**1. Если есть программное-обеспечение которое затрагивает перс.данных с разрешения самих иностранцев (не граждан РК), но деятельность может "затронуть" граждан РК. В таких случаях каждой компании владельцу ПО - будет необходимо создавать представительство и размещать базу данных на территории РК?**

В соответствии с пунктом 2 статьи 12 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (далее «**ЗПД**») хранение персональных данных осуществляется собственником и (или) оператором, а также третьим лицом в базе, находящейся на [территории Республики Казахстан](https://online.zakon.kz/Document/?link_id=1004947983). Срок хранения персональных данных определяется датой достижения целей их сбора и обработки, если иное не предусмотрено законодательством Республики Казахстан.

На основании пункта 1 статьи 25 ЗПД собственник и (или) оператор вправе собирать и обрабатывать персональные данные B порядке, установленном законодательством Республики Казахстан. Также согласно пункту 1 статьи 48 Закона Республики Казахстан от 6 апреля 2016 года № 480-V ЗРК «О правовых актах», действие Нормативных правовых актов Республики Казахстан распространяется на граждан и юридических лиц Республики Казахстан, а также на иностранных граждан и лиц без гражданства, находящихся на ее территории, и на юридические лица иностранных государств, включая их филиалы и представительства, только в случаях, прямо предусмотренных законодательными актами или международными договорами, ратифицированными Республикой Казахстан.

При этом в ЗПД отсутствуют прямые указания на необходимость соблюдения его требований иностранными юридическими лицами, не имеющими «правового» присутствия на территории Казахстана (дочерняя компания/филиал/представительство).

Следовательно, если иностранное юридическое лицо (оператор) не имеет физического присутствия в Республике Казахстан (в виде филиала или представительства) и не действует в рамках ратифицированных международных договоров, то требования законодательства Республики Казахстан, включая положения ЗПД, не распространяются на него.

Таким образом, мы полагаем, что если иностранная компания, владеющая иностранным программным обеспечением, обрабатывает персональные данные иностранных граждан с их согласия (при этом потенциально затрагивает интересы граждан Казахстана путем сбора и обработки их персональных данных), не имеет представительства в Казахстане и не осуществляет сбор и обработку персональных данных на территории Республики Казахстан, то ей не требуется размещать базу данных на территории Республики Казахстан ввиду неприменимости норм ЗПД к иностранным юридическим лицам, если такое лицо не действует в качестве третьего лица на территории Республики Казахстан.

**2. Онлайн-площадка - можно ли считать каждый интернет-ресурс, где выкладывают товары на продажу?**

Согласно пункту 58) статьи 1 Закона Республики Казахстан от 12 апреля 2004 года № 544-II «О регулировании торговой деятельности» (далее «**ЗТД**»), электронная торговая площадка определяется как интернет-ресурс, который предоставляет инфраструктуру участникам электронной торговли и поддерживает заключение договоров между ними с использованием информационно-коммуникационных технологий. Это определение предполагает, что для признания интернет-ресурса электронной торговой площадкой он должен предоставлять функционал, позволяющий не только размещать товары, но и обеспечивать весь процесс электронной торговли.

Пунктом 2-1. статьи 29-1 ЗТД устанавливается ряд обязательных требований к функционированию (инфраструктуре) электронной торговой площадки. Эти требования включают:

1) внутреннее требование электронной торговой площадки к участникам электронной торговли;

2) возможность безналичного расчета за товар, работы и услуги с использованием банковских платежных систем;

3) организация или координация доставки товара или услуги;

4) обеспечение взаиморасчетов между покупателем и продавцом, в том числе при возврате товара;

5) предоставление возможности совершения договора купли-продажи, договора об оказании услуг посредством информационно-коммуникационных технологий путем обмена электронными документами или электронными сообщениями.

Таким образом, мы полагаем, что интернет-ресурс не предоставляющий возможность выкладывать товары на продажу и не выполняет вышеперечисленных функций, он не считается полноценной электронной торговой площадкой в рамках Казахстанского Законодательства.

**3. В банковских приложениях, ПО, которые могут затрагивать персональные данные торговцев - телефон, фамилию и имя.**

В соответствии с пунктом 1 статьи 15 ЗПД, распространение персональных данных возможно только при наличии согласия самого субъекта персональных данных или его законного представителя, и только в тех случаях, когда при этом не нарушаются законные интересы других физических и юридических лиц. Так, пунктом 2 статьи 15 ЗПД предусматривается, что распространение персональных данных в случаях, выходящих за рамки ранее заявленных целей их сбора, осуществляется с согласия субъекта или его законного представителя. Пункт 2 статьи 20 ЗПД требует, чтобы сбор и обработка персональных данных осуществлялись при обеспечении их защиты. А согласно статье 11 ЗПД, собственники и (или) операторы, а также третьи лица, получающие доступ к персональным данным ограниченного доступа, обеспечивают их конфиденциальность путем соблюдения требований не допускать их распространения без согласия субъекта или его законного представителя либо наличия иного законного основания. Лица же, которым стали известны персональные данные ограниченного доступа в связи с профессиональной, служебной необходимостью, а также трудовыми отношениями, обязаны обеспечивать их конфиденциальность.

Таким образом, при использовании персональных данных торговцев соблюдение конфиденциальности и получения согласия является обязательным. При отсутствии такого согласия передача данных будет нарушением ЗПД.

**4. Компания заключила договор на использование баз данных (типа компры, адаты). Как правило, них содержится информация, как ограниченного доступа, так и для общего доступа. Специалисты внутри безопасности компании проверяют как сотрудников, так и потенциальных подрядчиков, третьих лиц. Ваше мнение по данному вопросу в соответствии с ЗПД.**

Согласно статье 6 ЗПД персональные данные подразделяются на общедоступные и ограниченного доступа. Под общедоступными данными понимаются те, для которых в соответствии с законами Республики Казахстан не распространяются требования соблюдения конфиденциальности, и доступ к которым является свободным с согласия субъекта. Персональными данными ограниченного доступа являются персональные данные, доступ к которым ограничен законодательством Республики Казахстан. Например, статьей 8 Закона Республики Казахстан от 30 декабря 2016 года № 40-VI «О дактилоскопической и геномной регистрации».

В соответствии со статьей 14 ЗПД, обработка персональных данных должна осуществляться в соответствии с целями их изначального сбора. При этом допускается повторный сбор, обработка и распространение третьими лицами персональных данных, опубликованных в общедоступных источниках при наличии согласия субъекта или его законного представителя и при условии наличия ссылки на источник информации в соответствии со статьей 7 ЗПД.

Таким образом, мы полагаем, что данные полученные при помощи платформ, которые собирают и систематизируют данные из открытых источников, могут быть использованы без нарушения конфиденциальности при условии, что их сбор и обработка соответствуют заявленным целям и получены в рамках законодательства.

**5. Можно ли передавать ПД третьим лицам, которые будут иметь доступ к базе данных, при том, что они не являются сотрудниками нашей компании? Общая БД для HR-специалистов, только специалисты из разных компаний, в том числе и иностранных.**

Также согласно 20 ЗПД сбор и обработка персональных данных осуществляются только в случаях обеспечения их защиты. В соответствии со статьей 15 ЗПД, распространение персональных данных допустимо только с согласия субъекта данных или его законного представителя. Это означает, что передача данных HR-специалистам из других компаний должна осуществляться в рамках согласованных и заявленных целей, на которые субъект данных дал своё согласие.

Также важно учитывать, что согласно статье 22 ЗПД собственник и (или) оператор, а также третье лицо обязаны принимать необходимые меры по защите персональных данных:

1) предотвращать несанкционированный доступ к персональным данным;

2) своевременно обнаруживать факт несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить;

3) минимизировать неблагоприятные последствия несанкционированного доступа к персональным данным;

4) предоставлять доступ государственной технической службе к объектам информатизации, использующим, хранящим, обрабатывающим и распространяющим персональные данные ограниченного доступа, содержащиеся в электронных информационных ресурсах, для осуществления обследования обеспечения защищенности процессов хранения, обработки и распространения персональных данных ограниченного доступа, содержащихся в электронных информационных ресурсах в порядке, определяемом уполномоченным органом;

5) вести регистрацию и учет действий, предусмотренных подпунктами 3), 4), 5) и 6) пункта 4 статьи 8 ЗПД.

Данные обязательства действуют с момента сбора персональных данных и продолжаются до их уничтожения или обезличивания.

Таким образом, мы полагаем, что передача персональных данных третьим лицам допускается при наличии согласия субъекта персональных данных. Также такая передача должна соответствовать целям, заявленным при сборе данных, и происходить при условии обеспечения защиты и конфиденциальности персональных данных.

**6. Можно ли использовать иностранное ПО, которое находится за пределами РК еще и без договора? (есть компания плательщик, договор будет заключен с ним) все сервера будут находиться за пределами РК. Согласия сотрудников на обработку ПД имеется.**

Согласно статье 12 ЗПД, накопление персональных данных должно производиться только в целях, необходимых для выполнения задач, осуществляемых собственником и (или) оператором, а также третьими лицами. При этом хранение персональных данных должно осуществляться на территории Республики Казахстан, если иное не предусмотрено законодательством Казахстана. Если персональные данные обрабатываются лицом, подпадающим под юрисдикцию Казахстана, с использованием иностранного ПО, то важно, чтобы сервера, на которых данные хранятся, находились на территории Казахстана.

Статья 16 ЗПД устанавливает, что трансграничная передача персональных данных за пределы Республики Казахстан возможна, если страна, в которую передаются данные, обеспечивает защиту персональных данных. Если же страна не обеспечивает должную защиту, то трансграничная передача данных может быть осуществлена в следующих случаях:

1) наличия согласия субъекта или его законного представителя на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами, ратифицированными Республикой Казахстан;

3) предусмотренных законами Республики Казахстан, если это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека и гражданина, здоровья и нравственности населения;

4) защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно.

Таким образом, мы полагаем, что Казахстанским оператором не запрещено использование иностранного ПО, находящегося за пределами Республики Казахстан, при условии, что первоначальная база была создана на территории Казахстана, а последующая трансграничная передача персональных данных осуществляется в соответствии с требованиями ЗПД.

**7. Благодарим за информацию! То есть мы правильно понимаем, что под трансграничной передачей данных подразумевается и их хранение за границей зарубежным юридическим лицом?**

Согласно статье 16 ЗПД, при трансграничной передаче персональных данных, передача производится на территорию иностранных государств. Трансграничная передача персональных данных осуществляется только в случае обеспечения иностранными государствами защиты персональных данных. Трансграничная передача персональных данных на территорию иностранных государств может быть запрещена или ограничена законами Республики Казахстан.

Накопление персональных данных производится путем сбора персональных данных, необходимых и достаточных для выполнения задач, осуществляемых собственником и (или) оператором, а также третьим лицом. Согласно статье 12 ЗПД хранение персональных данных осуществляется собственником и (или) оператором, а также третьим лицом в базе, находящейся на территории Республики Казахстан. Срок хранения персональных данных определяется датой достижения целей их сбора и обработки, если иное не предусмотрено законодательством Республики Казахстан.

Таким образом, мы полагаем, что под трансграничной передачей данных также подразумевается и их хранение, в том числе и за пределами Республики Казахстан.

**8. Прошу рассказать про требования регулятора в вопросе средств криптографической защиты информации по стандарту СТ РК 1073-2007 для шифрования Персональных данных ограниченного доступа. Вопрос как соблюдать данное требование, когда стоимость криптошифрования стоит более 30 млн.тг, а несоблюдение данного требования карается штрафом в 200 мрт (при утечки БД ПД). Как соблюдать данные требования малому и среднему бизнесу.**

Персональные данные подразделяются на общедоступные и ограниченного доступа. Согласно со статьей 6 ЗПД под общедоступными данными понимаются те, для которых в соответствии с законами Республики Казахстан не распространяются требования соблюдения конфиденциальности, доступ к которым является свободным с согласия субъекта. Персональными данными ограниченного доступа являются персональные данные, доступ к которым ограничен законодательством Республики Казахстан. Например, статья 8 Закона Республики Казахстан от 30 декабря 2016 года № 40-VI «О дактилоскопической и геномной регистрации».

Требования к средствам криптографической защиты информации, в частности, по стандарту СТ РК 1073-2007, касаются защиты персональных данных ограниченного доступа. Стандарт СТ РК 1073-2007 обязателен для применения государственными органами и организациями, а также предприятиями, чья деятельность связана с криптографической защитой информации, включая разработку, производство и эксплуатацию средств криптографической защиты информации. Это означает, что стандарт применяется к организациям, которые обрабатывают или защищают персональные данные ограниченного доступа, а не к общедоступным персональным данным.

Таким образом, мы делаем выводы, что СТ РК 1073-2007 применяется только к персональным данным ограниченного доступа и данные требования не применимы к малому и среднему бизнесу.