



Идораи ҳуқуқи Инсон
ва Риояи Қонуният
Bureau of Human Rights
and Rule of Law
Бюро по правам человека
и соблюдению законности

АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ ТАДЖИКИСТАН О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАнных



Душанбе, 2021 г.

ББК: 67,91

Ч: К-17

Настоящий анализ предназначен для граждан Республики Таджикистан.

Данная публикация разработана в рамках проекта «Защита персональных данных в Республике Таджикистан», реализуемого ОО «Бюро по правам человека и соблюдению законности».

Составитель: Тамар Калдани

Тираж: 200 экземпляров

Для бесплатного распространения

Душанбе, 2021 г.

Содержание

Анализ законодательства Республики Таджикистан о защите персональных данных.....	3
Вступление.....	3
Краткая информация о структуре документа	5
1. Ключевые определения	6
2. Сфера действия	9
3. Принципы обработки данных	11
4. Правовые основы для обработки данных.....	12
5. Обязанности контролера и процессора.....	15
6. Права субъекта данных.....	17
7. Трансграничная передача	19
8. Полномочия государственного органа по защите персональных данных.....	20
9. Правоприменение.....	23
Основные выводы	24

Анализ законодательства Республики Таджикистан о защите персональных данных

Вступление

Статья 23 Конституции от 6 ноября 1994 года является основополагающим положением для защиты частной жизни и персональных данных в Республике Таджикистан. Согласно этой статье “Обеспечивается тайна переписки, телефонных переговоров, телеграфных и иных личных сообщений за исключением случаев, предусмотренных законом. Сбор, хранение, использование и распространение сведений о личной жизни человека без его на то согласия запрещаются.”

До 2018 года вопросы защиты персональных данных в стране косвенно и фрагментально регулировались различными законами, в том числе законом о почтовой связи от 01 августа 2003 года, о защите информации от 02 декабря 2002 года, постановлением Правительства от 8 июня 2017 года о порядке хранения и уничтожения электронных документов, а также права и обязанности ответственных лиц. Уголовный кодекс от 21 мая 1998 года предусматривает уголовную ответственность за различные правонарушения, связанные с информацией, хранящейся в компьютерных системах; а Кодекс об административных правонарушениях от 31 декабря 2008 года предусматривает административную ответственность за непринятие мер, обес-

печивающих безопасность хранения и обработки информации в учреждениях и организациях независимо от формы собственности.

3 августа 2018 года был принят Закон о защите персональных данных (далее - закон РТ), который определяет правовые и организационные основы деятельности, связанные со сбором, обработкой и защитой персональных данных. Следует отметить, что принятие закона совпало по времени со вступлением в силу Общего регламента Европейского Союза о защите данных (GDPR) и модернизацией Конвенции 108 Совета Европы, которая до сих пор является единственным обязательным международным договором, имеющим глобальное значение. Из-за экстерриториальной сферы действия GDPR, экономического интереса к рынку ЕС и новых правил трансграничных потоков данных из ЕС многие страны, не входящие в ЕС, включили нововведения GDPR в свое законодательство или в настоящее время обновляют законодательство для обеспечения совместимости с GDPR.

В целом Закон РТ является прогрессивным и содержит множество положений, касающихся принципов и условий обработки данных, прав субъектов данных и трансграничных потоков данных, которые соответствуют международным и европейским стандартам защиты данных. Поэтому принятие закона, который также предусматривает создание надзорного органа, безусловно, является важным и позитивным событием. Тем не менее, в современном мире, где обработка персональных данных связана с множеством

рисков, связанных с использованием новых информационных и коммуникационных технологий, очень важно обеспечить защиту прав субъектов данных. Поэтому интересно проанализировать соответствие национального законодательства с европейскими и международными стандартами и изучить возможности дальнейшего совершенствования законодательства и его эффективного применения на практике.

Краткая информация о структуре документа

В этом документе проводится сравнение трех законодательных актов по следующим ключевым положениям:

1. Ключевые определения
2. Сфера действия Закона
3. Принципы обработки данных
4. Правовые основы для обработки данных
5. Обязанности контролера и процессора
6. Права субъекта данных
7. Трансграничная передача
8. Полномочия государственного органа по защите персональных данных
9. Правоприменение

Каждая тема включает соответствующие статьи и разделы из трех законодательных актов. В каждом разделе предлагается анализ сходства и различия между с одной стороны, Законом РТ о защите персональных

данных и с другой стороны GDPR и модернизированной конвенцией 108. Соответствие и согласованность оценивается следующим образом:

Соответствует	<ul style="list-style-type: none">• GDPR, Конвенция 108 + и Закон РТ во многом схожи по сути и сфере применения.
Частично Соответствует	<ul style="list-style-type: none">• GDPR, Конвенция 108 + и Закон РТ имеют несколько различий.
Не соответствует	<ul style="list-style-type: none">• GDPR, Конвенция 108 + и Закон РТ во многом отличаются.

1. Ключевые определения

Закон РТ	GDPR	Конвенция 108+
Статья 2	Статья 4	Статья 2

Основные сходства

Определение терминов “сбор персональных данных”, “уничтожение персональных данных”, “база персональных данных”, “оператор базы данных”, “обработка

персональных данных”, “распространение персональных данных”, “субъект персональных данных”, “третье лицо”, “трансграничная передача персональных данных” соответствует международно признанным определениям. Что касается термина “обезличивание” оно больше отражает суть “псевдонимизации”.

Основные отличия

- Определение персональных данных не полностью отражает элементы его аналога в правовых документах ЕС или Совета Европы. В Законе РТ персональные данные определяются как сведения о фактах, событиях и обстоятельствах жизни субъекта персональных данных, позволяющие идентифицировать его личность, так как согласно GDPR Персональные данные — это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. GDPR также поясняет, что идентифицируемое физическое лицо — это лицо, которое можно прямо или косвенно идентифицировать, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор или один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица. Такое определение персональных данных особенно важно в эпоху технологических достижений и новых возможностей идентификации людей с

помощью онлайн-идентификаторов, таких как IP-адрес или “cookie” файлов.

- Некоторые различия также могут наблюдаться в определении биометрических данных. Согласно Закону РТ биометрические персональные данные – это данные, определяющие физиологические и биологические особенности субъекта. Наряду с вышеупомянутыми элементами GDPR также упоминает поведенческие черты субъекта, которые позволяют произвести однозначную идентификацию физического лица. Кроме этого GDPR четко определяет, что биометрическими являются данные, полученные в результате специальной технической обработки и приводит примеры биометрических данных - изображение лица или дактилоскопические данные. Такие определения гарантируют, что к биометрическим данным не будут отнесены, например, все фото или видео с изображениями людей, но только тех, которые в результате специальной технической обработки, позволяют однозначную идентификацию физического лица.
- Что касается определения “обладатель”, согласно закону РТ, это государственный орган, физическое и юридическое лицо, имеющие в соответствии с законодательством Республики Таджикистан право владения, пользования, распоряжения базой данных. GDPR имеет более широкий подход и наряду с полномочиями обработки, определенными законодательством, он признает контролёром любое физическое

или юридическое лицо государственного органа и учреждения, которое самостоятельно или совместно с другими определяет цели и средства обработки персональных данных. Такое определение очень важно, особенно в случаях нарушения закона, когда важно определить, кто несет ответственность и кто на самом деле принял решение об обработке персональных данных.

2. Сфера действия

Закон РТ	GDPR	Конвенция 108+
Статья 3	Статьи 3, 4(1)	Статья 3

Основные сходства

- GDPR и Конвенция применяются к обработке персональных данных, осуществляемой полностью или частично с помощью автоматизированных средств, а также к неавтоматизированной обработке персональных данных, формирующих часть системы данных, либо предназначенных, чтобы стать частью системы данных. Поскольку Закон РТ не указывает, какой тип обработки он охватывает, это означает, что он применяется как к автоматизированной, так и к неавтоматизированной обработке данных.

- Аналогично GDPR и Конвенции, действие Закона РТ не распространяется на обработку и защиту персональных данных субъектами исключительно для личных и семейных нужд.
- Что касается исключения, связанного с обработкой персональных данных и документов, содержащихся в национальном архиве и других архивах, в соответствии с законодательством РТ, Конвенция предусматривает возможность ограничения прозрачности обработки и прав субъектов данных для целей архивирования, если это предусмотрено законом и если нет явного риска нарушения прав и основных свобод субъектов данных.

Основные отличия

- GDPR и Конвенция 108+ применяются к обработке данных как в государственном, так и в частном секторе, в то время как Закон РТ исключает применение закона на обработку и защиту персональных данных, отнесённых в соответствии с законодательством Республики Таджикистан к государственным секретам.
- В отличие от GDPR, Закон не содержит конкретных положений об экстерриториальной сфере его применения. GDPR применяется к обработке персональных данных в контексте деятельности организационной единицы контролёра или процессора в Союзе, независимо от того, производится обработка в Союзе или нет.

GDPR также применяется к обработке персональных данных субъектов, находящихся в Союзе, контролёром или процессором, не имеющими организационной единицы в Союзе, если процессы обработки данных касаются: (а) предложения товаров и услуг субъектам данных, находящимся в Союзе, независимо от того, требуется ли от них оплата, или нет, либо (б) мониторинга их поведения, если такое поведение происходит в Союзе. Хотя внешнее применение национальных законов не всегда возможно, многие страны, недавно обновившие законы, четко заявляют, что их законы применяются к обработке персональных данных, осуществляемой на их территории, а также к обработке, осуществляемой за пределами их территории если обработка касается лиц, находящихся под юрисдикцией этой республики.

- GDPR не применяется к анонимным данным, если данные больше не могут идентифицировать субъект данных. Подобного положения нет в Законе РТ.

3. Принципы обработки данных

Закон РТ	GDPR	Конвенция 108+
Статьи 4, 5 и 14	Статья 5	Статья 5

Основные сходства

Что касается принципов обработки данных, закон РТ в значительной степени соответствует международным стандартам, он содержит принципы законности, справедливости, прозрачности, минимизации и соразмерности, ограничения цели, точности данных, безопасности данных, ограничения хранения данных. Единственный принцип, который мог бы укрепить закон, - это принцип подотчетности. Более того, постановлением Правительства от 8 июня 2017 года определяется Порядок хранения и уничтожения электронных документов, а также права и обязанности ответственных лиц. Закон об оперативно-розыскной деятельности также определяет срок хранения в течение шести месяцев и правила уничтожения материалов, полученных в результате проведения оперативно-розыскных мероприятий в отношении лиц, виновность которых в совершении преступления не доказана. В том же законе сказано, что фонограммы и другие материалы, полученные в результате прослушивания телефонных разговоров и иных переговоров лиц, в отношении которых не было возбуждено уголовное дело, уничтожаются в течение шести месяцев с момента прекращения прослушивания.

4. Правовые основы для обработки данных

Закон РТ	GDPR	Конвенция 108+
-----------------	-------------	---------------------------

Основные сходства

Осмотрительный подход закона РТ к Распространению персональных данных, а также особые правила, касающиеся биометрических данных и указания конкретных оснований для их обработки, соответствуют подходам Конвенции 108+ и GDPR.

Основные отличия

- Согласно Закону РТ Сбор и обработка персональных данных осуществляются при наличии сертификата соответствия уполномоченного государственного органа по защите персональных данных и информационной безопасности. GDPR имеет более другой подход к сертификации. Это не предварительное условие обработки данных, а, скорее, механизм предназначенный для демонстрации соблюдения GDPR. При механизме сертификации во внимание принимаются особые потребности малых и средних предприятий.
- Согласно Закону РТ основным правовым основанием для обработки данных является согласие субъекта или его законного представителя. Субъект или его законный представитель не может отозвать согласие на сбор и обработку персональных данных в случаях, предусмотренных

статьёй 9 настоящего Закона. Это означает, что данные, содержащиеся в общедоступных ресурсах, в том числе в электронных информационных ресурсах, находятся вне контроля субъекта данных.

- Законодательство ЕС и Совета Европы в области защиты персональных данных устанавливает очень четкие условия для того, чтобы согласие было действительным - оно должно быть свободным, конкретным, информированным и недвусмысленным. Закон РТ не перечисляет элементы и условия для получения согласия и делает ссылку на то, что это определяется законодательством Республики Таджикистан.
- Кроме согласия, закон ссылается только на два других правовых оснований для обработки данных – а) выполнение государственными органами функций, предусмотренных законодательством Республики Таджикистан; б) защита конституционных прав и свобод человека и гражданина. Последнее основание может иметь очень широкое толкование, поэтому очень важно установить ограничения и надлежащий надзор за возможным злоупотреблением этим основанием. В отличие от закона РТ, GDPR содержит более длинный список возможных правовых оснований для обработки данных – например, обработка данных, необходимая для осуществления контакта с субъектом, для защиты жизненно важных интересов субъекта или возвышенных законных интересов контролёров или третьих

лиц. Эти правовые основания имеют большое практическое применение и ограничивают риски чрезмерного или неправильного использования согласия.

- В отличие от Закона РТ, GDPR и Конвенция 108+ определяют специальные категории данных и обеспечивают гарантии их защиты. К таким данным относятся данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, членство профессионального союза, генетические данные, биометрические данные, а также данные, касающиеся здоровья, половой жизни или сексуальной ориентации физического лица, правонарушений, уголовных разбирательств и обвинительных приговоров, а также соответствующих мер безопасности.

5. Обязанности контролера и процессора

Закон РТ	GDPR	Конвенция 108+
Статьи 5, 13, 21, 24-25	Статьи 24-36	Статьи 7-8 и 10

Основные сходства

- Обязательства по обеспечению безопасности, охраны и конфиденциальности персональных

данных, определенные Законом РТ, соответствуют обязательствам, определенным европейскими законодательными актами.

- Статья 21 закона РТ об уведомлении о передаче персональных данных также содержит прогрессивные положения и короткий период времени (3 дня) для предоставления информации субъекту данных.
- Владелец и оператор также должны утверждать перечень персональных данных, необходимых и достаточных для выполнения осуществляемых ими задач, что частично отражает обязательства, предусмотренные GDPR по ведению учета операций по обработке.
- Прогрессивное также положение, обязывающее владельца и оператора представлять доказательства о получении согласия субъекта на сбор и обработку его персональных данных.

Основные отличия

Наряду с вышеупомянутыми обязательствами GDPR и Конвенция 108+ устанавливают дополнительные обязательства, связанные с применением принципами конфиденциальности по дизайну и конфиденциальности по умолчанию, уведомление надзорного органа и субъекта данных о нарушении безопасности персональных данных, оценки воздействия планируемых операций обработки на защиту персональных данных, назначением офицера по защите персональных данных. Эти новинки являются мощным инструментом для обеспечения безопасности данных, повышения ответственности контролеров и минимизации рисков,

связанных с обработкой данных. Многие государства за пределами ЕС уже ввели или планируют внести эти нововведения в свое законодательство.

6. Права субъекта данных

Закон РТ	GDPR	Конвенция 108+
Статьи 10, 15, 22-23	Статьи 12-23	Статьи 8-9

Основные сходства

- Закон РТ предусматривает основные права субъекта данных, предусмотренные Конвенцией 108+ и GDPR, в том числе право на доступ к персональным данным, право на изменение, дополнение, уточнение его персональных данных, право подтверждения факта сбора и обработки и на получение информации, касающейся сбора и обработки его персональных данных. Закон РТ также предусматривает право субъекта требовать блокирования или уничтожения его персональных данных, в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством Республики Таджикистан меры по защите своих прав.

- Закон РТ о защите персональных данных не определяет конкретных оснований и условий для ограничения прав субъектов данных и по этому поводу ссылается на законодательство Республики Таджикистан, вероятно, включая закон „О праве на доступ к информации“.
- В соответствии с законом об оперативно-розыскной деятельности лицо, виновность которого в совершении преступления не доказана, то есть в отношении которого в возбуждении уголовного дела отказано, либо уголовное дело прекращено, и которое располагает фактами проведения в отношении его оперативно-розыскных мероприятий, вправе истребовать от органа, осуществляющего оперативно-розыскную деятельность, сведения о полученной о нем информации в пределах, допускаемых требованиями конспирации и исключающих возможность разглашения государственных секретов. В случае отказа, лицо вправе подать жалобу в суд.

Основные отличия

В дополнение к вышеупомянутым правам Конвенция 108+ и GDPR также гарантируют новые права субъектов, которые имеют особое значение в современном мире, где все чаще используются технологии искусственного интеллекта, распознавания лиц, профилирования, наблюдения и отслеживания. Новое поколение прав включает:

- право на знание мотивов, лежащих в основе обработки данных, когда результаты такой обработки применяются к субъекту.
- право не подвергаться решению, которое основано исключительно на автоматизированной обработке, в том числе профилировании, и требовать человеческого вмешательства со стороны контролёра, выражать свою позицию, а также оспаривать это решение.
- право на переносимость данных.
- право на получение помощи со стороны надзорного органа, независимо от его национальности или места жительства.

Как обычно, в законах о защите данных не принято устанавливать обязательства субъекта, как это предусмотрено статьей 23 Закона РТ. Конечно, это не означает, что соответствующие законы не могут устанавливать случаи и условия, при которых предоставление информации или документов необходимо - например, в случаях оперативно-розыскных мероприятий, таких как оперативный опрос, наведение справок и т.д.

7. Трансграничная передача

Закон РТ	GDPR	Конвенция 108+
Статья 18	Статьи 44-50	Статья 14

Основные сходства

В основном положения, относящиеся к трансграничным потокам данных, соответствуют Конвенции 108+, GDPR и законам многих других стран. Ограничения на трансграничный поток в целях защиты основ конституционного строя Республики Таджикистан, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства также соответствуют исключениям, установленным конвенцией.

8. Полномочия государственного органа по защите персональных данных

Закон РТ	GDPR	Конвенция 108+
Статьи 6-7	Статьи 51-59	Статья 15

Основные сходства

Роль надзорных органов по защите данных во всем мире возрастает. Конвенция Совета Европы 108+ и Регламент Европейского Союза (GDPR) укрепляют полномочия и сотрудничество надзорных органов. Важен тот факт, что Закон РТ предусматривает полномочия Президента Республики Таджикистан по утверждению нормативных правовых актов по защите персональных данных и определению уполномоченного государственного органа по защите персональных

данных. Закон также перечисляет основные полномочия государственного органа, которые в значительной степени отражают полномочия и функции надзорного органа, определенные GDPR и Конвенцией, а именно: утверждение порядка осуществления обладателем, оператором и третьим лицом мер по защите персональных данных; рассмотрение обращений физических и юридических лиц по вопросам защиты персональных данных; определение списка ответственных лиц за соблюдение законодательства Республики Таджикистан о защите персональных данных и принятие мер по привлечению их к ответственности.

Основные отличия

- Законодательство ЕС и Совета Европы рассматривает существование независимых надзорных органов как необходимое условие для эффективной защиты прав субъектов данных и обеспечение эффективного соблюдения законодательства о защите данных. Независимость надзорного органа, его членов и сотрудников от прямого или косвенного внешнего влияния имеет основополагающее значение для гарантии полной объективности при принятии решений. Не только закон, лежащий в основе создания надзорного органа, должен содержать положения, гарантирующие независимость, но и организационная структура органа тоже должна демонстрировать независимость.
- Европейские надзорные органы обладают следственными и исправительными полномочиями.

В соответствии со статьей 15 Модернизированной Конвенции 108 полномочия надзорных органов включают расследование и вмешательство, а также полномочия принимать решения и налагать административные санкции в отношении нарушений положений Конвенции, участвовать в судебных разбирательствах.

- Надзорные органы также обладают компетенцией рассматривать запросы и жалобы, поданные субъектами, повышать осведомленность общественности о законе о защите данных и давать рекомендации парламенту и правительству относительно любых законодательных или административных мер, которые предусматривают обработку персональных данных.
- Наряду с компетенциями надзорный орган должен иметь в законе механизмы для эффективного выполнения своих задач, например: должен иметь доступ ко всем данным и к информации, а также к любым помещениям, в которых хранится соответствующая информация. Контролёры обязаны сотрудничать с надзорными органами и предоставлять необходимую информацию или уведомления.
- Модернизированная Конвенция 108 также затрагивает вопрос сотрудничества и взаимопомощи между надзорными органами разных стран. Надзорные органы должны координировать свои расследования, проводить совместные действия и предоставлять друг другу информацию и документацию о своих законах и

административных практиках, касающихся защиты данных.

9. Правоприменение

Закон РТ	GDPR	Конвенция 108+
Статьи	Статьи	Статьи

Основные отличия

Для обеспечения защиты данных, одного принятия правовых инструментов может оказаться недостаточно. Для эффективного применения законодательства важно, чтобы надзорные органы имели право применять эффективные сдерживающие и соразмерные нарушению санкции. Согласно Модернизированной Конвенции 108, национальное законодательство должно устанавливать соответствующие средства правовой защиты и санкции против нарушений права на защиту данных. В Евросоюзе надзорные органы имеют право налагать административные штрафы за нарушение правил в размере до 20 млн. евро или, в случае предприятия, 4% от общего годового оборота - в зависимости от того, какая сумма больше.

В законе РТ, а также в Кодексе об административных правонарушениях нет положений, определяющих санкции за нарушение закона о защите персональных данных.

Основные выводы

Как сказано во введении, в целом Закон РТ является прогрессивным и его принятие безусловно положительный шаг для обеспечения лучшей защиты прав субъектов и баланса между интересами владельцев / обработчиков данных и субъектов данных. Тем не менее, как показывает анализ, существует множество возможностей для улучшения закона, приведения его в соответствие с современными международными стандартами и обеспечения механизмов практического применения закона. Наряду с размышлениями об улучшении положений закона, не менее важны повышение осведомленности общественности о правах, которые гарантирует этот закон, а также осведомленности владельцев / обработчиков данных об их обязанностях. Работа уполномоченного государственного органа также прояснит те области, в которых защита персональных данных является наиболее актуальной.

Органы по защите данных и неправительственные организации являются естественными союзниками, когда дело доходит до практического применения принципов защиты данных, расширения возможностей людей отстаивать свои права и привлечения контролёров данных к ответственности за свои действия. Организации гражданского общества могут внести свой вклад в разработку нормативных актов, которые могут вводить в действие положения закона. Они могут повышать актуальность вопросов защиты персональных данных с помощью обучения, кампаниями адвокации и исследовательской деятельности.