

**Исследование по персональным данным в коммерческом секторе  
Кыргызской Республики**

Исследователи: Нурбек Арзымбаев, Талант Султанов,  
Айпери Бозоева, Жазгуль Зуридинова

## Содержание

<b>1. Аббревиатуры</b>	<b>4</b>
<b>2. Термины</b>	<b>5</b>
<b>3. Резюме</b>	<b>6</b>
<b>4. Введение</b>	<b>8</b>
<b>5. Опыт других стран</b>	<b>9</b>
5.1    Краткая история регулирования ПД в европейских странах и их подход	9
5.2    США	13
5.3    Китай	14
5.4    Россия	15
5.5    Казахстан	15
<b>6. Ситуация с персональными данными в Кыргызской Республике</b>	<b>17</b>
6.1    Утечки персональных данных в Кыргызской Республике	20
<b>7. Сбор данных</b>	<b>22</b>
7.1    Методология	22
7.1.1    Сектор «Строительство»	23
7.1.2    Сектор «Промышленность»	24
7.1.3    Сектор «Сельское хозяйство»	24
7.1.4    Сектор «Услуги»	24
<b>8. Анализ данных</b>	<b>26</b>
8.1    Политика по обработке персональных данных	26
8.2    Сектор «Строительство»	29
8.3    Сектор «Промышленность»	29
8.4    Сектор «Сельское хозяйство»	29
8.5    Сектор «Услуги»	29
<b>9. Рекомендации</b>	<b>33</b>
9.1    Общие рекомендации	33
9.2    Независимый уполномоченный орган по защите персональных данных	34
9.3    Законодательство	35
9.4    Рекомендации по разработке политики по обработке ПД	36
<b>10. Приложения</b>	<b>39</b>
Приложение А. Список организаций, попавших в выборку	39
Приложение Б. Анализ Политик по защите персональных данных	46
Приложение В. Сравнение фактически собираемых данных и Политики	47
Приложение Г. Критерии независимости уполномоченного органа	49

Выражаем огромную благодарность Фонду «Сорос-Кыргызстан» (ФСК) за возможность проведения данного исследования. Также мы хотим поблагодарить директора Информационной программы Лиру Самыкбаеву и координатора Информационной программы Мээрим Токочеву за оказанную всестороннюю поддержку. А также благодарим Ирину Байкулову и Анну Гусарову за ценные комментарии и рецензии.

Отчет создан в рамках проекта «Мои цифровые права», реализуемого ОФ «Кыргызское отделение интернет-общества ISOC Kyrgyzstan Chapter» при поддержке Фонда «Сорос-Кыргызстан». Данный материал доступен для свободного копирования, переработки и распространения на любом носителе и в любом формате с обязательным указанием имени автора, для любых целей, включая коммерческие. Содержание видеоролика является предметом ответственности «Кыргызского отделения интернет-общества ISOC Kyrgyzstan Chapter». Мнения, выраженные в материале, необязательно отражают точку зрения Фонда «Сорос-Кыргызстан».



*Данная лицензия позволяет третьим лицам свободно распространять, создавать производные (ремиксы, переводы), перерабатывать, адаптировать, в том числе и в коммерческих целях, весь материал или любые его части с обязательной ссылкой на авторов.*

## 1. Аббревиатуры

ЕАЭС – Евразийский экономический союз.

КР – Кыргызская Республика.

МЭП КР – Министерство энергетики и промышленности Кыргызской Республики.

МЭФ КР – Министерство экономики и финансов Кыргызской Республики.

ПД – Персональные данные.

РК – Республика Казахстан.

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ.

РФ – Российская Федерация.

СНГ – Содружество Независимых Государств.

США – Соединенные Штаты Америки.

ФСБ – Федеральная служба безопасности РФ.

ФСТЭК – Федеральная служба по техническому и экспортному контролю РФ;

ЮНКТАД – Конференция ООН по торговле и развитию.

ССРА – Закон о конфиденциальности потребителей в штате Калифорния.

GDPR – Генеральный регламент по защите персональных данных, регулирование ПД в Европейском союзе.

## 2. Термины

**Информация персонального характера (персональные данные)** – зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном положении, финансовом положении, состоянии здоровья и прочее.

**Непосредственно предоставляемые персональные данные** – персональные данные, предоставленные гражданами путем ввода в соответствующие формы.

**Косвенно предоставляемые персональные данные** – данные, с помощью которых компании могут идентифицировать граждан. Данные, связанные с cookie-файлами, IP-адрес, данные о геолокации и другие могут быть примерами косвенно предоставляемых данных.

**Субъект персональных данных** – физическое лицо, к которому относятся соответствующие персональные данные.

**Согласие субъекта персональных данных** – выраженное в форме, предусмотренной Законом «Об информации персонального характера КР», свободное, конкретное, безоговорочное и осознанное волеизъявление лица, в соответствии с которым субъект оповещает о своем согласии на осуществление процедур, связанных с обработкой его персональных данных.

**Уполномоченный государственный орган** – государственный орган, который должен быть определен правительством Кыргызской Республики для осуществления функции и полномочия по обеспечению соответствия обработки персональных данных требованиям законодательства КР.

**Электронная подпись** – информация в электронной форме, которая присоединена к другой информации в электронной форме и (или) логически связана с ней и которая используется для определения лица, от имени которого подписана информация.

**Простая электронная подпись** – представляет собой комбинацию кодов, паролей и иных идентификаторов, которые подтверждают, что электронное сообщение отправлено конкретным лицом.

**Трансграничная передача персональных данных** – передача держателем (обладателем) персональных данных держателям, находящимся под юрисдикцией других государств.

### 3. Резюме

Главной задачей исследования было выяснить, как «рынок», коммерческий<sup>1</sup> сектор в Кыргызской Республике обеспечивают исполнение законодательства при сборе и обработке персональных данных, непосредственно предоставленных пользователями<sup>2</sup>, в условиях отсутствия органа, контролирующего исполнение законодательства.

По результатам нашего исследования мы можем утверждать, что подавляющее большинство изученных нами компаний нелегитимно собирают персональные данные, не ознакомливают пользователей о перечне собираемых персональных данных, целях их сбора и обработки, их правах, сроках хранения и об их защите.

Из просмотренных нами более 500 веб-сайтов компаний около 180 непосредственно собирают персональные данные (далее ПД) от пользователей. Подавляющее большинство собирают контактные данные пользователей для обратной связи и отправки информации об акциях и продукции компании.

Из 180 собирающих ПД только 44 компании получают согласие. Однако, по данным нашего исследования, абсолютное большинство онлайн-форм получения согласия по обработке персональных данных не соответствуют законодательству по персональным данным КР. По действующему законодательству, отсутствуют нормы дачи электронного согласия на сбор и обработку ПД, кроме использования электронной подписи. Несмотря на то, что в законе имеется более упрощенная форма – «простая электронная подпись», из просмотренного количества лишь единичные веб-ресурсы используют ее для получения согласия на сбор и обработку ПД.

Из 180 веб-сайтов, которые запрашивали ПД, более 40 % веб-сайтов находились за пределами страны. При этом только шесть компаний в форме согласия отображали пункты о трансграничной передаче данных.

Из 519 веб-сайтов только 17 (или 3 %) опубликовали на веб-сайтах Политику по обработке персональных данных<sup>3</sup>. Соответственно, они не ознакомливают пользователей с целями сбора ПД, условиями их обработки, хранения, уничтожения, правами и другими важными аспектами, связанными с ПД. Также необходимо отметить, что только одна компания из 519 разработала и опубликовала Политику обработки данных на кыргызском языке.

Достаточно сложно сделать однозначные выводы об объемах и чрезмерности собираемых данных из-за отсутствия целей сбора, опубликованных компаниями. Но нами зафиксированы случаи сбора специальных категорий ПД<sup>4</sup> и сбор ПД, не соответствующих тексту получаемых согласий.

В целом можно составить портрет компаний в коммерческом секторе – компания собирает непосредственно от пользователей персональные данные только для маркетинговых

---

<sup>1</sup> Вопрос сбора и обработки данных государственным сектором требует отдельного исследования.

<sup>2</sup> Необходимо отметить, что в исследовании мы разделяем понятия «непосредственно предоставляемые персональные данные» и «косвенно предоставляемые персональные данные». Исследование было проведено только по изучению непосредственно предоставляемых персональных данных. В последующих исследованиях мы рассмотрим косвенно предоставляемые персональные данные и отношение пользователей к ним.

<sup>3</sup> Документ, который часто также называют политикой конфиденциальности, определяет политику держателя/обработчика в отношении обработки персональных данных (далее Политика).

<sup>4</sup> В законе об информации персонального характера под специальными категориями понимаются расовое или этническое происхождение, национальная принадлежность, политические взгляды, религиозные или философские убеждения, а также данные, касающиеся состояния здоровья и сексуальных наклонностей.

рассылок, обратной связи или предоставления скидок; не получает легитимного согласия от пользователей на сбор и обработку ПД; не уведомляет пользователей о мерах, предпринимаемых для защиты ПД, о правах пользователей.

По результатам исследования можно сделать вывод, что отсутствие уполномоченного органа негативно сказывается на взаимоотношениях субъекта ПД с частным сектором. Субъекты ПД не могут реализовать свои законные права, коммерческий сектор фактически не соблюдает законодательство и другие акты по защите персональных данных страны. Также в ходе исследования, изучив законодательство страны, проверив исполнение прав субъектов ПД, проанализировав утечки ПД, мы считаем, что имеются существенные пробелы в законодательстве страны. К примеру, к основным можно отнести следующее: не четко прописаны права по отзыву согласия, сложность дачи электронного согласия (только электронная подпись), отсутствуют нормы по уведомлению об утечке, возможность отписки от маркетинговых рассылок и защиты ПД детей.

## 4. Введение

Согласно данным<sup>5</sup> ЮНКТАД, в 2020 году 124 страны из 194 приняли законы по защите персональных данных. Кыргызская Республика была одной из первых стран региона, принявшей Закон «Об информации персонального характера» в 2008 году, тем самым став лидером в Центральной Азии. Но в последние годы страна в различных рейтингах, в которых защита ПД является важным компонентом, занимает последние места<sup>6</sup> в регионе. Не только рейтинги указывают на проблемы в защите персональных данных, но и количество инцидентов, связанных с утечкой в случае неправомерного использования персональных данных граждан. Утечка фотографий из проекта «Безопасный город», массово обсуждаемых в социальных сетях в конце 2019 года, которая могла нанести гражданину ощутимый урон репутации и личной жизни, а также недавнее расследование «Азаттыка» о веб-индустрии, где имело место неправомерное использование ПД, являются яркими примерами.

Множество вопросов возникает при изучении темы защиты персональных данных в Кыргызской Республике. Но что же не так с защитой персональных данных в стране? Может, неверно выбран подход в регулировании защиты ПД? А какой подход выбрала Кыргызская Республика из двух существующих основных подходов – европейского и американского? Действительно ли отсутствие уполномоченного органа в стране сказывается на защите данных? Есть ли альтернативные варианты по защите персональных данных без уполномоченного органа? Насколько коммерческий сектор соблюдает законодательство? Какие данные собирает коммерческий сектор? Сообщают ли компании своим клиентам, какие данные, как, почему и зачем собирают? К примеру, насколько соблюдается требование получения согласия в ситуации, когда отсутствует контроль со стороны государства. Если требования законодательства не соблюдаются, возможно, недостаточно проработан закон о персональных данных или причина проблем с ПД в чем-то другом?

В данном исследовании мы постарались ответить на вышеобозначенные вопросы и предоставили свои рекомендации. Для этого мы изучили опыт других стран, основные отличия в подходах, также изучили веб-сайты компаний в Кыргызской Республике и собрали данные, которые нам помогут сделать наблюдения и ответить на эти вопросы.

---

<sup>5</sup> <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

<sup>6</sup> В отчете Cybersecurity Index 2020 Международного союза электросвязи КР среди стран СНГ опередила только Таджикистан и Туркменистан. Отчет учитывает различные аспекты кибербезопасности, включая защиту ПД – <https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/>. По другому индексу ситуация аналогичная – <https://ncsi.ega.ee/ncsi-index/?order=-ncsi>.

## 5. Опыт других стран

В данном разделе мы рассмотрим опыт европейских стран и США, так как история развития защиты персональных данных тесно связана с этими странами и регионами. Забегая вперед, ответим, что Кыргызская Республика из основных двух подходов – европейского и американского – выбрала первый. Основные отличия понятий европейского подхода – персональные данные принадлежат гражданину, для сбора и обработки необходимо получить согласие, регулирование осуществляется отдельным законом, предполагается иметь специальный уполномоченный орган. Другим альтернативным подходом являлся подход США, характеристиками которого являлось следующее: данные, собранные компаниями, принадлежат компаниям, отсутствует понятие получения согласия, регулируется секторальными законами<sup>7</sup> (за исключением некоторых штатов), отсутствует отдельный уполномоченный орган.

В данном разделе мы также рассмотрим направления развития ПД в Китае<sup>8</sup>, России и Казахстане<sup>9</sup>. Мы постарались осветить основные отличия и дать свою оценку в правильности выбранного подхода.

### 5.1 Краткая история регулирования ПД в европейских странах и их подход

Существенное развитие сферы защиты персональных данных произошло после Второй мировой войны в европейских странах. Причиной многие исследователи называют негативный опыт европейских стран, централизованные архивы и записи которых неправомерно были использованы нацистской секретной полицией. Сразу после Второй мировой войны Генеральной ассамблеей ООН была принята Всеобщая декларация прав человека в 1948 году, которая также включала право на частную жизнь. С ростом использования информационных систем в 60-70-х годах прошлого столетия множество западных стран начали принимать законы и другие акты по защите персональных данных.

Неудивительно, что первый закон о защите персональных данных появился в Земле Гессен (Hessen) в Германии в 1970 году, ведь немцы во второй раз столкнулись с практикой массовой слежки за населением в Германской Демократической Республике (ГДР). Закон регулировал автоматическую обработку персональных данных. Но на национальном уровне Швеция стала первой страной, принявшей закон о защите ПД в 1973 году. После многие европейские страны начали разрабатывать и принимать законы о защите персональных данных.

В 1980 году Организация экономического сотрудничества и развития (OECD) разработала Руководство по защите персональных данных и трансграничной передаче. Совет Европы разработал Конвенцию о защите физических лиц при автоматизированной

---

<sup>7</sup> В США имеются регулирование и защита ПД в финансовых учреждениях, телекоммуникационном секторе, здравоохранении, секторе кредитно-информационного обмена, информации о детях.

<sup>8</sup> Мы считаем, что опыт Китая необходимо рассматривать отдельно, так как он является сильным игроком в цифровой экономике, имеет общие границы с КР и, возможно, сменит в ближайшее время подход США на европейскую модель защиты ПД.

<sup>9</sup> Опыт России и Казахстана в регулировании ПД, возможно, будет интересен для нашей страны из-за партнерских отношений, членства в ЕАЭС и других тесных связей.

обработке персональных данных, которая была принята в 1981 году и ратифицирована многими странами. Конвенция и правила содержали основные принципы защиты персональных данных, такие как сбор честным и законным путем; использование ПД только для заранее указанных целей; адекватность целей; точность и актуальность ПД; доступ субъекта к своим данным; обеспечение конфиденциальности и уничтожение данных после достижения целей (Рис. 1). Данные принципы легли в основу законодательства многих стран.



Рис. 1. Принципы<sup>10</sup> OECD от 1980 г.<sup>11</sup>

Общеввропейским документом, регулирующим обработку персональных данных, стала принятая в 1995 году Директива 95/46/ЕС Европейского парламента и Совета Европы.

Общие	Уполномоченный орган
<p>Директива регулировала как автоматическую, так и ручную обработку ПД.</p> <p>Регистрация в уполномоченном органе. Держатели были обязаны уведомлять уполномоченный орган до начала обработки ПД (во многих странах это было в виде регистрации в уполномоченном органе, хотя некоторые страны не</p>	<p>Первый документ, в котором содержались обязательства по созданию отдельного уполномоченного органа по обеспечению соблюдения закона.</p> <p>Требование, чтобы уполномоченный орган был «полностью независимым», наделить его возможностью рассмотрения жалоб от частных лиц, мониторинга и исполнения</p>

<sup>10</sup> Необходимо отметить, что несмотря на схожесть принципов, количество и термины отличаются в различных документах. К примеру, Конвенция 180 (1981) выделяет 6 принципов, OECD – 8, GDPR – 7, ООН (1989) – 10.

<sup>11</sup><https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm>

требовали регистрации в случае назначения офицера по защите ПД).	закона, а также обязывал иметь навыки и достаточный опыт, необходимый для выполнения своих задач.
--	---

Таблица 1. Некоторые особенности Директивы 95/46/ЕС от 1995 г.

Однако в связи с резким развитием технологий после принятия Директивы многие исследователи утверждали, что технологии опередили регулирование, что она уже не отвечает требованиям и неэффективно защищает персональные данные.

Замена пришла только после более двадцати лет и под названием «Генеральный регламент по защите персональных данных» (далее GDPR), который был принят в 2016-м и вступил в силу в 2018 году. Регламент привнес достаточно много изменений и улучшений. К примеру, в нем отсутствуют требования по обязательному уведомлению уполномоченного органа до обработки ПД. Несмотря на то, что основные принципы считаются универсальными, в новом регулировании появился дополнительный принцип минимизации данных.

Основными<sup>12</sup> нововведениями в регламенте стали:

- экстерриториальное действие<sup>13</sup> и прямое применение;
- принципы «Защищенность по умолчанию – privacy by default»<sup>14</sup> и «Запланированная защищенность – privacy by design»<sup>15</sup>;
- уточнения про согласие. При его использовании оператор должен обеспечить, чтобы согласие было свободно данным, конкретным, информированным и недвусмысленным. В отдельных случаях оператор обязан проинформировать субъекта о рисках планируемой обработки данных и о предпринятых мерах по их смягчению;
- обязывает операторов уведомлять субъектов персональных данных и уполномоченные органы при возникновении инцидентов и утечках;
- обязанность операторов проводить оценку рисков нарушения защищенности данных (DPIA);
- максимальные штрафы за нарушение требований регламента выросли до 20 млн евро, или 4 % от годового оборота компании.

<sup>12</sup> Имеется множество нововведений, но в отчете перечислены только те, которые подпадают под фокус исследований.

<sup>13</sup> GDPR имеет экстерриториальное действие и применяется ко всем компаниям, обрабатывающим персональные данные резидентов и граждан ЕС, независимо от местонахождения такой компании. Это означает, что организации, обрабатывающие персональные данные европейцев в Кыргызстане при оказании услуг (например, банковское обслуживание, авиакомпания, гостиницы и иные), подпадают под действие GDPR и обязаны соблюдать европейские правила обработки персональных данных.

<sup>14</sup> Privacy by default – означает, что пользователю не нужно предпринимать никакие действия для защиты своей конфиденциальности. Настройки по сохранению конфиденциальности ПД установлены по умолчанию на наивысший имеющийся режим.

<sup>15</sup> Privacy by design – означает, что компания заблаговременно планирует защиту персональных данных во всех действиях, начинаниях и решениях компании.

Отдельно стоит отметить, что, согласно Статье 6 GPRR<sup>16</sup>, имеется шесть законных оснований для сбора и обработки ПД:

- A. Субъект персональных данных дал согласие на обработку своих персональных данных.
- B. Обработка необходима для исполнения договорных отношений, где субъект является стороной.
- C. Обработка необходима для выполнения юридических обязательств, возложенных на держателя ПД.
- D. Обработка необходима для защиты жизненно важных интересов субъекта или другого лица.
- E. Обработка необходима для выполнения задач, осуществляемых в государственных интересах или в рамках исполнения государственной власти в отношении держателей.
- F. Обработка необходима для целей, вытекающих из легитимных интересов, преследуемых держателем или третьим лицом, за исключением случаев, когда преимущество над такими интересами имеет интересы или фундаментальные права и свободы субъекта данных, требующие защиты персональных данных, в частности, когда субъектом данных является ребенок.

Как видно из вышеперечисленного, согласие наряду с другими является одним из оснований для сбора и обработки ПД. В GDPR отсутствуют специальные формы для предоставления согласия, а только требования к нему<sup>17</sup>, также любое однозначное и осознанное волеизъявление лица (an unambiguous indication by clear affirmative action) считается легитимным согласием. К примеру, все отметки в checkbox, нажатие ссылки и т. д.

В GDPR отсутствуют требования по так называемому data localisation – хранение данных в ЕС, но имеются требования по обеспечению защиты при трансграничной передаче данных за пределы ЕС. К примеру, существует список стран<sup>18</sup>, которые имеют адекватный уровень защиты и в которые не требуется никаких дополнительных требований.

Можно сделать следующие заключения о европейском подходе: регулирует защиту персональных данных единым отдельным законодательным актом, который регулирует как государственный, так и частный секторы; основывается на принципах, в том числе получения согласия до сбора и обработки; право на защиту персональных данных является одним из фундаментальных прав; есть независимый специальный уполномоченный орган по защите персональных данных.

---

<sup>16</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

<sup>17</sup> GDPR Article 4 ‘consent’ of the data subject means any **freely given, specific, informed** and **unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of personal data relating to him or her.

<sup>18</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

## 5.2 США

В 1974 году в США был принят нормативный акт, регулирующий автоматизированную обработку государственными органами персональных граждан. США по сей день являются страной, в которой отсутствует отдельный федеральный закон о защите персональных данных для частного сектора. Соответственно, отсутствуют многие принципы, используемые для защиты ПД в европейских странах. К примеру, не требуется получение согласия, несмотря на то что в некоторых штатах (Калифорния и Вирджиния) имеются отдельные законы, регулирующие персональные данные. Все остальные штаты в основном полагаются на секторальные законы.

	GDPR (Европа)	США	Закон CCPA (штат Калифорния)
Требуется согласие	да	нет	нет
Право доступа на свои данные	да	нет	да
Право на удаление своих данных	да	нет	да
Право на корректировку данных	да	нет	нет
Публикация политики по защите данных	да	нет	да (Privacy notice)
Отдельный уполномоченный орган	да	нет	нет
Экстерриториальное применение	да	нет	да

Таблица 2. Некоторые отличия в регулировании ПД.

Как видно из таблицы, Калифорнийский закон имеет некоторые схожести с GDPR, но из-за более мягких требований некоторые исследователи называют его «облегченной версией» GDPR (GDPR light). В законе штата Калифорния не требуется согласие на сбор и обработку ПД, отсутствует право на корректировку данных.

Также нужно отметить, что в США не существует специального уполномоченного органа, но часть функций по контролю справедливой обработки ПД возложена на Федеральную торговую комиссию. Она также следит за соблюдением акта по защите детей в Интернете (COPPA). С другой стороны, некоторые технологические гиганты, такие как

Apple<sup>19</sup>, Microsoft<sup>20</sup>, в последние годы просят власти США принять отдельный федеральный закон о защите персональных данных. Некоторые исследователи<sup>21</sup> предлагают абсолютно новые подходы исходя из реалий и истории США, например, создавать дата-трасты (Data Trusts) или союзы по защите персональных данных. Также в США отсутствуют требования по хранению данных в стране, хотя часто обсуждается запрет на хранение данных граждан в Китае. Будет ли принят федеральный закон, будет ли создан отдельный уполномоченный орган, будет ли data localisation – вопросы остаются открытыми.

### 5.3 Китай

Опыт Китая, как второй экономики мира, и имеющего общие границы с КР может представлять интерес для нашей страны. Так же как в США, в Китае не существует отдельного закона о защите данных, но аспекты защиты данных можно найти во множестве секторальных правовых актах, в Законе о защите потребителей (2014), в Законе о кибербезопасности (2017) и в Законе защиты персональных данных детей в Интернете (2019). В рамках данных актов были прописаны вопросы конфиденциальности и защиты данных, включая запреты на проведение операций обработки без согласия потребителя. Но наиболее интересным является то, что в конце 2020-го общественности был представлен на обсуждение новый закон, регулирующий персональные данные (PIPL 2020). Некоторые эксперты оценили данный проект закона как движение в сторону европейского подхода, так как многие аспекты схожи с GDPR. К примеру, детально прописаны права субъекта персональных данных, согласие является законным основанием для сбора и обработки и другие принципы. Так же как GDPR и CCPA, новый проект закона содержит пункты про экстерриториальное применение, т. е. закон распространяется на другие страны, собирающие и обрабатывающие данные граждан Китая. Предусмотрено требование о назначении офицера по персональным данным при достижении определенных условий.

Эксперты отмечают следующие основные отличия от GDPR: отсутствие разделения понятий обработчика и держателя; любые утечки должны сообщаться уполномоченным органам. Также нужно отметить, что предусмотрены санкции за нарушения и утечки персональных данных.

В свете движения Китая в сторону строгого регулирования персональных данных, в случае его принятия, мы сможем проверить гипотезу, высказываемую некоторыми руководителями технологических гигантов, таких как Джек Ма и Марк Цукерберг: строгое регулирование персональных данных может ограничить инновации, основанные на данных. Также может быть проверена на опыте Китая через какое-то время.

---

<sup>19</sup> <https://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/>

<sup>20</sup> <https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/>

<sup>21</sup> [https://www.technologyreview.com/2021/02/24/1017801/data-trust-cybersecurity-big-tech-privacy/amp/?\\_\\_twitter\\_impression=true&s=03](https://www.technologyreview.com/2021/02/24/1017801/data-trust-cybersecurity-big-tech-privacy/amp/?__twitter_impression=true&s=03)

## 5.4 Россия

Необходимо отметить, что Конвенцию 108 Совета Европы от 1981 года «О защите физических лиц при автоматизированной обработке персональных данных» ратифицировали многие постсоветские страны, включая Россию, Армению, Азербайджан, Грузию, Молдову, Украину и все балтийские страны.

В России понятие персональных данных впервые было прописано в Федеральном законе «Об информации, информатизации и защите информации» в 1995 году. Несмотря на то что Россия одобрила Конвенцию о защите физических лиц при автоматизированной обработке персональных данных (далее Конвенция 108) Совета Европы в 2001 году, она приняла свой первый отдельный закон о персональных данных только в 2006-м. В законе прописаны основные принципы, которые аналогичны принципам Конвенции 108.

В 2014 году в нее были внесены изменения, были включены требования по хранению и обработке персональных данных на территории Российской Федерации. Через два года в законе расширили административную ответственность и увеличили размеры штрафов. Также стоит отметить, что законы РФ не имеют экстерриториального характера. Многие эксперты склонны считать, что основным недостатком регулирования ПД в РФ являются относительно возможные малые штрафы, которые могут быть значительными только для небольших организаций, но для крупных технологических компаний совсем не значительны. К примеру, в РФ самый большой штраф за сбор и обработку персональных данных без согласия субъекта составляет всего 75 тысяч рублей. Стоит отметить, что контроль за соблюдением требований закона возложен на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Также она является ответственной за ведение Реестра операторов, осуществляющих обработку персональных данных, так как в Законе РФ «О персональных данных» операторы, осуществляющие обработку персональных данных, обязаны до начала обработки персональных данных уведомить уполномоченный орган. За технические меры по защите ПД отвечают также Федеральная служба по техническому и экспортному контролю РФ (ФСТЭК) и Федеральная служба безопасности РФ (ФСБ).

## 5.5 Казахстан

В Республике Казахстан (РК) закон о персональных данных был принят в 2013 году. До середины 2020 года функции уполномоченного органа в РК исполняла прокуратура. Некоторые исследователи<sup>22</sup> в 2020 году отмечали, что главной проблемой является не само законодательство, а основные проблемы лежат в ее реализации. Например, они отмечали, что ни один госорган или государственный служащий не был наказан за нарушение законодательства по ПД согласно действующим законам РК. «Ведение реестра операторов ПД» в РК присутствует, несмотря на то что во многих странах (в европейских странах, Израиле и др.) данный инструмент считается устаревшим и подобные требования отсутствуют в законодательствах. Как отмечено в статье «Дентонс»<sup>23</sup>, согласно последним изменениям от 25 июня 2020 г. «О внесении изменений и дополнений в некоторые

---

<sup>22</sup>[https://www.soros.kz/wp-content/uploads/2020/04/Personal\\_data\\_report.pdf](https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf)

<sup>23</sup><https://www.dentons.com/ru/insights/articles/2020/july/14/amendments-on-personal-data-protection-issues-in-kazakhstan#footnote1>

законодательные акты РК по вопросам регулирования цифровых технологий», вместо прокуратуры будет определен специальный уполномоченный орган. По последней информации, уполномоченным органом определен Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (МЦРИАП РК). Также, согласно изменениям, будут разработаны правила сбора, обработки персональных данных и требование о назначении лица, ответственного за организацию обработки персональных данных в учреждениях. Следует отдельно отметить, в закон включаются требования о том, чтобы содержание и объем собираемых персональных данных строго соответствовал конкретным, заранее заявленным и законным целям их обработки. Также, согласно внесенным изменениям от 2 января 2021 года № 399-VI «О персональных данных и их защите», «хранение персональных данных осуществляется собственником и (или) оператором, а также третьим лицом в базе, находящейся на территории Республики Казахстан» идет по пути РФ и требует хранения ПД в РК.

Несмотря на включение перспективных аспектов по защите ПД, некоторые исследования отмечают, что на практике ПД граждан слабо защищены на данный момент.

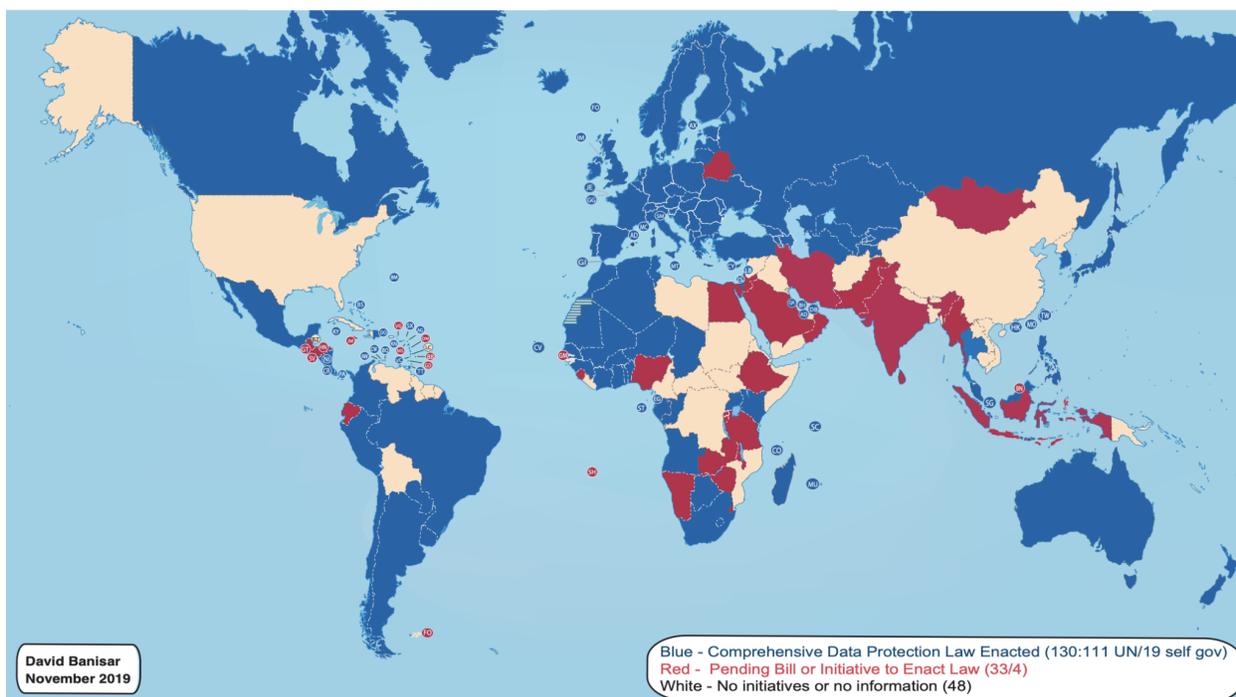


Рис. 2. Страны, которые используют отдельный закон о защите ПД, и имеющие уполномоченные органы<sup>24</sup>.

Как мы можем видеть на Рис. 2, более 130 стран используют отдельный специализированный закон о защите персональных данных и предполагают создание уполномоченного органа (синий цвет). Белым цветом обозначены страны, которые не

<sup>24</sup>Источник: [https://www.researchgate.net/publication/337060085\\_National\\_Comprehensive\\_Data\\_ProtectionPrivacy\\_Laws\\_and\\_Bills\\_-\\_November\\_2019](https://www.researchgate.net/publication/337060085_National_Comprehensive_Data_ProtectionPrivacy_Laws_and_Bills_-_November_2019)

имеют отдельных законов либо используют секторальные законы, например США и Китай. Как мы уже упоминали выше, основываясь на опубликованный закон о ПД в Китае, скорее всего Китай пополнит список стран, регулирующих ПД отдельным законом.

## 6. Ситуация с персональными данными в Кыргызской Республике

Некоторые исследователи<sup>25</sup>, например, профессор Грэм Гринлиф, анализируя законодательства множества стран, включая Кыргызскую Республику, считает, что влияние европейских стандартов и принципов легко читается в нормативных актах. Действительно, имеется множество схожестей закона Кыргызской Республики по персональным данным с Конвенцией 108 и европейской Директивой по защите персональных данных от 1995 года.

Первый закон КР от 2008 года также имеет множество схожестей с Модельным законом, разработанным в рамках Содружества Независимых Государств (СНГ). Одним из аспектов сотрудничества в рамках СНГ была разработка нормативно-правовой базы для стран СНГ, что, возможно, было актуально, так как страны имели тесные связи и схожие законодательные институты на протяжении многих лет. Модельный закон «О персональных данных»<sup>26</sup> был разработан и принят Межпарламентской ассамблеей СНГ, которая состоялась в 1999 году. Считается, что Кыргызская Республика и некоторые страны СНГ использовали данный документ при разработке собственных законов по защите персональных данных.

Большинство соседних стран и стран, с которыми наша страна имеет тесные экономические, исторические связи, как видно из Рис. 2, выбрали подход регулирования защиты ПД единым отдельным законом. На наш взгляд, учитывая активный оборот ПД между данными странами, выбор страны проевропейской модели в вопросах защиты является целесообразным и правильным.

Несмотря на то, что Кыргызская Республика была одна из первых стран Средней Азии, принявших закон о персональных данных в 2008 году<sup>27</sup>, закон по сей день не имеет механизмов контроля. В законе было предусмотрено создание уполномоченного органа для контроля за соответствием обработки персональных данных требованиям закона и защиты прав субъектов персональных данных. Как уже отмечалось, в европейской Директиве от 1995 года уже содержались требования к уполномоченным органам, такие как «полная независимость» (complete independence) и возможность проведения расследования (powers to investigate), но во многих странах, включая Кыргызскую Республику, подобные требования отсутствуют в законодательствах, несмотря на схожесть в других аспектах. На момент написания отчета статус по уполномоченному органу так и остается неопределенным<sup>28</sup>.

В 2017 году законы и другие нормативные акты по персональным данным были существенно улучшены, а именно произошли следующие изменения:

---

<sup>25</sup> [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1960299](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299)

<sup>26</sup> <https://docs.cntd.ru/document/901818602?marker>

<sup>27</sup> <http://cbd.minjust.gov.kg/act/view/ru-ru/202269>

<sup>28</sup> Правительство много раз в разные годы предпринимало попытки создать уполномоченный орган. По последней информации, он более не будет в составе Министерства цифрового развития, вопрос на рассмотрении в аппарате президента и правительства.

- обновление Закона Кыргызской Республики «Об информации персонального характера» от 20 июля 2017 года № 129<sup>29</sup>;
- постановление правительства Кыргызской Республики № 760<sup>30</sup> «Об утверждении Требований к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных» от 21 ноября 2017 года;
- принят Закон Кыргызской Республики «Об электронной подписи» от 19 июля 2017 года № 128<sup>31</sup>;
- постановление правительства Кыргызской Республики «Об утверждении Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядка и формы уведомления субъектов персональных данных о передаче их персональных данных третьей стороне» от 21 ноября 2017 года № 759.

Как видно из вышеприведенного списка, в 2017 году правительство КР разработало и приняло множество нормативных актов в сфере ПД, что может свидетельствовать о желании правительства того периода соответствовать высоким мировым стандартам по защите ПД<sup>32</sup>. Но существуют механизмы, которые усложняют предпринимателям соответствовать некоторым требованиям.

Из пункта в Законе «Об информации персонального характера» Глава 3, Статья 9: *«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».* Любые другие варианты предоставления согласия в КР являются нелегитимными. По сравнению с GDPR, которая позволяет предоставлять согласие различными способами, пункт Статьи 9 КР ограничивает способы получения согласия и делает нелегитимными все другие виды электронного получения согласия. Более того, согласно Статье 9 Закона об электронной подписи, четко прописаны условия использования простой электронной подписи:

*«Электронный документ считается подписанным простой электронной подписью при выполнении одного из следующих условий:*

---

<sup>29</sup> <http://cbd.minjust.gov.kg/act/view/ru-ru/202269>

<sup>30</sup> <http://cbd.minjust.gov.kg/act/view/ru-ru/11512>

<sup>31</sup> <http://cbd.minjust.gov.kg/act/view/ru-ru/111635>

<sup>32</sup> Ryan Moshell считает, что основными мотивами по внедрению регулирования защиты персональных данных отдельным законом в большинстве стран в мире являются:

- негативный опыт из прошлого. Недопущение в будущем несправедливостей, которые происходили из-за неадекватной защиты персональных данных. Опыт европейских стран;
- содействие экономической поддержки из-за все более глобализированного рынка. В качестве примера отмечают страны азиатского региона, которые принимали законы для содействия роста сектора электронной коммерции;
- желание обеспечить соответствие законов страны с лучшими практиками, а именно с европейской моделью регулирования, которая становится доминирующей в мире.

Скорее всего для Кыргызской Республики актуальным является третий случай, т. е. мотивом регулирования ПД является не исторический опыт, т. е. запрос от населения, не желание поддержать развитие электронной коммерции, а внедрение лучших мировых практик в области персональных данных.

1) простая электронная подпись содержится в самом электронном документе;

2) указание ключа простой электронной подписи в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляется создание и (или) отправка электронного документа, было необходимым условием создания и (или) отправки электронного документа с использованием такой информационной системы, и в созданном (отправленном) электронном документе содержится информация, однозначно указывающая на лицо, от имени которого был создан (отправлен) электронный документ...”

В Законе «Об информации персонального характера» имеется специальная Статья 25 «Трансграничная передача данных», где прописаны условия и меры при передаче данных. Но в случаях, когда компании хранят данные в зарубежных сервисах (хостинг сайтов), ссылаясь на пункт «Термины и определения» в Статье 3:

«Трансграничная передача персональных данных - передача держателем (обладателем) персональных данных держателям, находящимся под юрисдикцией других государств», утверждают, что никакой передачи данных не происходит. Компании утверждают, что передача от держателя другому держателю не происходит в этом случае. Необходимо внести изменения для однозначной трактовки вопросов относительно трансграничной передачи данных.

Несмотря на улучшения, на наш взгляд, существенные аспекты не были учтены, а именно:

- явно не прописаны права на отзыв согласия;
- договорные отношения не являются законным основанием для сбора и обработки ПД<sup>33</sup>;
- использование электронной подписи для согласия сильно ограничивает возможности и создает сложности при получении электронных форм согласия;
- отсутствует право пользователей на отказ от прямого маркетинга;
- отсутствует необходимость уведомления об утечке информации (как уполномоченного органа, так и пользователей);
- требуются пояснения относительно трансграничной передачи данных;
- отсутствуют меры ответственности за многие правонарушения и преступления с персональными данными;
- отсутствие понятий защиты персональных данных детей.

Не успел закон фактически вступить в действие (из-за отсутствия механизмов контроля), как уже отстал от современных мировых трендов по защите данных, как, например, в GDPR:

- Право на забвение.
- Право на переносимость данных.
- Отсутствуют понятия «встроенная защита персональных данных» и «защита по умолчанию».

---

<sup>33</sup> Если сравнивать с GDPR, многие пункты правовых оснований для сбора совпадают, но в Законе о ПД в КР в Статье 5 отсутствует упоминание о договорных отношениях, как один из законных видов сбора и обработки данных.

Учитывая отсутствие требований об уведомлении утечки информации и уполномоченного органа в Кыргызской Республике, нечасто публикуются данные об утечках персональных данных.

## 6.1 Утечки персональных данных в Кыргызской Республике

Как известно, персональные данные могут быть как конечной целью злоумышленников для продажи на маркетплейсах даркнета<sup>34</sup> или могут быть промежуточной – для реализации последующих атак. Последующие атаки обычно проводятся с использованием социальной инженерии для мошенничества, фишинга (телефонный, видео)<sup>35</sup>.

Если так называемые нормальные персональные данные в основном используются для мошенничества и для таргетированных атак, то утечки чувствительных персональных данных могут кардинально изменить и нарушить обычный расклад жизни жертвы.

В нашей стране множество случаев взломов и утечек обсуждается только в узких специализированных кругах. Например, обсуждались взломы университетов, банков и операторов связи, которые не публиковались на информационных ресурсах. Множество утечек и взломов могут быть неизвестны широкой общественности из-за отсутствия требований по уведомлению утечек. Ниже мы приведем примеры взломов и утечек, которые широко обсуждались в обществе.

Активно обсуждалась в кыргызском сегменте Интернета утечка фотографий с камер «Безопасного города», на которых один и тот же госномер, вероятно, подложный, использовался на пяти разных автомобилях. Тогда пользователи Сети начали предполагать, что на одной из фотографий мог быть глава Государственной регистрационной службы (ГРС). Данный случай является примером, когда утечка персональных данных могла нанести гражданину ощутимый урон репутации и навредить личной жизни. Тогда премьер-министр страны поручил провести служебное расследование Госкомитету информационных технологий<sup>36</sup>. Позже была информация, что два сотрудника Центра мониторинга Главного управления по обеспечению безопасности дорожного движения МВД КР (ГУОБДД) за допущенные нарушения и ненадлежащее исполнение своих обязанностей, а именно использование в неслужебных целях служебную информацию и распространение данного фото посторонним лицам, были уволены. Известно, что один из операторов Центра мониторинга ГУОБДД скачал служебную информацию по нарушению правил дорожного движения на свой служебный компьютер с последующей передачей через WhatsApp другим лицам. Он был задержан по статье 98 УПК КР по подозрению в совершении преступления, предусмотренного статьей 304 часть 2 «Неправомерный доступ к компьютерной информации» и водворен в ИВС. В прессе не удалось найти дальнейшую судьбу задержанного.

---

<sup>34</sup>Стоимость персональных данных варьируется от типа, страны и других критериев <https://www.privacyaffairs.com/dark-web-price-index-2021/>

<sup>35</sup> Как известно, в мире, а в особенности в России, популярной является мошенническая схема, когда звонят якобы сотрудники банков и под разными предложениями, чаще для блокировки подозрительных активностей, пытаются получить детали банковских карт.

<sup>36</sup><https://kloop.kg/blog/2019/12/05/premer-poruchil-provesti-rassledovanie-iz-za-utechki-dannyh-bezopasnogo-goroda/>

Также имеются другие опубликованные взломы, но по ним сложно оценить утечки персональных данных. К примеру, взлом банков<sup>37</sup> (2017), взлом веб-сайта Жогорку Кенеша<sup>38</sup> (2020). Необходимо учитывать тот факт, что в случае если в утечке участвовали данные граждан ЕС, то возможны серьезные последствия для предприятий согласно GDPR, так как закон, как уже упоминалось выше, имеет экстерриториальный характер.

В ходе проведения исследования с нами поделились примером нарушения защиты персональных данных, который стоит отдельного упоминания. На текущий момент перед госпитализацией в государственные больницы у пациентов берут ПЦР-тесты. По идее, результаты должны приходить в виде SMS индивидуально на указанный номер телефона. Но также в месте приема ПЦР-тестов висит вывеска с номерами телефонов, где можно запросить результаты через приложение WhatsApp. На запрос о результатах сотрудники больницы отправили полный список (в нашем случае 103 человека), кто сдавал анализы в тот день с результатами. Как вы можете увидеть на Рис. 3, в документе указаны Ф. И. О., дата рождения, дата сдачи и результаты ПЦР. Подобные утечки в разных странах приводили в 2020 году к различным видам травли и являются ярким примером несоблюдения законов по ПД.

№	Ф. И. О.	Дата рождения	Дата сдачи	Результат
44	Кирпич	28.07.1974	26.04.2021	Положительный
45	Кирпич	30.11.2006	26.04.2021	Положительный
46	Кочуновна	05.05.1961	26.04.2021	Отрицательный
47	Кочунович	05.02.1982	26.04.2021	Положительный
48	Кочунович	19.03.1961	26.04.2021	Отрицательный
49	Кулукович	05.03.1953	26.04.2021	Отрицательный
50	Курманбекович	27.12.1966	26.04.2021	Отрицательный
51	Курманбаевна	15.08.1971	26.04.2021	Отрицательный
52	Кузиевна	07.07.1972	26.04.2021	Отрицательный
53	Мамрозобаевич	25.10.1969	26.04.2021	Отрицательный
54	Мамна	11.07.2001	26.04.2021	Положительный
55	Мамна	16.02.1976	26.04.2021	Отрицательный
56	Молдонишбекович	16.03.1973	26.04.2021	Отрицательный
57	Молдонишбекович	30.10.1966	26.04.2021	Отрицательный
58	Муминовна	20.02.1966	26.04.2021	Отрицательный
59	Мусуновна	08.12.1966	26.04.2021	Отрицательный

Рис. 3. Результаты ПЦР-теста с персональными данными граждан.

<sup>37</sup>[https://kaktus.media/doc/355983\\_syd\\_ne\\_stal\\_sajat\\_hakera\\_pohitivshego\\_polmilliona\\_somov\\_iz\\_bankomata.html](https://kaktus.media/doc/355983_syd_ne_stal_sajat_hakera_pohitivshego_polmilliona_somov_iz_bankomata.html)

<sup>38</sup><https://kloop.kg/blog/2020/10/19/neizvestnye-vzломali-sajt-parlamenta-i-potrebovali-vykup-v-10-tysyach-dollarov-v-zhogorku-keneshe-nazvali-eto-hakerskoj-atakoj/>

## 7. Сбор данных

Сектора	Количество компаний	Собирают данные	Получают согласие	Опубликовали политику	Опубликовали политику на государственном языке
Строительство	35	20	0	0	0
Промышленность	107	26	1	2	0
Сельское хозяйство	15	1	0	0	0
Услуги	370	127	34	23	1
<b>Всего</b>	<b>527</b>	<b>174</b>	<b>35</b>	<b>17<sup>39</sup></b>	<b>1</b>

Таблица 3. Общая статистика

### 7.1 Методология

#### Метод сбора данных

В рамках реализации данного проекта произведен сбор первичных данных, а именно анализ веб-сайтов и бумажных форм, которые собирали ПД. Также в рамках проекта изучались соответствующая литература, законы и подходы других стран в обеспечении защиты персональных данных.

#### Выборка исследования

Выборка исследования составила 527 сайтов, и этот охват позволил получить статистические данные по различным отраслям. Для анализа были выбраны компании из четырех основных макроэкономических секторов: промышленность, сельское хозяйство, услуги и строительство, которые используются в Министерстве экономики и финансов КР.

---

<sup>39</sup> Исключены политики, которые не были адаптированы под КР. К примеру, ссылки на политику google, политики, в которых использовались ссылки на законодательство РФ.

Необходимо отметить, для получения предварительных списков компаний по секторам использовались официальные веб-сайты государственных структур. Только в случаях невозможности найти списки использовались другие источники для определения списков для анализа. Итого по результатам проанализированных веб-страниц и мобильных приложений наибольшим количеством является сектор «Услуги» (71,7 %). Следом идет сектор «Промышленность» с 20 %, «Строительство» – около 5 %, наименьшее взаимодействие у сектора «Сельское хозяйство» (2,8 %).

#### Количество просмотренных компаний из каждого сектора

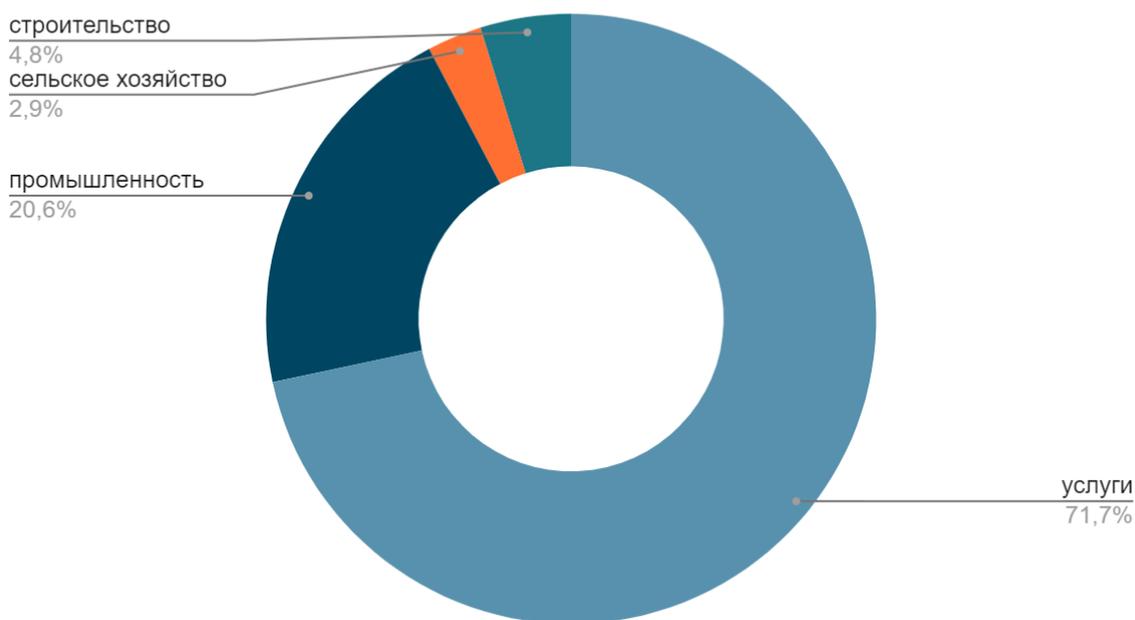


Рис. 4. Соотношение общего количества компаний, проанализированных из каждого сектора.

#### 7.1.1 Сектор «Строительство»

##### Источники

В первую очередь был просмотрен сайт Государственного агентства архитектуры, строительства и жилищно-коммунального хозяйства при кабинете министров КР<sup>40</sup>, где мы не смогли найти списки действующих строительных компаний. По этой причине для анализа сбора данных в этом секторе были использованы списки с сайтов «Акчабар»<sup>41</sup> и «Элитка КГ»<sup>42</sup>.

##### Количество

<sup>40</sup> <http://gosstroy.gov.kg/ru/>

<sup>41</sup> <https://www.akchabar.kg/ru/realty/>

<sup>42</sup> <https://elitka.kg/builder/index>

Всего просмотрены 35 строительных компаний, из которых сбор данных осуществлялся на сайтах 19 компаний.

Все 19 компаний осуществляли сбор ПД для обратного звонка, запрашивали Ф. И. О., мобильный номер телефона, семь компаний – электронную почту.

### 7.1.2 Сектор «Промышленность»

#### **Источники**

Список данного сектора получен с сайта Министерства энергетики и промышленности КР<sup>43</sup>. Всего просмотрено 107 действующих крупных предприятий, из которых 26 собирали данные персонального характера, две компании опубликовали Политику обработки ПД.

#### **Количество**

В основном сбор данных осуществлялся для обратной связи (34,6 %), для заказа товаров и услуг (26,9 %), а также для возможности оставить заявку (26,9 %).

### 7.1.3 Сектор «Сельское хозяйство»

#### **Источники**

Поиск компаний, собирающих данные, производился через сайт Министерства сельского, водного хозяйства и развития регионов Кыргызской Республики<sup>44</sup>; поиск в Интернете; данные других источников<sup>45</sup>.

#### **Количество**

По итогу были просмотрены 15 сельскохозяйственных предприятий. Из данного списка только на одном сайте запрашивались ПД для обратной связи.

### 7.1.4 Сектор «Услуги»

#### **Источники**

Для обширного охвата различных отраслей сферы услуг формирование списков происходило следующими этапами:

изучение видов услуг, указанных на сайте Министерства экономики КР;

поиск компаний по видам в Google search, 2GIS, Instagram, Lalafo и т. д.;

анализ списка самых посещаемых сайтов в КР.

Питание и проживание. Источники формирования списков в этой отрасли: веб-сайт - Рестораны<sup>46</sup>, 2GIS, топ используемых приложений в Google Play Market.

Транспорт и связь. Поиск организаций этой отрасли происходил через сайт Ассоциации операторов связи<sup>47</sup>, а также через поиск в Интернете организаций, предоставляющих транспортные услуги.

Услуги в сфере образования. Список сектора «Образование» формировался из нескольких групп: детские сады, частные школы, учебные курсы.

---

<sup>43</sup> <http://www.gkpen.kg/>

<sup>44</sup> <https://agro.gov.kg/language/ru/main/>

<sup>45</sup> <http://www.inform.kg/>

<sup>46</sup> <https://restoran.kg/restaurant>

<sup>47</sup> <http://aoc.kg/>

Детские сады. Поиск организаций этой отрасли происходил через сайт Министерства образования и науки Кыргызской Республики, частных детских садов – из источника «Кактус Медиа»<sup>48</sup>, 20 – из источника Catalog<sup>49</sup> и 28 – из карты 2GIS.

Частные школы. Список частных школ для просмотра был взят из источника «Кактус Медиа»<sup>50</sup>.

Услуги в сфере «Здравоохранение и спорт». Список этого раздела формировался из медицинских центров, аптечных учреждений, лабораторий и спортивных учреждений в основном из сайта «Спутник»<sup>51</sup>.

Медиаиндустрия. Для первичного анализа были отобраны наиболее посещаемые новостные сайты КР, по данным исследования «Медиапредпочтения населения Кыргызстана» (8 волна)<sup>52</sup>.

Банки. Список проанализированных сайтов банков получен из официального сайта Национального банка КР<sup>53</sup>.

Бытовое обслуживание населения<sup>54</sup>. Для анализа отбирались сервисные центры, услуги по доставке, доски объявлений, ассоциации и прочее. Формировался из списка 100 самых посещаемых сайтов КР.

## **Количество**

Итого были просмотрены более 370 единиц бизнеса, которые предоставляли услуги по следующим отраслям:

Торговля (оптовая и розничная). Из данной отрасли были просмотрены более 50 единиц бизнеса. Основную массу исследуемых компаний составили интернет-магазины и мультифилиальные супермаркеты. Политика обработки ПД имела у четырех компаний.

Питание и проживание. Всего просмотрели более 70 единиц бизнеса, из которых 11 проанализированы, у трех имела Политика обработки ПД.

Транспорт и связь. Из общего числа просмотренных компаний ПД собирают 15. Политика обработки ПД присутствует у трех компаний.

Услуги в сфере образования. Были просмотрены 77 частных детских садов. Количество просмотренных частных школ составило 42 единицы. Так как предоставление услуг по повышению квалификации и прохождению курсов было просмотрено более 40 единиц в этой сфере. Итого было просмотрено 149 единиц.

---

<sup>48</sup>[https://kaktus.media/doc/384422\\_gid\\_kaktus:\\_detskie\\_sadiki\\_s\\_osobymi\\_metodikami\\_vospitaniia.\\_spisok\\_ceny\\_adresa.html](https://kaktus.media/doc/384422_gid_kaktus:_detskie_sadiki_s_osobymi_metodikami_vospitaniia._spisok_ceny_adresa.html)

<sup>49</sup> <https://www.catalog.kg/maps/nauka-i-obrazovanie/detskie-sady>

<sup>50</sup>[https://kaktus.media/doc/338956\\_gid\\_kaktus.\\_chastnye\\_shkoly\\_bishkeka.\\_ysloviia\\_i\\_ceny\\_obnovleno\\_19\\_maia.html](https://kaktus.media/doc/338956_gid_kaktus._chastnye_shkoly_bishkeka._ysloviia_i_ceny_obnovleno_19_maia.html)

<sup>51</sup> <https://ru.sputnik.kg/sport/20181023/1041663957/fitnes-centry-bishkek-spisok.html>

<sup>52</sup> <https://soros.kg/wp-content/uploads/2017/12/Otchet-Mediapredpochteniya-naseleniya-KR-8-volna.pdf>

<sup>53</sup> <https://www.nbkr.kg/index1.jsp?item=69&lang=RUS>

<sup>54</sup>К сфере бытового обслуживания населения не относятся услуги, находящиеся в ведении других специализированных отраслей обслуживания населения, таких как образование, торговля, общественное питание, жилищно-коммунальное хозяйство, здравоохранение, культура, пассажирский транспорт, связь.

Услуги в сфере «Здравоохранение и спорт». Было просмотрено 124 единицы, онлайн-сбор осуществлялся 27 компаниями. Политика обработки данных была у двух организаций.

Медиаиндустрия. Сбор персональных данных производился только на пяти сайтах. Кроме прочего, в данный раздел включены медиаресурсы, такие как «Намба» и ONLINE CINEMA.

Банки. Всего просмотрено 23 сайта банков, из которых мы проанализировали 15 сайтов, сбор ПД через сайт проводился только у двух банков.

Бытовое обслуживание населения. Всего отобраны и проанализированы 23 компании.

## 8. Анализ данных

В данном разделе мы проанализируем опубликованные политики по защите персональных данных. Для анализа политики мы рассмотрим наличие требований по публикации в других странах и рекомендуемые шаблоны политики.

В первую очередь мы хотим отметить, что, несмотря на то что только менее 3 % изученных сайтов компаний разработали и опубликовали политику, данные компании демонстрируют положительную практику по защите персональных данных клиентов.

Мы заметили, что некоторые компании опубликовали на сайтах Политику по защите персональных без адаптации для КР. К примеру, некоторые из них ссылаются на Политику конфиденциальности и Условия использования компании Google. Другие используют политику, в которой используются ссылки на законодательство РФ («Текстиль Транс»<sup>55</sup>, Codify Lab<sup>56</sup>). Данные политики не были детально проанализированы и не участвуют в статистике ниже.

Также в рамках анализа мы изучим количество собираемых ПД и сопоставим их с данными из политик, а именно сравним перечень данных с фактически собираемыми данными и сопоставим фактически собираемые данные с заявленными целями.

### 8.1 Политика по обработке персональных данных

В США, Китае, Европе и в законах РФ имеются требования по публикации политики обработки ПД. В США закон ССРА требует, чтобы коммерческие организации разработали политику и включили туда минимум следующие права потребителей – на доступ, на удаление, запрет на продажу ПД, на недискриминацию. В GDPR имеются требования о прозрачности при сборе и обработке ПД, согласно которым операторы должны четко представлять физическим лицам информацию о том, кто обрабатывает их персональные данные и почему. В Интернете достаточно много сервисов для генерации политик под требования GDPR, ССРА<sup>57</sup>. В РФ в статье 13.11 Кодекса РФ об административных правонарушениях есть требования и прописаны штрафы. В случае если оператор персональных данных не опубликовал информацию и не обеспечил доступ к документу, в

<sup>55</sup> [https://www.textiletrans.com/include/licenses\\_detail.php](https://www.textiletrans.com/include/licenses_detail.php)

<sup>56</sup> <https://www.codifylab.com/privacypolicy>

<sup>57</sup> Существует множество сервисов для генерации политик. Некоторые из них перечислены: <https://digital.com/privacy-policy-generators/>

котором прописаны все условия использования персональных данных или сведения о реализуемых требованиях, ему может быть вынесено предупреждение или выписан административный штраф. Для физических лиц он составляет от 700 до 1 500 рублей; для должностных лиц от 3 000 до 6 000 рублей; для индивидуальных предпринимателей от 5 000 до 10 000 рублей, для юридических лиц от 15 000 до 30 000 рублей.

Из более чем 527 изученных сайтов, которые осуществляют сбор ПД, только 23 опубликовали политику ПД по сбору и обработке на веб-сайтах (см. Приложение Б). Возможно, это является следствием того, что в КР отсутствуют требования по публикации политики. Требование в постановлении правительства КР № 760 (для «синего уровня защищенности<sup>58</sup>») – «*принятием документа, определяющего политику держателя (обладателя) массива персональных данных в отношении обработки персональных данных, и доведением содержания данного документа до работников и контрагентов держателя (обладателя) массива персональных данных*» – скорее всего относится к организации защиты ПД внутри организаций, так как в данном пункте ничего не сказано про доступ субъекта ПД к данной политике.

### **Подготовка чек-листа для анализа политики по защите ПД**

Так как в КР отсутствуют требования к разработке политики по защите ПД и/или доступу к нему субъекта, соответственно, отсутствуют рекомендации по содержанию политики. Для анализа политики, которую используют компании в КР, мы изучили рекомендации GDPR и РФ по содержанию политики<sup>59</sup>.

GDPR рекомендует<sup>60</sup> включить следующую информацию в политику<sup>61</sup> по ПД:

- информация о вас (контакты, адреса, дочерние компании и т. д.);
- почему вы обрабатываете ПД;
- какова правовая основа;
- кто получит данные (если применимо);
- контактная информация уполномоченного по защите данных (DPO) (если применимо);
- каков законный интерес, преследуемый компанией, когда вы полагаетесь на это правовое основание для обработки;
- меры, применяемые для передачи данных в страну за пределами ЕС;
- как долго данные будут храниться;
- права человека на защиту данных (т. е. право на доступ, исправление, стирание, ограничение, возражение, переносимость и т. д.);

---

<sup>58</sup> Согласно постановлению правительства КР № 760 от 21 ноября 2017 года, имеются различные уровни защищенности персональных данных в зависимости от угроз безопасности. Согласно рейтингу угроз безопасности, выделены синий, зеленый, желтый и красные уровни, где синий – наименьшее наличие угроз, а красный – максимальное наличие угроз.

<sup>59</sup> В связи с существенной разницей подхода США в регулировании ПД с КР (отсутствие прав субъекта, согласия и др.), мы не рассматривали рекомендации США. Рекомендации РК по разработке и содержанию политики нам не удалось найти.

<sup>60</sup> <https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf>

<sup>61</sup> Часто в ЕС объединяют Уведомление об обработке ПД (Privacy Notice), Политику по сбору и обработке Cookie-файлов (Cookies Policy) в Политику по сбору и обработке ПД (Privacy Policy).

- как согласие может быть отозвано (когда согласие является законным основанием для обработки);
- есть ли законодательное или договорное обязательство по предоставлению данных;
- в случае автоматизированного принятия решения – информация о логике, значимости и последствиях решения.

Также имеется требование, что политика должна быть написана ясным, простым и понятным языком.

В РФ Роскомнадзор разработал Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных<sup>62</sup>. В политику рекомендуется включить следующие структурные компоненты:

- общие положения;
- цели сбора персональных данных;
- правовые основания обработки персональных данных;
- объем и категории обрабатываемых персональных данных, категории субъектов персональных данных;
- порядок и условия обработки персональных данных;
- актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным.

Сравнивая рекомендации, можно сделать вывод, что большинство пунктов рекомендаций РФ и GDPR перекликаются между собой.

Для разработки чек-листа для анализа имеющихся политик компаний КР нам необходимо было проанализировать законодательство и другие нормативные акты КР. Первым критерием являлась непротиворечивость вышеупомянутых пунктов рекомендаций нормативным актам КР. Неприменимые рекомендации и пункты были удалены. Учитывая фокус нашего исследования, мы добавили в чек-лист пункты об использовании простой электронной подписи для дачи согласия и заявлений об использовании обезличенных данных.

В итоге мы получили следующий чек-лист, согласно которому были проанализированы политики.

#	Наименование	Общие положения	Контактные данные организации	Перечень собираемых ПД	Основания сбора/обработки ПД (согласие, договорные отношения, иное)	Цели обработки ПД	Передача ПД	Перечень источников ПД	Хранение ПД (места хранения, срок, уничтожение данных)	Права субъекта ПД (актуальность, отзыв согласия, на доступ)	Возможность обжалования и контакты для жалоб (DPO)	Соблюдение требований конфиденциальности	Marketing	Cookies	Соглашение об использовании простой электронной подписи	Использование и/или передача обезличенных данных
---	--------------	-----------------	-------------------------------	------------------------	---	-------------------	-------------	------------------------	--	---	--	--	-----------	---------	---	--

Рис. 5. Чек-лист для анализа опубликованных политик по защите ПД.

<sup>62</sup> <https://rkn.gov.ru/docs/Rekomendacii31072017.docx>

## 8.2 Сектор «Строительство»

Все веб-сайты изученных нами строительных компаний собирали ПД только для осуществления обратного звонка, где запрашивались контактные данные для связи, такие как Ф. И. О., мобильный номер телефона и электронная почта.

Только одна компания включила пункт согласия, который не соответствует законодательству, – без электронной подписи. Ни одна строительная компания не опубликовала политику на сайте. В перечне фактически собираемых данных через сайты отсутствуют излишне собираемые ПД.

## 8.3 Сектор «Промышленность»

Производственные предприятия в основном собирают ПД для предоставления возможности заказа товаров и обратной связи с клиентами. В отличие от сектора «Строительство», кроме контактных данных (Ф. И. О., мобильный телефон, электронный адрес), шесть компаний собирают адреса (для доставки товаров).

Из 26 собирающих ПД компаний только одна получает согласие («Куликовский»). Также только две компании опубликовали Политику по обработке ПД. Одна из них использовала политику, не адаптированную под законодательство КР. Мы сравнили фактически собираемые данные компанией «Куликовский» с перечнем из политики и соответствия целей и заключили, что данные соответствуют полностью заявленным целям и перечню, за исключением несущественного отличия<sup>63</sup>.

## 8.4 Сектор «Сельское хозяйство»

К сожалению, нам не удалось проанализировать достаточное количество компаний в секторе «Сельское хозяйство».

## 8.5 Сектор «Услуги»

Сектор «Услуги» наиболее представлен в веб-пространстве. Нам удалось проанализировать большее количество форм сбора персональных данных, чем в других секторах. Из 127 осуществляющих сбор ПД только 34 имеют формы согласия, что составляет 26 %. Из 34 только несколько компаний собирают данные во время или после регистрации (логин/пароль) и/или идентификации, что может считаться использованием простой электронной подписи. Из 127 только одна компания включила Соглашение об использовании простой электронной подписи в свою политику, что, согласно Статье 6 Закона об электронной подписи, может быть признано равнозначно документам на бумажном носителе, подписанным собственноручной подписью. Также пять компаний используют бумажные версии для сбора персональных данных с включенными пунктами о согласии, что соответствует законодательству страны.

---

<sup>63</sup> Компания «Куликовский» собирает данные «Пол» в мобильной версии, но не указал в перечне политики данное поле.

Также нам удалось найти только у 23 компаний опубликованные Политики по сбору и защите ПД (см. Таблицу 3).

Из 127 компаний, осуществляющих сбор и обработку ПД из данной сферы, у 58 сайты находятся за пределами Кыргызской Республики. Но только восемь компаний включили текст согласия на трансграничную передачу данных.

Что касается анализа политики, то мы составили обобщенную таблицу по соответствию политики в нашем чек-листе. Учтены только полностью соответствующие пункты, к примеру, если политика содержит права субъекта, но не указано право на отзыв согласия, данные не включены в статистику ниже.

### Наблюдения опубликованных политик по сектору «Услуги»

Цели обработки ПД	Передача ПД	Общие положения	Основания сбора/обработки ПД (согласие, договорные отношения, иное)	Соблюдение требований конфиденциальности	Перечень собираемых ПД	Cookies	Контактные данные организации	Возможность обжалования и контакты для жалоб (DPO)	Права субъекта ПД (актуальность, отзыв согласия, на доступ)	Хранение ПД (места хранения, срок, уничтожение данных)	Marketing	Перечень источников ПД	Соглашение об использовании простой электронной подписи	Использование и/или передача обезличенных данных
16	16	14	14	14	11	7	6	6	5	4	3	1	1	1

Рис. 6. Результаты соответствия политик компаний чек-листу.

Как видно из таблицы, абсолютное большинство политик содержат цели сбора и обработки ПД и пункты про передачу ПД. Большинство отметили в политике пункты про легитимную основу для сбора (14 из 17), ответственность по соблюдению требований конфиденциальности (14 и 17) и привели перечни собираемых ПД. Меньше половины политик содержат разделы про Cookie-файлы, контактные данные организации, возможности обжалования и права субъектов ПД.

Наиболее полными, согласно нашему чек-листу, являются политики компаний Glovo, «Скай Мобайл». Следом идут компании Lalafo и «Нават».

Только компания Glovo опубликовала политику на кыргызском и русском языках. Также она опубликовала отдельную политику по использованию файлов Cookie. В политике компании прописывается право пользователей на переносимость данных и право возражения против обработки личных данных. Эти пункты соответствуют требованиям GDPR.

Как уже отмечалось, по действующему законодательству КР только собственноручно подписанные согласия и согласия, в которых использовались электронные подписи, являются легитимными. Только в одной из политик (ОсОО «Скай Мобайл») было подписано соглашение об использовании простой электронной подписи.

Нам удалось найти только две политики по защите персональных данных среди 23 банков КР. Политики опубликовали только «Оптим Банк» и «Дос-Кредобанк».

Только две организации (Namba food, «Предприниматель») прописали в политике, что при утрате или разглашении персональных данных администрация сайта, мобильного приложения информирует пользователя об утрате или разглашении персональных данных.

Только одна организация («Нур Телеком») прописала пункты о защите ПД детей. Она призвала в политике детей, не достигших 18 лет, не регистрироваться на веб-ресурсах

и не осуществлять их использование без разрешения и участия родителей или опекунов, или иных законных представителей, а также не предоставлять какие-либо сведения о себе.

Только одна организация (Lalafо) отметила возможность передачи обезличенных данных для лучшего понимания заинтересованности пользователей тех или иных услуг и рекламы.

Интересно отметить, что наиболее полные политики оказались у компаний, которые являются дочерними европейских компаний.

### **Сравнение фактически собираемых данных с перечнем из политики**

Из 370 просмотренных нами компаний 127 осуществляют сбор и обработку ПД. В наиболее собираемый перечень входят (см. Таблицу 4) Ф. И. О. (109), мобильный телефон (105), электронный адрес (81), адрес (36), дата рождения (33) и пол (19).

Копии паспортов (11) собираются банками, компаниями, предоставляющими связь, и компаниями, осуществляющими перевозки и доставку товаров из-за рубежа. В основном торговые компании для предоставления дисконтных карт и маркетинга собирают информацию о наличии детей (6), наличии авто (4), наличии животных (3). Банки и торговые компании собирают социальный статус (7), семейное положение (7). ИНН (8), фотографию (5), различные виды услуг. Особую озабоченность вызывают компании, которые обрабатывают специальные категории персональных данных<sup>64</sup>, такие как национальность.

Название поля	Количество	Название поля	Количество	Название поля	Количество
Ф. И. О.	109	Копия паспорта	11	Адрес	36
Дата рождения	33	Семейное положение	7	Дом. телефон	4
Национальность	2	Социальный статус	7	Моб. телефон	105
Пол	19	Образование	2	Электронный адрес	81
Наличие авто	4	Дети	6	Фотография	5
ИНН <sup>65</sup> и/или удостоверение личности	8	Наличие животных	3	Аккаунты в соцсетях	1

<sup>64</sup>К специальным категориям, согласно Закону КР «Об информации персонального характера», относятся расовое или этническое происхождение, национальная принадлежность, политические взгляды, религиозные или философские убеждения, а также касающиеся состояния здоровья и сексуальных наклонностей.

<sup>65</sup>Зная только ИНН, можно проверить на государственных порталах следующую информацию без регистрации: семейное положение; наличие транспортного средства; статус по готовности паспорта; проверка наличия адреса регистрации; статус выплаты «балага суйунчу» (если ИНН ребенка). Если дополнительно известен госномер авто, то можно проверить штраф по проекту «Безопасный город» с фотографиями по нарушениям. Зная паспортные данные, можно получить сертификат по вакцинации.

Таблица 4. Перечень и количество ПД в секторе «Услуги».

Некоторые компании, опубликовавшие Политику, детально не прописали перечень собираемых данных, например, Газпром<sup>66</sup>, «Намба Фуд»<sup>67</sup>, KUPI.KG<sup>68</sup>, Svetofor<sup>69</sup>, соответственно было невозможно сравнить фактические данные с перечнем из Политики.

Мы сравнили фактически собираемые ПД, указанные в Политике, в следующих компаниях: «Предприниматель», Shisha.kg, Parajohns.kg, «Дос-Кредобанк», «Оптима Банк», «АзияИнфо», Navat, Glovo, «Скай Мобайл», «Нур Телеком», «Лалафо». Мы утверждаем, что фактически собираемые данные совпадают с заявленным в Политике перечнем.

У некоторых компаний имеются отличия между перечнем из Политики и фактически собираемыми данными. К примеру, ОсОО «Технодом Оператор» собирает большее количество ПД по сравнению с заявленным в Политике. К примеру, фактически собираемые данные, которые не указаны в Политике, – дата рождения, ИНН, удостоверение личности, состоит ли в браке, наличие детей (детали смотрите в Приложении В).

Мы также проверили, насколько компании соблюдают права субъектов ПД. Мы направили запросы на доступ к информации и запросы на удаление ПД. По итогам из 23 компаний письма удалось отправить 14. Ответ на наши письма дали лишь пять компаний. Нам не удалось связаться через почту со службой поддержки девяти компаний. А другие девять не ответили на наши письма.

Только 3 % из изученных сайтов имеют Политику по защите персональных данных. Эти компании демонстрируют высокий уровень зрелости и являются лидерами, по сравнению с 97 % компаний, которые не имеют Политики.

---

<sup>66</sup>[https://www.gpnbonus.ru/upload/%D0%9F%D0%9A-S\\_08.02.01.01\\_%D0%9F%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0\\_%D0%BE%D0%B1%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B8\\_%D0%9F%D0%94.PDF](https://www.gpnbonus.ru/upload/%D0%9F%D0%9A-S_08.02.01.01_%D0%9F%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0_%D0%BE%D0%B1%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B8_%D0%9F%D0%94.PDF)

<sup>67</sup><https://nambafood.kg/privacy.html>

<sup>68</sup>Магазин не детально прописал перечень. Для регистрации на сайте магазина пользователь обязан внести некоторую персональную информацию, такую как имя, фамилия, адрес, E-mail, телефон и т. п. <https://kupi.kg/rules>

<sup>69</sup>[https://svetofor.info/politika-konfidencialnosti.html?city\\_id=0](https://svetofor.info/politika-konfidencialnosti.html?city_id=0)

## 9. Рекомендации

### 9.1 Общие рекомендации

В 2018 году Ассоциация GSMA выпустила отчет<sup>70</sup> и рекомендации для стран Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) и некоторых азиатских стран. Например, предложила дорожную карту с временными интервалами по внедрению элементов и механизмов по защите персональных данных (см. рис. 7). Хронология и внедрение элементов в КР сильно отличается от рекомендованного в отчете подхода.

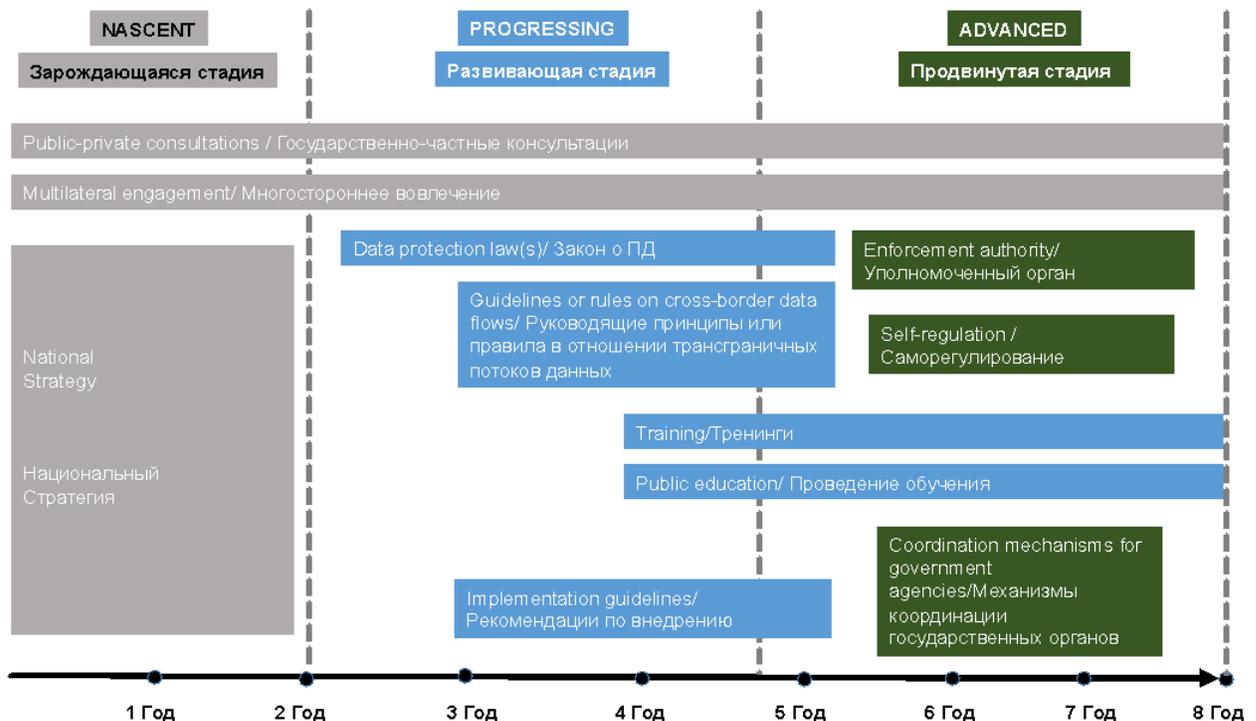


Рис. 7. Дорожная карта по внедрению элементов ПД.

В Кыргызской Республике из вышеуказанных элементов был принят только закон о персональных данных (2008 г., обновление в 2017 г.) Другие элементы из дорожной карты не были внедрены. Как видно из дорожной карты, контроль за исполнением законодательства путем создания уполномоченного органа был рекомендован после публикации Рекомендаций по применению законодательства, Правил по трансграничной передаче данных и после начала активностей повышения осведомленности населения и частного сектора.

Мы считаем, что в нашей стране необходимо создать уполномоченный орган, и рекомендуем ему разработать рекомендации по внедрению законодательства и по трансграничной передаче, провести обучение частного сектора по защите персональных данных, начать проводить активности по повышению осведомленности граждан. Только

<sup>70</sup>[https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows\\_Full-Report\\_Sept-2018.pdf](https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf)

после выполнения вышеуказанных мероприятий, после 3 лет (как рекомендовано в отчете), наделить полномочиями по проверке исполнения законодательства организациями.

## 9.2 Независимый уполномоченный орган по защите персональных данных

Как известно, множество международных стандартов рекомендуют создать не только уполномоченный орган, но и сделать орган независимым. К примеру, первым международным документом считается Резолюция<sup>71</sup> ООН от 1990 года, которая рекомендовала странам следующее:

*«В любом законодательстве должен быть указан орган, который в соответствии с внутренней юридической системой обязан контролировать соблюдение вышеуказанных принципов. Этот орган должен гарантировать соблюдение принципов беспристрастности, независимости по отношению к лицам или органам, ответственным за их обработку и применение, а также техническую компетентность. В случае нарушения положений внутреннего законодательства, касающихся применения вышеуказанных принципов, следует предусмотреть возможность применения уголовно-правовых и других санкций, а также использование соответствующих средств индивидуальной правовой защиты».*

Необходимо отметить, что международные стандарты отмечают различные факторы независимости уполномоченного органа (см. Приложение Г). В силу требований GDPR все европейские страны имеют независимые уполномоченные органы. Что касается постсоветских стран, насколько нам известно, страны Балтии, Грузия и Украина обеспечили определенный уровень независимости уполномоченных органов от исполнительной власти. Несмотря на сложности обеспечения независимости, на наш взгляд, опыт бизнес-омбудсмена – уполномоченного лица по защите прав, свобод и законных интересов субъектов предпринимательской деятельности – мог бы помочь в обеспечении независимости органа.

Одной из стратегических целей уполномоченного органа могло бы стать стремление получить статус страны с адекватной защитой по европейским меркам<sup>72</sup>. Естественно, учитывая, что только 12 стран во всем мире отвечают данным требованиям, это является долгосрочной перспективой. Но стремление получить данный статус может помочь сильно подтянуть компетенции и навыки самого уполномоченного органа, обеспечить обмен опытом с самым передовым регионом по защите ПД, продемонстрировало стремление страны к самым высоким стандартам защиты ПД.

Возможно, на данном этапе было бы рационально обязать Национальный банк КР в рамках проводимых проверок включить проверки соответствия финансово-кредитных учреждений законодательству страны по персональным данным.

<sup>71</sup> [https://digitallibrary.un.org/record/85149/files/E\\_CN.4\\_1990\\_72-RU.pdf](https://digitallibrary.un.org/record/85149/files/E_CN.4_1990_72-RU.pdf)

<sup>72</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

Одними из первоочередных задач уполномоченного органа являются разработка и доведение Рекомендаций по внедрению требований закона о ПД. Как видно из результатов исследования, абсолютно большая часть компаний получают согласия, которые не соответствуют текущему законодательству.

Необходимо проводить активности, направленные на повышение осведомленности населения в вопросах защиты персональных данных, чтобы они могли требовать исполнения своих законных прав.

Одной из основных сложностей, с которой сталкиваются уполномоченные, является защита персональных данных в сервисах, которые находятся в других юрисдикциях. Необходимо наладить контакты и заключить соглашения с уполномоченными органами в других странах и различными объединениями уполномоченных органов GPEN<sup>73</sup>. Необходимо приоритизировать сотрудничество со странами, в которых наши компании осуществляют хостинг. Согласно нашему исследованию, наши компании активно пользуются хостингом в таких странах, как РФ, США, Казахстан, Великобритания, Германия. Возможно рассмотреть сотрудничество в рамках таких площадок, как ЕАЭС, ШОС, в других региональных объединениях.

### 9.3 Законодательство

Два года назад ассоциацией GSMA был выпущен отчет<sup>74</sup> с рекомендациями, какими должны быть «умные» законы по защите персональных данных. Несмотря на то, что отчет направлен на поощрение трансграничного обмена ПД, многие рекомендации могут помочь обновить законодательство страны, учитывая современные тренды.

Мы считаем, что необходимо отменить обязательную регистрацию в уполномоченном органе, но оставить требование только для чувствительного перечня, к примеру, биометрические данные. Также необходимо учесть, что отказ от регистрации уполномоченным органом в современном цифровом мире фактически означает остановку функционирования бизнеса. Мы считаем, что наделение подобными полномочиями (отказ от регистрации) может создать дополнительные риски (коррупционные, бюрократические) для частного сектора.

Основные рекомендации, выявленные по результатам исследования в сфере законодательства:

- прописать в Административном кодексе КР штрафы за нарушения сбора и обработки ПД;
- явно прописать права на отзыв согласия;
- исключить требование использования электронной подписи при получении согласия в электронной форме; добавить, что держатель или обработчик должны быть в состоянии продемонстрировать получение согласия по аналогии с GDPR;
- добавить право отказа от прямого маркетинга;
- дополнить в законные основания для сбора и обработки ПД пункт о договорных отношениях;

---

<sup>73</sup><https://www.privacyenforcement.net/>

<sup>74</sup>[https://www.gsma.com/publicpolicy/wp-content/uploads/2019/06/GSMA\\_Smart-Data-Privacy-Laws\\_Report\\_June-2019.pdf](https://www.gsma.com/publicpolicy/wp-content/uploads/2019/06/GSMA_Smart-Data-Privacy-Laws_Report_June-2019.pdf)

- требуются пояснения относительно трансграничной передачи данных – именно когда компания не передает ПД другим держателям, а использует облачные сервисы, хостинг и др., подпадают ли данные действия под определение трансграничной передачи данных.
- добавить требование о необходимости уведомления об утечке информации субъекта персональных данных и уполномоченного органа (исключить данное требование для зашифрованных данных);
- добавить разделы защиты персональных данных детей, а именно ограничения сбора данных ниже определенного возраста.

#### 9.4 Рекомендации по разработке политики по обработке ПД

По результатам исследования становится очевидным, что необходимо добавить в нормативные акты требования о наличии Политики по защите персональных данных. Без данного требования единичные компании публикуют принципы и процессы по сбору, обработке и защите персональных данных.

Также по результатам изучения опубликованных политик по защите персональных данных, стало очевидным, что необходимо добавить требование, что политики должны быть написаны ясным, простым и понятным языком по аналогии GDPR. К примеру, политики некоторых компаний были написаны с использованием специфических юридических терминов, множество различной информации было представлено без использования структурирования и разделов, что в свою очередь создавало трудности для понимания содержания. Мы рекомендуем вновь создаваемому уполномоченному органу разработать шаблон и опубликовать его, так как единый шаблон поможет легко ориентироваться в политике различных организаций и может повысить доверие населения к защите ПД.

№	Рекомендации	Ответственные
1	Создать независимый уполномоченный орган	Правительство/Администрация президента
2	Предусмотреть мораторий проверки частных компаний на соблюдение ПД на 3 года	Правительство
3	Разработать рекомендации по внедрению требований законодательства и других постановлений по ПД	Созданный уполномоченный орган
4	Разработать правила для трансграничной передачи данных	Созданный уполномоченный орган
5	Рекомендовать Национальному банку КР включить в аудиты/проверки соответствия финансово-кредитных учреждений законодательству страны по персональным данным	НБ КР
6	<p>Дополнить законодательство:</p> <ul style="list-style-type: none"> <li>● прописать в Административном кодексе КР штрафы за нарушения, связанные с нарушениями ПД;</li> <li>● исключить требование использования в соответствии с законодательством Кыргызской Республики электронной подписи при получении согласия в электронной форме, а добавить, что держатель или обработчик должны быть в состоянии продемонстрировать получение согласия по аналогии с GDPR.</li> <li>● добавить дополнительные законные основания, такие как договорные отношения;</li> <li>● явно прописать право на отзыв согласия;</li> <li>● добавить право отказа от прямого маркетинга;</li> <li>● уведомление утечки информации (исключить данное требование для зашифрованных данных);</li> <li>● внесение уточнения и изменения относительно понятий трансграничной передачи данных;</li> <li>● добавить раздел защиты персональных данных детей;</li> </ul> <p>Рассмотреть к дополнению современными требованиями:</p> <ul style="list-style-type: none"> <li>● понятие «встроенная защита персональных данных и защита по умолчанию»;</li> </ul>	Правительство по предложению созданного уполномоченного органа

	<ul style="list-style-type: none"> <li>● понятие «псевдонимизация» как один из основных методов защиты конфиденциальности персональных данных.</li> </ul>	
7	Добавить требования о наличии Политики по ПД и ее содержанию. Разработать рекомендации по разработке Политик по защите персональных данных	Созданный уполномоченный орган

Таблица 5. Рекомендации в виде таблицы.

## 10. Приложения

### Приложение А. Список организаций, попавших в выборку

№	Наименование	Сектор	Вид бизнеса
1	«Автогид»	Бытовое обслуживание населения	Доска объявлений
2	«Автогид Дилер»	Бытовое обслуживание населения	Доска объявлений
3	«Доставка 312»	Бытовое обслуживание населения	Услуги доставки
4	«Интермедиа»	Бытовое обслуживание населения	Сервисный центр
5	«Компмастер»	Бытовое обслуживание населения	Сервисный центр
6	«Меди»	Бытовое обслуживание населения	Трудоустройство
7	«Намба Фуд»	Бытовое обслуживание населения	Услуги доставки
8	«Предприниматель»	Бытовое обслуживание населения	Бизнес-форум
9	Alby Kg	Бытовое обслуживание населения	Рекламное агентство
10	<a href="#">Autobaza.Kg</a>	Бытовое обслуживание населения	Доска объявлений
11	Cargo Jet	Бытовое обслуживание населения	Услуги доставки
12	<a href="#">Doska.Kg</a>	Бытовое обслуживание населения	Доска объявлений
13	Employment. Kg	Бытовое обслуживание населения	Трудоустройство
14	Expressus	Бытовое обслуживание населения	Услуги доставки
15	Glovo	Бытовое обслуживание населения	Услуги доставки
16	<a href="#">Gorizont.Kg</a>	Бытовое обслуживание населения	Рекламное агентство
17	Head Hunter	Бытовое обслуживание населения	Трудоустройство

18	Jia	Бытовое обслуживание населения	Бизнес-ассоциация
19	Job Kg	Бытовое обслуживание населения	Трудоустройство
20	Lalafo Kg	Бытовое обслуживание населения	Доска объявлений
21	Mashina.Kg	Бытовое обслуживание населения	Доска объявлений
22	<a href="#">Revizor.Kg</a>	Бытовое обслуживание населения	Доска объявлений
23	Upgrade	Бытовое обслуживание населения	Рекламное агентство
24	32	Здравоохранение и спорт	Медцентр
25	«Авиценна»	Здравоохранение и спорт	Медцентр
26	«Дипломат»	Здравоохранение и спорт	Стоматология
27	Клиника профессора Асымбековой	Здравоохранение и спорт	Медцентр
28	Клиника профессора Балтабаева	Здравоохранение и спорт	Медцентр
29	«Кортекс»	Здравоохранение и спорт	Медцентр
30	Лаборатория Бонецкого	Здравоохранение и спорт	Частная лаборатория
31	Медицинский центр КГМА	Здравоохранение и спорт	Медцентр
32	«Неман»	Здравоохранение и спорт	Фармацевтика
33	«Неомед»	Здравоохранение и спорт	Медцентр
34	Сеть аптек «Лекарь»	Здравоохранение и спорт	Фармацевтика
35	«Эдельвейс»	Здравоохранение и спорт	Медцентр
36	«Юнит-реактив-фарма»	Здравоохранение и спорт	Медцентр
37	«Юрфа»	Здравоохранение и спорт	Медцентр
38	Aqua Lab	Здравоохранение и спорт	Частная лаборатория
39	Change	Здравоохранение и спорт	Тренажерный зал
40	Dasmia Fitness	Здравоохранение и спорт	Тренажерный зал

41	Europeasia	Здравоохранение и спорт	Медцентр
42	Invitro	Здравоохранение и спорт	Медцентр
43	K-med	Здравоохранение и спорт	Медцентр
44	Medcenter Kg	Здравоохранение и спорт	Медцентр
45	Medik Kg	Здравоохранение и спорт	Медсервис
46	On Clinic	Здравоохранение и спорт	Медцентр
47	Prime Clinic	Здравоохранение и спорт	Медцентр
48	Pulse	Здравоохранение и спорт	Тренажерный зал
49	Viva Clinic	Здравоохранение и спорт	Медцентр
50	«Кто есть кто»	Медиаиндустрия	Онлайн-издание
51	«Намба»	Медиаиндустрия	Медиаресурсы
52	Akipress Сводка	Медиаиндустрия	Информационное агентство
53	Akipress Tazabek Kg	Медиаиндустрия	Информационное агентство
54	Akipress Zdorovie	Медиаиндустрия	Информационное агентство
55	Online Cinema	Медиаиндустрия	Медиаресурсы
56	Super.Kg	Медиаиндустрия	Информационное агентство
57	«Бамбини»	Образование	Частный садик
58	«Илим»	Образование	Частная школа
59	«Келечек Mit»	Образование	Частный садик
60	«Таберик»	Образование	Частный садик
61	Abiturient	Образование	Частная школа
62	Attractor	Образование	Курсы
63	Bilimkana Auca High School	Образование	Частная школа
64	Bilimkana Chinese School/American School/European School	Образование	Частная школа
65	Bishkek International School	Образование	Частная школа
66	Codify lab	Образование	Курсы
67	DevIT При Ауца	Образование	Курсы

68	It-academy Kg	Образование	Курсы
69	Oxford	Образование	Частная школа
70	Redmouse	Образование	Курсы
71	Secom	Образование	Курсы
72	Silk-road	Образование	Частная школа
73	«Бублик»	Питание	Кофейня
74	«Золотой дракон»	Питание и проживание	Гостиница
75	«Империя пиццы»	Питание	Еда на вынос
76	«Нават»	Питание	Еда на вынос
77	«Наша марка»	Питание	Кондитерская
78	Assorti Project	Питание	Еда на вынос
79	Vambook	Питание	Еда на вынос
80	Parajohns	Питание	Ресторан
81	Torro Grill & Bar	Питание	Ресторан
82	«Абдыш-ата»	Промышленность	Пищевая промышленность
83	«Автомаш-радиатор»	Промышленность	Машиностроение и металлообработка
84	«Ак-бата»	Промышленность	Пищевая промышленность
85	«Алия»	Промышленность	Легкая промышленность
86	«Алтын-ажыдаар»	Промышленность	Лесная, деревообрабатывающая и целлюлозно-бумажная промышленность
87	«Аю»	Промышленность	Пищевая промышленность
88	«Биовит»	Промышленность	Медицинская промышленность
89	«Газпром»	Промышленность	Топливная промышленность
90	«Келечек»	Промышленность	Пищевая промышленность
91	«Куликовский торт»	Промышленность	Пищевая промышленность
92	«Кумтор Голд Компани»	Промышленность	Нефтеперерабатывающая промышленность
93	«Кыргыз Бетон»	Промышленность	Промышленность строительных материалов
94	«Кыргыз коньягы»	Промышленность	Пищевая промышленность

95	«Кыргызмебель»	Промышленность	Легкая промышленность
96	«Наши окна»	Промышленность	Легкая промышленность
97	«Оско»	Промышленность	Пищевая промышленность
98	«Резби»	Промышленность	Легкая промышленность
99	«Силикат»	Промышленность	Легкая промышленность
100	«Сладости Востока»	Промышленность	Пищевая промышленность
101	Столичный вино-водочный завод	Промышленность	Пищевая промышленность
102	«Текстиль Транс»	Промышленность	Легкая промышленность
103	Трубно-шиферное производство	Промышленность	Промышленность строительных материалов
104	«Уни Пласт»	Промышленность	Легкая промышленность
105	«Учкун»	Промышленность	Полиграфическая промышленность
106	«Шоро»	Промышленность	Пищевая промышленность
107	«Памир»	Сельское хозяйство	
108	«Аалам Строй»	Строительство	Строительная компания
109	«Авангард»	Строительство	Строительная компания
110	«Альфа»	Строительство	Строительная компания
111	«Бай Таш Групп»	Строительство	Строительная компания
112	«Имарат Строй»	Строительство	Строительная компания
113	«Елизавета»	Строительство	Строительная компания
114	«Элит Хаус»	Строительство	Строительная компания
115	Borsan	Строительство	Строительная компания
116	Burana Grand	Строительство	Строительная компания
117	Capstroy Kg	Строительство	Строительная компания
118	Emark	Строительство	Строительная компания
119	Family Village	Строительство	Строительная компания
120	Golden Stroy	Строительство	Строительная компания
121	Imarat Progress	Строительство	Строительная компания
122	Kanat Group	Строительство	Строительная компания

123	Kg Group	Строительство	Строительная компания
124	Munara Stroy	Строительство	Строительная компания
125	Premium Development	Строительство	Строительная компания
126	Ts Group	Строительство	Строительная компания
127	«Глобус»	Торговля	Продуктовые магазины
128	«Купи»	Торговля	Интернет-магазин
129	Мах	Торговля	Интернет-магазин
130	«Народный»	Торговля	Продуктовые магазины
131	«Светофор»	Торговля	Интернет-магазин
132	«Технодом»	Торговля	Интернет-магазин
133	«Фрунзе»	Торговля	Продуктовые Магазины
134	«Цветкофф»	Торговля	Интернет-магазин
135	Kivano	Торговля	Интернет-магазин
136	Megashop	Торговля	Интернет-магазин
137	Shisha.Kg	Торговля	Интернет-магазин
138	Sulprak	Торговля	Интернет-магазин
139	Тао.Kg	Торговля	Интернет-магазин
140	«Азияинфо»	Транспорт и связь	Интернет-услуги
141	«Кыргызтелеком»	Транспорт и связь	Интернет-услуги
142	О! («Нур Телеком»)	Транспорт и связь	Мобильный оператор
143	«Трансфер Групп»	Транспорт и связь	Интернет-услуги
144	«Элкат»	Транспорт и связь	Интернет-услуги
145	«Яндекс Такси»	Транспорт и связь	Услуги такси
146	Aknet	Транспорт и связь	Интернет-услуги
147	Beeline («Скай Мобайл»)	Транспорт и связь	Мобильный оператор
148	Camex Kg	Транспорт и связь	Международные перевозки
149	E-posylka	Транспорт и связь	Международные перевозки
150	Homeline	Транспорт и связь	Интернет-услуги

151	Megacom («Альфа Телеком»)	Транспорт и связь	Мобильный оператор
152	Megaline	Транспорт и связь	Интернет-услуги
153	Saima Telecom	Транспорт и связь	Интернет-услуги
154	«Банк Азии»	Финансы и страхование	Банк
155	Банк «Компаньон»	Финансы и страхование	Банк
156	Кыргызско-швейцарский банк	Финансы и страхование	Банк
157	«Финка Банк»	Финансы и страхование	Банк
158	«Айыл Банк»	Финансы и страхование	Банк
159	«Бакай Банк»	Финансы и страхование	Банк
160	«Дос-Кредобанк»	Финансы и страхование	Банк
161	«Керемет Банк»	Финансы и страхование	Банк
162	Коммерческий банк «Кыргызстан»	Финансы и страхование	Банк
163	«Оптима Банк»	Финансы и страхование	Банк
164	«РСК Банк»	Финансы и страхование	Банк
165	«Финанскредитбанк»	Финансы и страхование	Банк
166	Банк «Бай-Тушум»	Финансы и страхование	Банк
167	Gazprom	Энергетическая компания	Энергетическая компания
168	Geektech	Образование	Курсы
169	Кыргызский инвестиционно-кредитный банк	Финансы и страхование	Банк
170	«Экоисламикбанк»	Финансы и страхование	Банк
171	«Толубай»	Финансы и страхование	Банк
172	Евразийский сберегательный банк	Финансы и страхование	Банк
173	«Кыргызкоммерцбанк»	Финансы и страхование	Банк
174	«Демир Кыргыз Интернэшнл Банк»	Финансы и страхование	Банк

Приложение Б. Анализ Политик по защите персональных данных

№	Наименования
1	<a href="#">Optimabank</a>
2	<a href="#">ООО «Скай Мобайл»</a>
3	<a href="#">GLOVO</a>
4	<a href="#">lalafo</a>
5	<a href="#">Navat</a>
6	<a href="#">ОсОО «АЗИЯИНФО»</a>
7	<a href="#">«КУЛИКОВСКИЙ»</a>
8	<a href="#">ОсОО «Технодом Оператор»</a>
9	<a href="#">«Дос-Кредобанк»</a>
10	<a href="#">Papajohns</a>
11	<a href="#">shisha.kg</a>
12	<a href="#">o.kg</a>
13	<a href="#">Namba food</a>
14	<a href="#">ОсОО «Газпром нефть Азия»</a>
15	<a href="#">«Предприниматель»</a>
16	<a href="#">KUPI.KG</a>
17	<a href="#">SVETOFOR</a>

## Приложение В. Сравнение фактически собираемых данных и Политики ОсОО «Технодом Оператор»

### 2. Предмет политики конфиденциальности

2.1. Настоящая Политика конфиденциальности устанавливает обязательства Продавца по неразглашению и обеспечению режима защиты конфиденциальности персональных данных, которые Покупатель предоставляет по запросу Продавца при регистрации на сайте Интернет-магазина и/или при оформлении заказа для приобретения товара.

2.2. Персональные данные, разрешённые к обработке в рамках настоящей Политики конфиденциальности, предоставляются Покупателем путём заполнения регистрационной формы на сайте Интернет-магазина и включают в себя следующую информацию:

2.2.1. фамилию, имя, отчество (отчество – по желанию) Покупателя;

2.2.2. контактный телефон Покупателя;

2.2.3. адрес электронной почты (e-mail);

2.2.4. адрес доставки Товара;

2.2.5. место жительства Покупателя.

2.3. Любая иная персональная информация неоговоренная выше (история покупок, используемые браузеры и операционные системы и т.д.) также подлежит надежному хранению и нераспространению, за исключением случаев, предусмотренных в п.4.3. и п.4.4. настоящей Политики конфиденциальности.

Выдержка из Политики по конфиденциальности ПД<sup>75</sup>.

---

<sup>75</sup> <https://www.technodom.kg/confidentiality>

## Заполнение анкеты

Поля анкеты, помеченные знаком \*, обязательны к заполнению!

Своей подписью я подтверждаю, что ознакомлен и согласен с правилами клубной программы «Технобонус». Я разрешаю компании ОсОО «Технодом Оператор» направлять мне корреспонденцию на указанный мною почтовый адрес, адрес электронной почты и/или на номер предоставленного мной телефона, включая информацию о проводимых компанией ОсОО «Технодом Оператор» и ее партнерами рекламных кампаниях, а так же пересылать подарки или призы. Так же, в целях реализации клубной программы «Технобонус», я разрешаю компании ОсОО «Технодом Оператор» и ее уполномоченными представителями получать, собирать, хранить и использовать мои персональные данные: фамилию, имя, отчество, дату рождения, почтовый адрес, мобильные телефоны, адрес почтовой почты. В любой момент согласие может быть мной отозвано путем направления уведомления на электронную почту [bonuskg@technodom.kg](mailto:bonuskg@technodom.kg).

Я согласен(на) \*

Номер вашей карты \*

Получить новую виртуальную бонусную карту

### Персональные данные

Обращение \*

Фамилия \*

Имя \*

Отчество

Дата рождения \*

ИИН

Удостоверение личности

Способ коммуникации

Язык обслуживания

В браке

Дети

ОТПРАВИТЬ

### Контактная информация

Домашний телефон

Мобильный телефон \*

Электронная почта

Область

Район

Город \*

Улица

Дом

Квартира

Фактически собираемые данные<sup>76</sup>

<sup>76</sup> <https://www.technodom.kg/technobonusform>

## Приложение Г. Критерии независимости уполномоченного органа

	Факторы	Парижское соглашение	EU/A29	CoE	ECOWAS	C'wealth	IDPPCC	AFAPD	Stewart	GDPR	ICDPPC
1	Утвержден законодательными актами	✓	✓			✓	✓	✓	✓	✓	✓
2	Независимость прописана в законе	✓	✓	✓			✓	✓	✓	✓	✓
3	Фиксированный срок полномочий руководителя	✓				✓	✓	✓	✓	✓	✓
4	Расписан порядок увольнения руководителя/членов					✓	✓	✓	✓	✓	✓
5	Иммунитет от исков					✓	✓	✓	✓	✓	✓
6	Назначается законодательной ветвью власти									*	
7	Адекватность ресурсов	✓				✓	✓	✓	✓	✓	✓
8	Отчитывается перед парламентом и/или обществом		✓	✓		✓	✓		✓	✓	✓
9	Положительная квалификация	✓			✓		✓	✓	✓	✓	✓
10	Запрет на одновременное занятие других позиций	✓			✓	✓		✓			
11	Запрет/раскрытие конфликтов				✓	✓		✓	✓	✓	✓
12	Право на апелляцию на решения уполномоченного органа		✓	✓		✓		✓		✓	

Таблица факторов независимости уполномоченного органа по защите ПД<sup>77</sup>

<sup>77</sup> При составлении таблицы использовались данные Greenleaf, G., 2012. Independence of data privacy authorities (Part I) и адаптированы путем добавления GDPR и ICDPPC. [https://globalprivacyassembly.org/wp-content/uploads/2019/12/ICDPPC-Background-document-on-independence-criteria\\_post-Coe-comment.pdf](https://globalprivacyassembly.org/wp-content/uploads/2019/12/ICDPPC-Background-document-on-independence-criteria_post-Coe-comment.pdf)