. Однако решение представленных проблем не должно налагаться только на государство, напротив, общественность, различные специалисты в области права и информационной безопасности также должны принимать активное участие в разработке предложений по усовершенствованию законодательства в данной области.

Взаимодействие государства и населения, повышение уровня правовой грамотности последних, также ответственность каждого при предоставлении своих персональных данных третьим лицам позволят в полной мере реализовать законодательство в сфере защиты персональных данных.

Актуальность решения.

Актуальность решения возникшей проблемы определяется тем, что для полноценной реализации Закона Кыргызской Республики «О защите персональных данных» необходимо его усовершенствование и принятие в новой редакции. В первую очередь задачей предлагаемой редакции выступает защита интересов общества в целом от несанкционированных утечек конфиденциальной информации для совершения неправомерных деяний злоумышленниками с вытекающими различными негативными последствиями.

4. Международный опыт

В ходе подготовки аналитической записки был изучен опыт стран ближнего и дальнего зарубежья по имеющейся ответственности за

нарушение законодательства в области защиты персональных данных. В частности, был изучен опыт следующих стран:

- Российская Федерация;
- Республика Казахстан;
- Республика Беларусь;

Кроме того наравне с изучением опыта указанных стран, было изучено и европейское законодательство.

Защита данных не похожа на охрану окружающей среды, где государства могут договориться о желаемом уровне токсинов и при этом иметь относительное четкое взаимное представление об этом уровне. Защита данных требует более целостного подхода, предполагающего участие в совместной работе широкого круга действующих лиц – обработчиков данных, субъектов данных, регулирующих органов. Здесь требуется совместный процесс обучения и посредничества снизу вверх, равно как и меры регулирования и принудительного исполнения сверху вниз.[1]

Глобальное информационное пространство, сформировавшееся в результате реализации таких инициатив, можно представить, как группу «островов», каждый из которых символизирует собой сообщество стран, гармонизировавших свое законодательство о защите данных под эгидой конкретной международной организации (ОЭСР, Совета Европы, Евросоюза, ОАГ). Эти «острова» гармонизированного законодательства окружены «морем» стран, не располагающих адекватным (по критериям международных организаций) или вообще каким-либо законодательством о защите персональных данных. Внутри каждого сообщества стран, гармонизировавших свое законодательство по определенным критериям осуществляется свободный трансграничный обмен персональными данными. Вектор дальнейшего развития информационного пространства в рамках таких сообществ - создание интегрированной информационной инфраструктуры на базе концепции «информационных магистралей» (information highway), одним из главных аспектов которого является формирование единообразного законодательства в рамках данного сообщества стран.

Ключевой проблемой международного правового регулирования обработки и передачи персональных данных с самого начала стала необходимость достижения консенсуса относительно фундаментальных принципов, на которых должна была основываться защита данных. Без достижения такого консенсуса невозможно разрешение конфликта законодательств разных стран при трансграничной передаче данных. Поскольку не существовало никакой международной организации, которая

---

[1] Bennett, C.(1998) Application of a Methodology designed to Assess the Adequacy of the Level of Protection of Individuals with regard to Processing Personal Data: Test of the Method on Several Categories of Transfer. European Commission Tender No. XV/97/18/D, September 1998. Доступно через: http:// ec.europa.eu/justice/data-protection/document/studies/files/19980901_adequacy_methodology_en.pdf.

могла бы установить единые «правила игры», инициативу взяли на себя транснациональные организации, представляющие политико-экономические союзы и сообщества государств: ООН, ОЭСР, Совет Европы, Европейский союз.

В резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (ноябрь, 1999 г.) отмечается необходимость разработки международных принципов, которые были бы направлены на усиление безопасности глобальных информационных и телекоммуникационных систем и способствовали борьбе с информационным терроризмом и криминалом.[2]

В настоящее время высказываются предложения о том, что органом, обеспечивающим надлежащую защиту прав субъектов персональных данных на глобальном уровне может стать межправительственное объединение – Организация Объединенных Наций.[3]

Правовая система Кыргызской Республики в целом образуется из международных стандартов. Исключением в данной ситуации Закон Кыргызской Республики «О защите персональных данных» не является, поскольку полностью отвечает современным международным требованиям в области защиты персональных данных.

Однако с бурной эволюцией информационных технологий перед нормотворцами возникает необходимость своевременных доработок законодательства с учетом современных реалий. Главным общеевропейским документом, определяющим работу с персональными данными, обеспечивающим защиту прав пользователей в интернете, регулирующим, в частности, передачу, обработку, хранение персональных данных каждого человека, который находится на территории Евросоюза, либо является гражданином ЕС, выступает общеевропейская директива «Общие правила защиты данных», или General Data Protection Regulation (GDPR), вступившая в силу на территории ЕС 25 мая 2018 года.

Формальное соблюдение норм GDPR не распространяется на Кыргызскую Республику, однако Общий регламент о защите данных действует не только на территории Евросоюза, а применяется всеми его гражданами, вне зависимости их местонахождения. Если субъект Кыргызской Республики собрал и обработал персональные данные резидента Евросоюза — он обязан был это сделать по нормативам GDPR.

Так, предлагаемый законопроект «О защите персональных данных» в новой редакции разработан в целях гармонизации с международными стандартами.

---

[2] Генеральная Ассамблея ООН (1999) Резолюция A/RES/54/49 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Доступно через: http://daccessdds-ny.un.org/doc/UNDOC/GEN/N99/777/15/PDF/N9977715.pdf?OpenElement

[3] Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/ groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf

II. Описание предлагаемого регулирования

5. Цель государственного регулирования

Основной целью государственного регулирования является внедрение эффективных мер обеспечения соблюдения 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, достижение которой будет способствовать развитию системы защиты персональных данных в Кыргызской Республике.

Наименование показателя оценки прогресса	**Целевое значение**	**Срок достижения**
Количественные индикаторы		
Согласие субъекта персональных данных	В соответствии со статьей 9 действующего Закона согласие субъекта должно быть выражено в письменной форме на бумажном носителе, либо в форме электронного документа, подписанного в соответствии с законодательством Кыргызской Республики электронной подписью. Учитывая, что существующий порядок получения согласия является сложным и устаревшим, проектом Закона предлагается упростить существующий порядок получения согласия субъекта персональных данных путем установления порядка получения согласия в добровольном, конкретном, информированном и однозначном волеизъявлении, в котором субъект персональных данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных, в форме, позволяющей подтвердить факт его получения. Кроме того включаются нормы о необходимости получения согласия субъекта персональных данных только в письменной форме или в виде цифрового документа иными законодательными актами.	II квартал 2025 года
Отзыв согласия субъектом персональных данных	Действующим законодательством не предусмотрено право субъекта на отзыв своего согласия на обработку его персональных данных, который ограничивает права субъектов персональных данных, в связи с чем, предусматривается ввести статью «Отзыв согласия субъектом персональных данных», который может	III квартал 2025 года

	являться основанием для уничтожения его персональных данных, собранных, обрабатываемых и хранящихся у держателя, в том числе тех данных, которые переданы обработчикам и третьим лицам.	

6. Предлагаемое регулирование

В ходе проведения анализа регулятивного воздействия перед рабочей группой были рассмотрены следующие варианты:

Вариант № 1. «Оставить все как есть»

Вариант № 2. Разработать новый Закон Кыргызской Республики «О защите персональных данных» и признать утратившим силу действующий Закон Кыргызской Республики «Об информации персонального характера».

1) **Вариант № 1:** «Оставить все как есть»

Данный вариант не меняет существующее регулирование. В случае его сохранения для уполномоченного органа сохранятся условия ненадлежащего выполнения своих функций.

Также не будут эффективно реализованы требования законодательства Кыргызской Республики в области защиты персонального характера, в особенности в части касающихся персональных данных детей.

В настоящее время отсутствует общее понимание ценности персональных данных детей и необходимости их сохранности в кибер-пространстве, в том числе мессенджерах и социальных сетях у основной массы родителей, самих детей, сотрудников и руководителей образовательных учреждений в Кыргызской Республике. Системный подход в решении проблемы защиты детей в киберпространстве возможно внесением изменений в действующий Закон Кыргызской Республики «Об информации персонального характера», в котором следует предусмотреть раздел по защите детей, регулирующий кибербезопасность несовершеннолетних в Кыргызской Республике.

Действующим Законом биометрические данные и генетические персональные данные не рассматриваются как часть специальных категорий персональных данных, так как биометрика выведена в отдельный институт, а также отсутствуют понятия профилирования и псевдонимизации.

Выведение биометрики в отдельный от персональных данных институт создает проблемы, особенно сейчас, когда идет активное использование информационно-коммуникационных технологий для достижения целей модернизации государственного управления, экономики и социальной сферы посредством инновационных технологий, где основным идентификатором гражданина будут выступать только его персональные данные.

При сохранении варианта «Оставить все как есть» сохранится на прежнем уровне защита персональных данных, а нарушенные права могут быть защищены только в судебном порядке, что также существенно забюрократизирует возможность защиты своих прав в досудебном порядке и снизит возможности профилактики и недопущения защиты прав граждан.

Одновременно снизится качество внедрения единообразного подхода в вопросах защиты персональных данных держателями и обработчиками персональных данных.

Также норма об обязательном информировании субъектов персональных данных об осуществленной передаче его персональных данных третьей стороне в любой форме в недельный срок не исполняется большинством держателей персональных данных, что порождает факт увеличения числа мертвых или нереализуемых норм.

2) **Вариант № 2:**

Разработать новый Закон Кыргызской Республики «О защите персональных данных» и признать утратившим силу действующий Закон Кыргызской Республики «Об информации персонального характера».

Способ регулирования

Предлагается следующее регулирование.

Задача.

Создать эффективную систему правового регулирования сбора, обработки и хранения персональных данных посредством гармонизации законодательства, унификации терминов и понятий, а также внедрить международные стандарты в области защиты персональных данных в целях устранения барьеров и развития международного научно-технического и правового сотрудничества, обеспечения полноценного участия Кыргызской Республики в международных механизмах регулирования отношений, связанных с обеспечением защиты персональных данных.

Проблемы субъектов регулирования	Предлагаемое регулирование
Отсутствие четкости в определении правовой базы биометрических персональных данных. Наличие специализированного Закона КР «О биометрической идентификации граждан» и содержания статьи 1 Закона выводит регулирование вопросов биометрических граждан в отдельный институт. При этом в данном институте не предусматривается возможность использования биометрических данных коммерческими организациями, в том числе финансово-кредитными	Предлагается предусмотреть в новом проекте Закона определение биометрических персональных данных и генетических персональных данных, как части специальных категорий персональных данных и их правового режима, а также понятий профилирования и псевдонимизации. Также необходимо определить статус базы биометрических данных и субъектов, которые могут получать к ней доступ при соблюдении всех

организациями. Более того, сбор, хранение и обработка таких данных может осуществляться только в порядке, определяемом Кабинетом Министров Кыргызской Республики и только в объеме, определенном частью 3 статьи 5 вышеназванного закона.	требований в области безопасности и с соблюдением требований по получению согласия субъектов биометрических данных на обработку их биометрических данных.
Проблемы получения согласия при заключении гражданско-правового договора с субъектом персональных данных в соответствии с ч. 2 ст. 2, ч.1 ст. 7, ч. 1 ст.381, ч. 1 ст.382 ГК КР. В соответствии со статьей 9 действующего Закона Кыргызской Республики «Об информации персонального характера» согласие субъекта должно быть выражено в письменной форме на бумажном носителе, либо в форме электронного документа, подписанного в соответствии с законодательством Кыргызской Республики электронной подписью. Учитывая, что существующий порядок получения согласия является сложным и устаревшим.	Предлагается в новом проекте Закона исключить необходимость получения согласия субъекта персональных данных на сбор и обработку его данных, поскольку сам факт заключения гражданско-правового договора уже является согласием субъекта персональных данных на вступление в правоотношения и, соответственно, осуществление необходимых действий с его персональными данными, в целях своевременного и надлежащего исполнения обязательств по договору, исходя из предмета договора, прав и обязанностей сторон договора.
Отсутствие у субъекта персональных данных права на отзыв своего согласия на обработку его персональных данных, который ограничивает права субъектов персональных данных.	Предусматривается ввести статью «Отзыв согласия субъектом персональных данных», который может являться основанием для уничтожения его персональных данных, собранных, обрабатываемых и хранящихся у держателя, в том числе тех данных, которые переданы обработчикам и третьим лицам.
Отсутствие право на возражения субъектом по вопросам обработки его персональных данных, в том числе отказ от обработки для целей прямого маркетинга, а также полномочия уполномоченного государственного органа по персональным данным рассматривать заявления субъекта персональных данных о прекращении обработки излишних персональных данных, а также персональных данных, которые используются в целях прямого маркетинга или рассылки уведомлений, а также незаконной передачи третьим лицам.	Предлагается предусмотреть право возражения субъектом по вопросам обработки его персональных данных, в том числе отказ от обработки для целей прямого маркетинга, а также предусмотреть полномочия уполномоченного государственного органа по персональным данным рассматривать заявления субъекта персональных данных о прекращении обработки излишних персональных данных, а также персональных данных, которые используются в целях прямого

	маркетинга или рассылки уведомлений, а также незаконной передачи третьим лицам.
Регулирование сбора, хранения и использования персональных данных детей урегулировано недостаточно четко законодательством Кыргызской Республики. Обеспечение защиты персональных данных детей является одной из важнейших задач в области защиты данных. Дети в интернете сталкиваются с множеством угроз, таких как онлайн-хулиганство, кибербуллинг, недопустимый контент и другие риски. Для того, чтобы предотвратить эти угрозы, необходимо обеспечить эффективную защиту их персональных данных. Данная проблема является важной еще и из-за стремительного развития цифровых технологий и интернет-сервисов.	Предлагается предусмотреть нормы, которые подробно регулируют особенности обработки персональных данных детей. Также рассмотреть случаи обработки персональных данных детей.
Проблема регистрации в реестре держателей (обладателей) массивов персональных данных. В соответствии с частью 2 статьи 16 действующего Закона Кыргызской Республики «Об информации персонального характера» юридические лица имеют право на работу с персональными данными после регистрации в Уполномоченном государственном органе в качестве держателя (обладателя) массива персональных данных. В настоящее время должны пройти регистрацию в реестре все юридические лица, которые работают с массивами персональных данных вне зависимости от количества записей. Учитывая, что количество субъектов предпринимательства по информации Государственной налоговой службы при Министерстве финансов Кыргызской Республики на территории Кыргызской Республики насчитывается около **166 255** юридических лиц, обязывать юридических лиц, имеющих массивы персональных данных в пределах штатной численности сотрудников, либо не относящиеся к специальным	Предлагается предусмотреть регистрацию в реестре держателей (обладателей) массивов персональных данных юридических и физических лиц, имеющих массивы персональных данных с данными более 10000 субъектов персональных данных, а также специальные категории персональных данных. Данная мера позволит юридическим лицам, не имеющим массивы менее 10000 записей персональных данных, к примеру организации, имеющие несколько сотрудников в штате и не имеющие информационные системы или базы данных с персональными данными граждан.

категориям персональных данных, **нецелесообразно**.	
Действующим Законом держатель (обладатель) массива персональных данных обязан информировать субъект персональных данных об осуществленной передаче его персональных данных третьей стороне в любой форме **в недельный срок.** Данная норма не выполняется большинством держателей персональных данных, что порождает факт увеличения числа мертвых или нереализуемых норм. Исполнение указанной нормы порождает дополнительные финансовые и организационные нагрузки на держателя персональных данных, поскольку уведомление субъекта в любой предусмотренной форме должна выражаться направлением уведомления через почту, либо через мессенджеры, либо другим способом каждого субъекта персональных данных.	При разработке проекта Закона в новой редакции предлагается указать норму, по которой держатель обязан информировать субъект персональных данных об осуществленной передаче его персональных данных третьей стороне **по запросу субъекта.**

7. Оценка вероятных социальных и экономических последствий регулирования

7.1. Ожидаемая результативность (уровень достижения цели регулирования) на дату.

Предлагаемый законопроект в новой редакции должен обеспечить соблюдение законодательства в области защиты персональных данных, создав условия, при которых, с одной стороны, держателями (обладателями) массивов персональных данных будут предприниматься необходимые меры по недопущению нарушений прав субъектов персональных данных, а с другой стороны, субъекты будут уверены в наличии достаточных правовых оснований для защиты их персональных данных.

Такой баланс взаимоотношений между держателями (обладателями) массивов персональных данных и субъектами персональных данных, выражающийся в приведении своих бизнес-процессов и организационно-правовых основ деятельности к уровню, установленному законодательством – с одной стороны, и доверие субъектов к держателям (обладателям) – с другой стороны, позволит обеспечить развитие института защиты персональных данных в полном объеме.

Сами по себе значительные новшества должны в ближайшие несколько лет с момента принятия законопроекта обеспечить соответствующий уровень контроля за соблюдением требований в области защиты персональных данных, создание дополнительных внутренних бизнес-процессов, обеспечивающих прозрачность деятельности держателей (обладателей) массивов персональных данных. Указанные нововведения, связанные с защитой персональных данных, дают гражданам больше возможностей по контролю использования своей личной информации.

7.2. Ожидаемое воздействие на экономику, социальный сектор и экологию:

1) воздействие на экономику: ожидается качественное изменение на уровне защищенности информационных систем и информации персонального характера, что будет позитивным сдвигом для повышения интеграционных процессов внутри экономики Кыргызской Республики, а также повышение качества электронных услуг;

2) воздействие на социальную сферу: повышается защищенность персональных данных граждан, детей и их правовая обеспеченность;

3) воздействие на экологию: какого-либо воздействия не ожидается. Более того, при росте защищенности персональных данных будет осуществляться и рост взаимодействия граждан и частного сектора. Посредством информационных технологий благодаря повышению доверия взаимодействие между гражданами и государством, а также государством и частным сектором также перейдет в цифровую плоскость, что будет благотворно влиять на экологию ввиду снижения использования бумаги и вырубки лесного покрова Земли.

7.3. Ожидаемое воздействие на основные группы заинтересованных сторон - адресатов регулирования:

1) государственные органы (с разделением по государственным органам):

Уполномоченный орган – Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики

Позитивное последствие:

Будут внедрены нормативно-правовые основы по обеспечению прав граждан в области персональных данных.

За счет средств получаемых в ходе правоприменительной практики будет пополняться республиканский бюджет, что будет способствовать частичному покрытию его дефицита.

Негативное последствие: отсутствует.

2) предприниматели (с разделением по выбранному критерию):

Держатели массивов персональных данных:

Позитивное последствие:

Совершенствуется система защиты персональных данных в соответствии с требованиями законодательства с целью создания дополнительных внутренних бизнес-процессов, обеспечивающих прозрачность деятельности субъектов предпринимательства на всех уровнях.

Качественно новый подход к работе с персональными данными клиентов и информацией в целом будет способствовать повышению качества оказываемых услуг, как на территории Кыргызской Республики, так и за ее пределами.

Негативное последствие: отсутствует.

3) население (с разделением по выбранному критерию):

Субъекты персональных данных (физические лица):

Позитивное последствие: снижение рисков, связанных с нарушениями режимов конфиденциальности персональных данных при их сборе, хранении и обработке, создание эффективной системы реагирования со стороны контролирующего органа на инциденты, связанные с их персональными данными, обеспечение прав отдельной категории уязвимого населения - детей в области защиты их персональных данных, а также предоставление гарантии со стороны государства на компенсацию причиненного ущерба и морального вреда вследствие нарушения сбора, обработки, передачи и хранения персональных данных.

Также предусматривается, что разработка и интеграция представленного законопроекта позволит субъектам персональных данных получать более качественные услуги, а также снизить необходимость избыточного сбора и обработки данных субъектов персональных данных со стороны субъектов предпринимательства.

Негативное последствие: отсутствует.

8. Оценка затрат и выгод

8.1. Оценка затрат и выгод субъектов предпринимательства:

Затраты. Реализация данного варианта регулирования должна обеспечить соблюдение Закона Кыргызской Республики «Об информации персонального характера» путем внедрения комплекса организационно-технических мер для обеспечения режима конфиденциальности персональных данных. Таким образом, **возможные затраты субъектов регулирования** могут быть связаны с тем, что им придется приводить свои внутренние правила, процедуры, а также техническое оснащение в соответствие с требованиями отраслевого закона, а также Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных, утвержденных постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 760.

Вместе с тем, дополнительные затраты могут возникнуть при реализации нормы, предусматривающую организацию обучения правилам и рекомендациям в сфере обработки персональных данных кадровых штатов субъектов регулирования и организацию их эффективного применения, проводимых за счет самих субъектов регулирования.

Выгоды. Внедрение механизма справедливого контроля субъектов предпринимательства с учетом соблюдения прав субъектов исключает излишнее вмешательство в предпринимательскую деятельность в виде необоснованных проверок. Из-за исключения необоснованных плановых проверок снижается регуляторная нагрузка на бизнес, что позволяет ему

повышать прибыль и развиваться, в том числе посредством внедрения новых технологий.

8.2. Оценка затрат и выгод государственного бюджета:

Затраты. Отсутствуют.

Выгоды. Создание благоприятных правовых условий для обеспечения 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. Предлагаемый проект внедряет единые требования ко всем участникам рынка, что будет способствовать выравниванию уровней защиты персональных данных при их обработке в информационных системах держателей массивов персональных данных, что позволит повысить интенсивность предпринимательской активности, внедрению новых технологий, а также будет способствовать повышению интеграции и информационному взаимодействию всех участников рынка.

Общий вывод по оценкам: предложенное регулирование позволяет обеспечить прогресс в достижении цели и решить идентифицированные проблемы. При этом ожидается достижение важного социального-экономического эффекта в виде повышения защищенности персональных данных и улучшения предпринимательской среды. Воздействие на основных адресатов регулирования являются не обременительными и соответствуют требованиям действующих нормативных правовых актов в области защиты персональных данных.

9. Оценка реализационных рисков

1. Риски недостаточности необходимых материальных и человеческих ресурсов.

Оценка риска: оценивается как отсутствующий.

Меры смягчения - не требуются.

2. Риски необеспечения надлежащего контроля за соблюдением требований, вводимых предложенным регулированием.

Оценка риска: оценивается как отсутствующий, поскольку обеспечение контроля за соблюдением нового регулирования закреплено за Государственным агентством по защите персональных данных при Кабинете Министров Кыргызской Республики.

Меры смягчения - не требуются.

3. Риски недостаточности механизмов для реализации предложенного регулирования.

Оценка риска: оценивается как низкий, так как реализации предложенного регулирования не требует изменения существующего механизма.

Меры смягчения– не требуются.

4. Риски несоответствия предложенного регулирования и существующего административно-управленческого потенциала для его реализации.

Оценка риска: оценивается как отсутствующий, так как объем регулятивного вмешательства незначительный, а существующего потенциала для реализации достаточно.

Меры смягчения – не требуются.

10. Оценка воздействия на конкуренцию

Предложенный вариант регулирования не оказывает негативного воздействия на конкуренцию. Подробнее оценка воздействия на конкуренцию изложена в Таблице 1.

Таблица 1

№ фактора	Фактор, ограничивающий конкуренцию	Оценка "да"или "нет"
1	2	3
Оценка уровня концентрации товарного рынка		
1	Имеется ли доминирующее положение, при котором доля какого- либо хозяйствующего субъекта на данном товарном рынке составляет 35 процентов или выше - при наличии данных?	**Нет**
2	Имеется ли доминирующее положение, при котором совокупное доминирование более чем трех хозяйствующих субъектов, доля каждого из которых больше доли других субъектов на этом рынке и в совокупности превышает 50 процентов, или совокупная доля не более чем пяти хозяйствующих субъектов, доля каждого из которых больше долей других хозяйствующих субъектов на соответствующем рынке - при наличии данных?	**Нет**
Оценка экономических ограничений входа-выхода на товарный рынок		
3	Приведет ли новое регулирование к непропорционально высоким затратам: - для потенциальных участников рынка, чем это было для действующих; - для малых предприятий, чем это предполагается для крупных предприятий и т.д.	**Нет**

4	Приведет ли новое регулирование к существенному ограничению доступа потенциальных участников к ресурсам (материально- вещественным, нематериальным и другим), предложение которых на рынке ограничено?	**Нет**
5	Приведет ли новое регулирование к неприемлемо высоким (способным подорвать экономическую устойчивость) издержкам действующих хозяйствующих субъектов при их вынужденном прекращении деятельности на данном товарном рынке, связанным с новым регулированием?	**Нет**
Оценка административных ограничений входа на товарный рынок		
6	Приведет ли новое регулирование к существенному росту лицензионных требований и стоимости процедур получения лицензии для потенциальных участников рынка?	**Нет**
7	Приведет ли новое регулирование к нарушению условий равенства прав хозяйствующих субъектов при административном распределении ограниченных ресурсов?	**Нет**
8	Приведет ли новое регулирование к ограничению действующих хозяйствующих субъектов выбирать механизм ценообразования, определять качество продукции, местонахождение размещения производственных мощностей?	**Нет**
Оценка стратегических ограничений входа на товарный рынок		

9	Приведет ли новое регулирование к получению дополнительных преимуществ для участников различных устойчивых форм хозяйственной интеграции (холдинги, финансово-промышленные объединения, кластеры с низким уровнем взаимной конкуренции его участников и высоким уровнем кооперации и другие) по сравнению с другими потенциальными участниками рынка, не входящими в такие формы интеграции?	**Нет**

11. Мнения заинтересованных сторон

В соответствии с Методикой проведения анализа регулятивного воздействия нормативных правовых актов на деятельность субъектов предпринимательства, утвержденная постановлением Кабинета Министров Кыргызской Республики от 10 августа 2022 года № 444 (далее – Методика), уведомление о разработке проекта нормативного правового акта для сбора предложений заинтересованных лиц был размещен на официальном сайте Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики https://dpa.gov.kg/ru/npa/42 6 ноября 2023 года для проведения публичных консультаций на срок не менее 15 дней.

В ходе публичных консультаций в рамках проведения анализа регулятивного воздействия при разработке соответствующего законопроекта поступил ряд предложений от заинтересованных сторон, которые были рассмотрены рабочей группой и приняты к сведению для дальнейшей его проработки.

В целом принятие законопроекта в сфере защиты персональных данных в новой редакции поддерживается всеми участниками рабочей группы в проводимом анализе регулятивного воздействия .

Данные о замечаниях и предложениях отображены в Таблице 2.

Таблица 2

Участник публичных консультаций	Количество замечаний и предложений, внесенных в Реестр замечаний и ответов
Член рабочей группы от ОЮЛ «Ассоциация операторов связи» Бозгорпоев Дж.Б.	14

12. Обоснование выбора предлагаемого регулирования

Сравнение вариантов регулирования:

Вариант № 1 «Оставить все как есть»;

Вариант № 2 «Разработать новый Закон Кыргызской Республики «О защите персональных данных» и признать утратившим силу действующий Закон Кыргызской Республики «Об информации персонального характера».

показало:

В варианте №1 «Оставить все как есть» сохраняются все проблемы, указанные в разделе 1. Проблемы и основания для изменения регулирования.

В варианте № 2 - все идентифицированные проблемы устраняются.

Руководствуясь критериями достижения цели, решения проблем и отсутствия негативных эффектов в экономике, социальной сфере и экологии, а также отсутствия чрезмерных административных издержек для держателей (обладателей) массивов персональных данных и затрат государства, вариант регулирования № 2 признан более предпочтительным.

Указанные в разделе 1 проблемы Уполномоченного органа по персональным данным, а также трудности держателей (обладателей) массивов персональных данных в процессе своей деятельности и в результате внедрения предлагаемого регулирования будут решены.

Так, нововведения должны обеспечить соблюдение законодательства в области защиты персональных данных в целом, создав систему гарантированного обеспечения безопасности государством информации персонального характера на всех уровнях государственной деятельности.

Одновременно будут решены вопросы уменьшения рисков, связанных с нарушениями режимов конфиденциальности персональных данных при их сборе, хранении и обработке, создания эффективной системы реагирования со стороны контролирующего органа на инциденты, связанные с их персональными данными, обеспечения прав отдельной категории уязвимого населения - детей в области защиты их персональных данных, а также предоставления гарантии со стороны государства на компенсацию причиненного ущерба и морального вреда вследствие нарушения сбора, обработки, передачи и хранения персональных данных.

В перспективе в случае разработки и принятия соответствующего законопроекта должно быть обеспечено планомерное внедрение системы контроля за соблюдением требований в области защиты персональных данных, создание дополнительных внутренних бизнес-процессов, обеспечивающих прозрачность деятельности субъектов предпринимательства на всех уровнях.

Вывод: в результате проведенного анализа регулятивного воздействия можно прийти к однозначному выводу, что в настоящее время целесообразно применить вариант № 2, предполагающий разработку Закон Кыргызской Республики «О защите персональных данных» в новой редакции с соответствующим признанием утратившим силу действующего Закона Кыргызской Республики «Об информации персонального характера».

13. Приложения

К аналитической записке прилагаются:

- развернутая оценка ожидаемых экономических последствий для предлагаемого регулирования (оценка отражена в аналитической записке);
- уведомление о разработке проекта Закона Кыргызской Республики «О защите персональных данных» (Приложение 1);
- Реестр предложений и ответов (Приложение 2);
- отчет о проведении публичных консультаций (Приложение 3);
- приказ об образовании рабочей группы по АРВ (прилагается копия);
- Сравнительно-правовой обзор предлагаемого регулирования в области защиты персональных данных на примере стран ближнего зарубежья (Приложение 5).

Приложение 5

Сравнительно-правовой обзор предлагаемого регулирования в области защиты персональных данных на примере стран ближнего зарубежья

	Страны			
	Кыргызская Республика Проект Закона КР «О защите персональных данных»	**Республика Казахстан** Закон РК «О персональных данных и их защите»	**Российская Федерация** ФЗ «О персональных данных»	**GDPR**
Отзыв согласия субъектом персональных данных	**Ст. 9 Согласие субъекта персональных данных на предоставление и обработку его персональных данных** Согласие может быть отозвано субъектом персональных данных после исполнения им своих гражданско-правовых обязательств перед владельцем записей. Отзыв согласия субъектом персональных данных является основанием для уничтожения его персональных данных, собранных, обрабатываемых и хранящихся у владельца записей, в том числе тех данных, которые переданы обработчикам и третьим лицам, за исключением случаев, когда уничтожение таких данных прямо запрещено законами Кыргызской Республики, а также имеются обязательные сроки хранения персональных данных. Отзыв согласия субъекта персональных данных не имеет обратной силы, то есть обработка персональных данных до ее прекращения не является незаконной.	**Ст.8 Порядок дачи (отзыва) согласия субъекта на сбор, обработку персональных данных** 1. Субъект или его законный представитель дает (отзывает) согласие на сбор, обработку персональных данных письменно, посредством государственного сервиса, негосударственного сервиса либо иным способом, позволяющим подтвердить получение согласия. При сборе и (или) обработке персональных данных, содержащихся в объектах информатизации государственных органов и (или) государственных юридических лиц, согласие предоставляется посредством государственного сервиса.	**Ст.9 Согласие субъекта персональных данных на обработку его персональных данных** 2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона. **Ст.21 Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных**	**Ст. 21 Право на возражение** 1. Субъект данных, по основаниям, связанным с его/ее конкретной ситуацией, имеет право в любой момент заявить возражение против обработки своих персональных данных, которая базируется на пункте (e) или (f) Статьи 6(1), в том числе против профилирования, основанного на данных положениях. Контролёр не в праве далее обрабатывать персональные данные, пока не продемонстрирует наличие убедительных легитимных оснований для обработки, которые превалируют над интересами, правами и свободами субъекта данных, или для заявления, осуществления или оспаривания правовых требований и исков. 2. Если персональные данные обрабатываются для целей прямого маркетинга, субъект персональных данных имеет право в любое время возражать против обработки своих персональных данных для целей такого маркетинга, в том числе профилирования, в той мере, в которой обработка относится к данному прямому маркетингу. 3. Если субъект данных возражает против

	Процедура отзыва согласия не должна быть более обременительной, чем процедура предоставления согласия.	2. Субъект или его законный представитель не может отозвать согласие на сбор, обработку персональных данных в случаях, если это противоречит законам Республики Казахстан, либо при наличии неисполненного обязательства.	5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными	обработки в целях прямого маркетинга, персональные данные больше нельзя обрабатывать для таких целей. 4. Не позднее момента первой коммуникации с субъектом данных, право, указанное в параграфах 1 и 2, должно быть отчетливо доведено до сведения субъекта данных и должно быть представлено ясно и отдельно от любой иной информации. 5. В связи с использованием услуг информационного общества и не умаляя положений Директивы 2002/58/ЕС субъект данных может реализовать свое право на возражение посредством автоматизированных средств, использующих технические спецификации. 6. В случае если персональные данные обрабатываются в целях научного или исторического исследования согласно Статье 89 (1), субъект данных должен иметь право на возражение по причинам, связанным с его конкретной ситуацией, против обработки относящихся к нему персональных данных, за исключением случаев, когда обработка необходима для выполнения задачи, осуществляемой по причинам публичного интереса.

			законами.	
Возмещение убытков и (или) компенсация морального вреда	**Ст. 16. Возмещение убытков и (или) компенсация морального вреда** 1. Субъект персональных данных имеет право на компенсацию причиненного ущерба и морального вреда из средств, поступающих от взысканий, применяемых к владельцам записей в соответствии с Кодексом Кыргызской Республики о правонарушениях, но не более 1/5 от суммы взыскания. 2. В случае наличия двух и более субъектов персональных данных, которым причинен ущерб или нанесен моральный вред, то причитающаяся компенсационная сумма, поступающая от взысканий, подлежит разделению в равных долях между всеми субъектами персональных данных, пострадавшими в результате действий этого владельца записей. 3. Часть 2 настоящей статьи не распространяется на случаи, когда более 5 субъектов персональных данных претендуют на компенсацию по одному и тому же обстоятельству. В такой ситуации субъекты персональных данных имеют право добиваться получения компенсации в порядке, предусмотренном частями 4, 5 и 8 настоящей статьи. 4. В целях получения дополнительной компенсации причиненного ущерба и морального вреда, полученного субъектом персональных данных вследствие действий владельца записей субъект персональных данных вправе обратиться к услугам медиатора в соответствии с Законом Кыргызской	**Ст. 24. Права и обязанности субъекта** Субъект имеет право на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда.	**Статья 17. Право на обжалование действий или бездействия оператора** 1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке. 2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.	**Статья 82. Ответственность и право на компенсацию** 1. Любое лицо, которое понесло материальный или нематериальный ущерб в результате нарушения положений настоящего Регламента, имеет право на получение компенсации от контролёра или процессора за понесенный ущерб. **2.** Любой контролёр, участвующий в обработке, несет ответственность за ущерб, причиненный в результате обработки, нарушающей настоящий Регламент. Процессор несет ответственность за ущерб, причиненный в результате обработки только если он не выполнил требования настоящего Регламента, специально установленные для процессоров, или если он действовал за рамками или в нарушение законных распоряжений контролёра. **3.** Контролёр или процессор освобождается от ответственности, упомянутой в параграфе 2, если докажет, что никоим образом не несет ответственность за событие, которое явилось причиной ущерба. **4.** Если более одного контролёра или процессора участвуют в одной и той же обработке данных, и если они согласно параграфам 2 и 3 несут ответственность за любой ущерб, причиненный обработкой, каждый контролёр или процессор несет ответственность за весь ущерб для гарантии эффективной компенсации субъекту данных. **5.** Если контролёр или процессор полность

	Республики «О медиации». 5. Для создания условий по всесторонней защите своих прав при Уполномоченном государственном органе создается независимый арбитраж по рассмотрению споров, касающихся компенсации причиненного ущерба и морального вреда, действующий на принципах независимости при формировании арбитров и самофинансирования за. Порядок формирования арбитража и регламент его работы определяются Кабинетом Министров Кыргызской Республики. Обращение в арбитраж допускается после неудачи урегулирования вопросов, связанных с компенсацией причиненного ущерба и морального вреда посредством непосредственного взаимодействия субъекта персональных данных и владельца записей в том числе с привлечением услуг медиатора. 6. Финансирование секретариата Арбитража, а также вознаграждений арбитров осуществляется за счет средств поступающих от рассмотрения споров по компенсации причиненного ущерба и морального вреда в размере 20 процентов от заявленной суммы требований. 7. В случае отсутствия зафиксированного размера суммы возмещения, то споры к рассмотрению Арбитражем не принимаются. 8. Решения арбитража носят обязательный характер для владельцев записей. 9. Решения арбитража могут быть пересмотрены в судебном порядке по			ю компенсировал согласно параграфу 4 причиненный ущерб, такой контролёр или процессор вправе предъявлять регрессный иск к другим контролёрам или процессорам, которые участвовали в этой же обработке, с целью возврата части компенсации, соответствующей их части ответственности за ущерб в соответствии с условиями параграфа 2. 6. Судебный иск об осуществлении права на компенсацию должен быть предъявлен в суд, компетентный согласно законодательству государства-члена, как указано в Статье 79(2).

	заявлению владельца записей. 10. Субъект персональных данных также имеет право на возмещение причиненного ущерба и на компенсацию морального вреда в судебном порядке.			
Персональные данные детей	**Статья 18. Особенности обработки персональных данных детей** 1. Обработка персональных данных детей допускается только в перечисленных ниже случаях и только если при этом учитываются интересы ребенка, а также закреплены в законе и применяются гарантии защиты основных прав и свобод детей: 1) обработка осуществляется на основании закона Кыргызской Республики, прямо предусматривающего необходимость обработки персональных данных детей, и определяющего цели их обработки; 2) обработка является необходимой для защиты жизненно важных интересов ребенка (субъекта персональных данных) или иного физического лица или группы лиц; 3) 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; 4) обработка осуществляется для защиты существенных интересов в области	**Аналогичная норма отсутствует**	**Аналогичная норма отсутствует**	**Статья 8. Условия, применимые к согласию ребенка в случае оказания услуг информационного общества** 1. Если применяется пункт (а) Статьи 6(1) при предоставлении услуг информационного общества непосредственно ребенку, обработка персональных данных ребенка является законной только в случае, если ребенку исполнилось как минимум 16 лет. Если ребенок еще не достиг возраста 16 лет, такая обработка является законной, исключительно в случаях, когда согласие было дано лицом, обладающим родительскими правами в отношении ребенка, или было дано с его одобрения. Государства-члены могут законодательно предусмотреть меньший возраст для указанных целей при условии, что такой возраст не ниже 13 лет. 2. В таких случаях контролёр, учитывая доступные технологические возможности, должен принять разумные усилия для того, чтобы удостовериться, что согласие было дано лицом, обладающим родительскими правами в отношении ребенка, или было дано с его одобрения. 3. Параграф 1 не влияет на общее договорное право государств-членов, например, на нормы о действительности, заключения сделки или правовых последствиях сделки в отношении ребенка.

	общественного здравоохранения, например, для мониторинга и защиты от опасной для жизни эпидемии и ее распространения или в целях гуманитарной помощи; 5) обработка необходима в связи с осуществлением правосудия, в том числе в рамках третейского производства; 6) обработка осуществляется для защиты национальной безопасности, обороны, общественной безопасности или предотвращения, расследования и судебного преследования уголовных преступлений и исполнения уголовных наказаний; 7) обработка осуществляется для медицинских, образовательных или консультационных услуг, предлагаемых непосредственно ребенку. 2. При отсутствии оснований, предусмотренных частью 1 настоящей статьи, 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. 3. 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. 4. Владельцы данных обязаны принимать меры, необходимые для предотвращения незаконной обработки персональных данных детей			
Оценка воздействия на защиту персональных данных	**Статья 25. Оценка воздействия на защиту персональных данных** 1. владелец записей перед обработкой персональных данных должен провести оценку воздействия планируемой обработки на защиту персональных данных. Применительно к набору схожих операций по обработке персональных данных, которые представляют схожий высокий риск, может быть проведена единая оценка. 3. Оценка воздействия на защиту персональных данных, проводится в обязательном порядке в следующих случаях: 1) систематической и комплексной оценки определенных личных аспектов физических лиц, которая основана на автоматизированной обработке, в том числе профилировании, и является основанием для решений, порождающих правовые последствия для физического лица или схожим образом существенно влияющих на физическое лицо; 2) крупномасштабной обработки особых категорий персональных данных; 3) систематического мониторинга публичных мест техническими средствами в том числе с использованием новых технологий. 4. Уполномоченный государственный орган по персональным данным определяет перечень операций по обработке, для которых требуется оценка	**Аналогичная норма отсутствует**	**Аналогичная норма отсутствует**	**Статья 35. Оценка воздействия на защиту персональных данных** **1.** Если какой-либо вид обработки, в особенности с использованием новых технологий, с точки зрения своей природы, масштаба, контекста и цели, ожидаемо приведет к высокому риску для прав и свобод физических лиц, контролёр перед обработкой должен провести оценку воздействия планируемых операций обработки на защиту персональных данных. Применительно к набору схожих операций обработки данных, которые представляют схожий высокий риск, может быть проведена единая оценка. **2.** При проведении оценки воздействия на защиту персональных данных, контролёр должен проконсультироваться с инспектором по защите персональных данных, если тот был назначен. 3. Оценка воздействия на защиту персональных данных, указанная в параграфе 1, требуется, в частности, в случае: (а) систематической и комплексной оценки определенных личных аспектов физических лиц, которая основана на автоматизированной обработке, в том числе профилировании, и является основанием для решений, порождающих правовые последствия для физического лица или схожим образом существенно влияющих на

	воздействия на защиту персональных данных, а также перечень операций по обработке, для которых оценка воздействия на защиту данных не требуется. 5. Оценка воздействия на защиту персональных данных должна включать в себя: 1) системное описание планируемых операций по обработке, а также целей обработки; 2) оценку необходимости и пропорциональности операций по обработке, а также достаточности или избыточности персональных данных в отношении целей; 3) оценку рисков для прав и свобод субъектов персональных данных; 4) меры, запланированные для устранения рисков, включая гарантии, меры безопасности и механизмы для обеспечения защиты персональных данных с учетом прав и интересов субъектов данных и других заинтересованных лиц. 6. В процессе оценки рисков владелец записей должен учесть мнения субъектов персональных данных из соответствующей целевой аудитории по поводу запланированной обработки их персональных данных, если это не повлечет ущерб для защиты коммерческих или общественных интересов или безопасности операций по обработке персональных данных. 7. В случае необходимости, в том числе при изменении набора операций или перечней персональных данных, владелец записей должен осуществить			физическое лицо; **(b)** крупномасштабной обработки особых категорий персональных данных, указанных в статье 9(1), или персональных данных, относящихся к судимостям и правонарушениям, приведенных в статье 10. **(c)** систематического мониторинга общедос тупных мест в крупных масштабах. **4.** Надзорный орган должен установить и обнародовать список видов операций по обработке, для которых требуется оценка воздействия на защиту персональных данных в соответствии с параграфом 1. Надзорный орган должен предоставить данные списки Европейскому совету по защите персональных данных, о котором говорится в ст. 68. **5.** Надзорный орган может также установить и обнародовать список видов операций по обработке, для которых оценка воздействия на защиту данных не требуется. Надзорный орган должен предоставить данные списки Европейскому совету по защите персональных данных. **6.** До утверждения списков, упомянутых в параграфах 4 и 5, компетентный надзорный орган должен применить механизм согласованности, указанный в статье 63, если указанные списки включают деятельность по обработке, связанную с предложением товаров или услуг субъектам данных, или с мониторингом их поведения в нескольких государствах-членах, или могут существенно сказаться на свободном движении персональных данных внутри Союза.

	пересмотр оценки воздействия, чтобы определить, выполняется ли обработка в соответствии с оценкой воздействия на защиту персональных данных.			**7.** Оценка должна включать в себя, по меньшей мере: **(a)** системное описание планируемых операций по обработке, а также целей обработки, в том числе, в соответствующих случаях – легитимного интереса, преследуемого контролёром; **(b)** оценку необходимости и пропорциональности операций по обработке в отношении целей; **(c)** оценку рисков для прав и свобод субъектов данных, о которых идет речь в параграфе 1; и **(d)** меры, запланированные для устранения рисков, включая гарантии, меры безопасности и механизмы для обеспечения защиты персональных данных и для подтверждения соблюдения данного Регламента с учетом прав и легитимный интересов субъектов данных и других заинтересованных лиц. **9.** В соответствующих случаях контролёр должен узнавать мнения субъектов данных или их представителей по поводу запланированной обработки, без ущерба для защиты коммерческих или общественных интересов или безопасности операций по обработке. 11. В случае необходимости, и как минимум, когда изменяется риск, сопряженный с операциями по обработке, контролёр должен осуществить пересмотр, чтобы определить, выполняется ли обработка в соответствии с оценкой воздействия на защиту персональных данных.
	Ст. 38. Назначение ответственного лица по защите персональных данных 1. Владелец записей и обработчик,	**Ст. 25. Права и обязанности собственника и (или)**	**Статья 22.1. Лица, ответственные за организацию обработки персональных**	**Статья 37. Назначение инспектора по защите персональных данных** 1. Контролёр и процессор должны

Наличие ответственного лица по защите персональных данных	назначают ответственное лицо по защите персональных данных если имеется хотя бы один из следующих фактов: 1) обработка осуществляется государственным органом, органом местного самоуправления или их подведомственными организациями; 2) деятельность владельца записей или обработчика непосредственно заключается в осуществлении операций по обработке данных на постоянной основе, которые в силу своего характера, объема и/или целей, требуют регулярного и систематического мониторинга субъектов персональных данных в количестве, превышающем пять тысяч субъектов персональных данных; 3) основная деятельность владельца записей или обработчика заключается в обработке специальных категорий персональных данных. 2. Лицо, ответственное за защиту персональных данных может быть отдельно определенным сотрудником владельца записей, обработчика, данные функции могут быть закреплены за подразделением, в таком случае непосредственная ответственность за принятые решения в качестве ответственного лица по защите персональных данных возлагается на руководителя данного подразделения. 3. Ответственным лицом по защите персональных данных может выступать отдельное юридическое или физическое лицо, которое по договору с владельцем записей и/или обработчиком определено в качестве ответственного лица по	**оператора, лица, ответственного за организацию обработки персональных данных** 3. Лицо, ответственное за организацию обработки персональных данных, обязано: 1) осуществлять внутренний контроль за соблюдением собственником и (или) оператором и его работниками законодательства Республики Казахстан о персональных данных и их защите, в том числе требований к защите персональных данных; 2) доводить до сведения работников собственника и (или) оператора положения законодательства Республики Казахстан о персональных данных и их защите по вопросам обработки персональных данных, требования к защите персональных данных; 3) осуществлять контроль за приемом и обработкой обращений субъектов или их законных представителей.	**данных в организациях** 1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных. 2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему. 3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона. 4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано: 1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных; 2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите	назначить инспектора по защите персональных данных в любом из следующих случаев: (a) обработка осуществляется государственным органом или учреждением, за исключением судов при осуществлении правосудия; (b) основная деятельность контролёра или процессора с остоит из операций по обработке данных, которые в силу своего характера, объема и/или целей, требуют регулярного и систематического мониторинга субъектов данных в больших масштабах; или (c) основная деятельность контролёра или процессора за ключается в обработке специальных категорий данных в больших масштабах согласно статье 9 и персональных данных, касающихся судимостей и правонарушений согласно статье 10. 2. Группа компаний может назначить единого инспектора по защите персональных данных при условии, что инспектор по защите персональных данных легко доступен из каждой организационной единицы. **6.** Инспектор по защите персональных данных может являться сотрудником контролёра или процессора, либо выполнять задачи на основе договора об оказании услуг. **7.** Контролёр или процессор публикует контактные данные инспектора по защите персональных данных и сообщает их надзорному органу.

	защите персональных данных. 4. Лицо, выступающее в качестве ответственного за защиту персональных данных для осуществления своей деятельности, проходит аккредитацию в Уполномоченном государственном органе по персональным данным.		персональных данных; 3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.	