

Защита персональных данных в Кыргызской Республике

В связи с развитием технологий и количеством информации, генерируемой на ежедневной основе, множество стран придают важную роль защите персональных данных и конфиденциальной информации в целом. Одни страны придерживаются принципа защиты данных на национальном уровне и всевозможного ограничения распространения любой информации. В то время как другие страны верят в то, что информация является критически важным фактором в развитии мировой экономики и глобального процветания, и, тем самым, отменяют положения, ограничивающие трансграничную передачу данных.

Давайте рассмотрим ситуацию с защитой персональных данных в нашей стране. Конституцией Кыргызской Республики закреплено право каждого человека на неприкосновенность личной жизни, а именно запрет сбора, хранения, использования и распространения конфиденциальной информации и информации о частной жизни человека без его согласия. В 2008 году был принят Закон “Об информации персонального характера” No. 58 от 14.04.2008 (далее по тексту «Закон о персональных данных»), направленный на правовое регулирование работы с персональными данными (далее по тексту “ПД”). Также Кыргызстан является страной-участницей Международных соглашений, в соответствии с которыми законодатель установил спектр прав и обязанностей собственника, держателя, третьих лиц и уполномоченного государственного органа, обеспечивающего защиту ПД. Однако несмотря на наличие законодательства в данной сфере, на практике отсутствует эффективный механизм защиты ПД, и требуется доработка ряда процедурных моментов, а также создание механизма надзора за соответствием сбора, обработки, хранения и защиты ПД, процедуры обжалования неправомерных действий держателей данных и системы санкций за нарушение установленных требований.

По нашему мнению для обеспечения полной защиты ПД государство должно направить свои силы на три основных сектора:

- 1) информационно-образовательная деятельность субъектов ПД;
- 2) создание и усиление полномочий государственного уполномоченного органа по защите прав субъектов ПД;
- 3) активное проведение работы по защите данных посредством уполномоченного государственного органа.

Основным фактором системного нарушения законодательства в области ПД является недостаточный уровень информированности граждан о своих правах. Граждане, ставшие жертвами нарушений законодательства в сфере защиты ПД, зачастую не предпринимают никаких действий. Бездействие граждан часто связано с тем, что в настоящее время люди не осознают опасность разглашения ПД или не знают, какие действия можно предпринять в таких случаях, какой орган регулирует защиту ПД и какие гарантии предоставляет государство. Соответственно одними из основных задач государства должны быть повышение правовой грамотности населения, пропаганда

бережного отношения к личным данным, а также повышение уровня взаимодействия участников данных правоотношений, т.е. государства, держателей и граждан. Субъекты персональных данных должны быть осведомлены о системных нарушениях, мерах наказаний за сбор избыточных сведений и других неправомерных действий в сфере ПД. Для обеспечения эффективности защиты ПД государство должно разработать рекомендации по ведению прозрачной работы с данными, приведению внутренних документов держателей данных в соответствие с требованиями законодательства, разработать инструкции и методологии для правильного сбора, обработки и хранения ПД. Законом о персональных данных предусмотрена обязанность держателя данных определять обработчика для обработки ПД, предоставляющего гарантии в отношении мер технической безопасности и организационных мер, регулирующих обработку ПД, за исключением случаев, когда держатель самостоятельно возлагает на себя функции и обязанности обработчика.¹ Однако на практике держатели не выполняют данную обязанность в связи с тем, что отсутствуют инструкции по мерам технической безопасности, которые должны быть соблюдены держателями данных при сборе, обработке, хранении и защите данных, а также в связи с отсутствием надзорного органа, регулирующего соблюдение таких мер. Законодательство Кыргызской Республики в сфере защиты персональных данных состоит лишь из Закона о персональных данных и вышеуказанной нормы в Конституции Кыргызской Республики.

Согласно Закону о персональных данных, в Кыргызской Республике действует уполномоченный государственный орган в сфере защиты ПД (далее по тексту «Уполномоченный орган»), на который возложены функции по регистрации держателей массива ПД, ведению Реестра держателей и другие функции, предусмотренные настоящим Законом. Статья 18 Закона о персональных данных предусматривает, что юридические лица имеют право на работу с ПД только после регистрации в уполномоченном органе. Держатель ПД и обработчик обязаны обеспечивать охрану данных во избежание несанкционированного доступа, блокирования, передачи, а равно их случайного или несанкционированного уничтожения, изменения или утраты.²

Также согласно вышеуказанному Закону, настоящий уполномоченный орган осуществляет роль надзорного органа и в случае выявления недостоверности данных или неправомерности действий, субъект ПД вправе подать заявление в уполномоченный орган. Однако Правительством Кыргызской Республики не был утвержден такой орган и, следовательно, на практике держатели ПД не регистрируются в качестве держателей данных, не публикуются в Реестре держателей данных и нарушения в сфере защиты ПД остаются безнаказанными.

В то же время во множестве европейских стран действует офис комиссара по защите персональных данных, который обеспечивает соблюдение прав собственников ПД и проводит проверки по мере поступления жалоб. В Великобритании таким органом является орган защиты данных, руководство деятельностью которого осуществляет

¹ Закон Кыргызской Республики “Об информации персонального характера” 2008, No. 58, статья 17

² Закон Кыргызской Республики “Об информации персонального характера” 2008, No. 58, статья 6

Управление Комиссара по информации (ICO).³ В полномочия настоящего органа входит проверка государственных ведомств, частных лиц, а также организаций частного сектора и в случае выявления нарушений, данный орган вправе наложить штраф в зависимости от степени тяжести нарушения или передать дело для уголовного разбирательства. В Королевстве Бельгии вышеописанными полномочиями обладает Комиссия по защите неприкосновенности частной жизни, Омбудсмен по защите данных (Tietosuojavaltuutettu) является надзорным органом в Финляндии, а в Германии в каждой отдельной федеральной земле имеется орган по защите данных, который несет ответственность за соблюдение законодательства в сфере защиты данных.⁴ Вышеперечисленные органы осуществляют не только надзор, но также повышают правосознание физических лиц и организаций в сфере защиты данных и разрабатывают технические и организационные меры по защите этих данных. В других странах за пределами Европы за последние пять лет произошли существенные законодательные изменения, включая страны Азии и СНГ. Наиболее заметные сдвиги заметны в Сингапуре, где существует Комиссия по защите персональных данных, в функции которой входит: разработка и реализация политики и соответствующих положений в сфере защиты ПД, обеспечивающий баланс между необходимостью ограничения сбора и защиты данных физических лиц и потребности организаций в использовании ПД; разработка инструкций для держателей ПД; рассмотрение дел и выдача соответствующих решений и указаний; представление государства на международном уровне; а также ведение образовательной и информационно-пропагандистской деятельности для организаций и физических лиц.⁵ В свою очередь в 2006 году в Российской Федерации был принят Федеральный Закон «О персональных данных» и уже в 2008 был утвержден уполномоченный орган по защите прав субъектов персональных данных. На данный момент в Российской Федерации уполномоченным органом в сфере защиты ПД является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, а именно Управление по защите прав субъектов персональных данных. Данное Управление осуществляет функции контроля и надзора за соответствием обработки ПД, рассмотрения жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой ПД. В 2015 году Управление по защите прав субъектов провело 805 проверок в отношении держателей ПД, в ходе которых были выявлены 1188 нарушений.⁶

С повседневным развитием технологии и электронной коммерции организациям открывается возможность выходить на международный рынок и, несмотря на географические ограничения, предлагать и поставлять свои товары и услуги широкому

кругу клиентов. Однако для того, чтобы функционировать на международном рынке, предприятиям необходим надежный и непрерывный доступ к данным, где бы такая

³ Getting the Deal Through, “Data Protection & Privacy 2015,” (London: 2015): 202

⁴ DLA Piper, “Data Protection Laws of the World”: 41, 132, 146

⁵ Personal Data Protection Commission Singapore, последнее обновление от 29.02.2016, <https://www.pdpc.gov.sg/about-us/what-we-do>

⁶ “ComNews: На персональные данные прольется свет”, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, последнее изменение 11 ноября 2015 года, <https://rkn.gov.ru/press/publications/news35923.htm>

информация ни находилась. Существует такое мнение, что если страны не будут придерживаться принципа локализации данных, то это даст толчок представителям большого, среднего и малого бизнеса функционировать на международном рынке, что означает, что свободная трансграничная передача данных способствует развитию экономики каждой отдельной страны и мировой экономики в целом. Данный факт является причиной тому, что настоящий вопрос поднимается на международном уровне, обсуждается бизнес сообществами, и многие страны начинают проводить реформы в законодательстве. К примеру, в Соединенных Штатах Америки (далее по тексту “США”) законодательство не содержит ограничения на передачу данных через границу и позволяет организациям хранить и перемещать, как корпоративные данные организации, так и ПД сотрудников, обеспечивая адекватную защиту таких данных. Тогда как во многих странах Европы трансграничная передача данных за пределы Европейского Союза запрещена, кроме случаев когда такая страна обеспечивает адекватную защиту ПД или если собственник ПД дал свое письменное согласие на передачу данных. В нашей стране, так же как и в Российской Федерации трансграничная передача ПД возможна, если держатель массива ПД, передающий данные, исходит из наличия международного договора между сторонами, согласно которому получающая сторона должна обеспечить адекватный уровень защиты прав и свобод субъектов ПД и охраны ПД.⁷ Однако возникает вопрос, что значит “адекватный уровень защиты” и кто обязан определять обеспечивает ли иностранное государство адекватный уровень защиты прав и свобод субъектов ПД? Практика Российской Федерации показывает, что под странами обеспечивающими адекватную защиту, понимаются страны, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных No. 108 от 28.01.1981, а также иностранные государства, перечень которых установил Роскомнадзор. Однако в нашей стране данный вопрос остается открытым так, как невозможно определить какой уровень защиты предоставляет та или иная страна и на практике держатели ПД самостоятельно определяют возможна ли передача данных. Соответственно разумно включить в обязанности уполномоченного органа определять круг стран, обеспечивающих адекватный уровень защиты ПД и обязать держателей ПД письменно уведомлять уполномоченный орган о передаче данных, отражать такую передачу во внутренних документах, и в случае согласия собственника на передачу ПД получать такое согласие в письменном виде.

В целях обеспечения защиты ПД и надзора за деятельностью держателей данных считаем, что Кыргызская Республика должна утвердить уполномоченный орган или возложить обязанности такого органа на существующий институт, что обеспечит контроль держателей данных при сборе, обработке, хранении и защите данных. Должны быть разработаны так же методологические рекомендации по работе самого органа, а именно рекомендации по ведению реестра держателей данных, порядку организации и проведения государственного контроля над соответствием сбора, обработки, хранения и защиты ПД, по предупреждению и выявлению нарушений, а также система санкций за нарушение законодательства в сфере защиты ПД. В свою очередь, уполномоченный орган

⁷ Закон Кыргызской Республики “Об информации персонального характера” 2008, No. 58, статья 25

должен установить доступную для общества процедуру обжалования неправомерных действий субъектов ПД, а также систему санкций за нарушение установленных требований. Для того чтобы деятельность данного органа была прозрачной, на основании жалоб заявителей и системных нарушений, настоящий орган должен проводить ежегодный анализ, разрабатывать и публиковать дальнейшую стратегию работы органа и тем самым обеспечивать стабильность общего состояния защиты прав субъектов ПД.