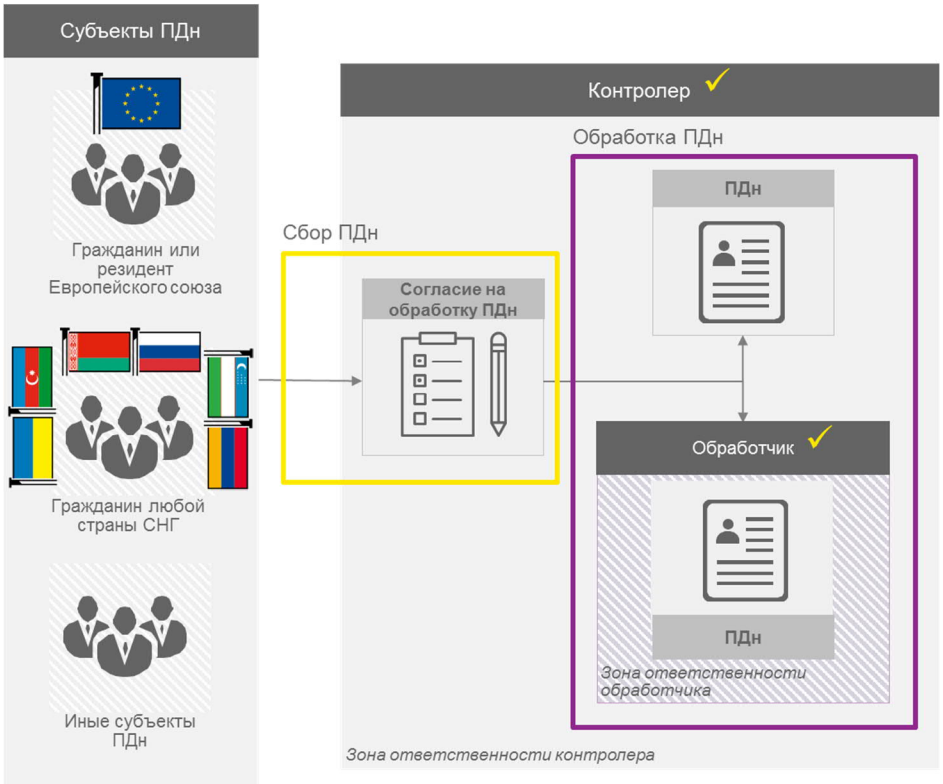
Влияние GDPR на работу компаний-нерезидентов Европейского союза: новый порядок работы с персональными данными

25 мая 2018 года вступил в силу обязательный к применению Общеевропейский регламент о персональных данных Регламент Европейского союза («Регламент» или «GDPR»), направленный на гармонизацию защиты основных прав и свобод физических лиц в отношении обработки данных и обеспечения свободного перемещения персональных данных («ПДн») между государствами-членами Евросоюза. Регламент полностью отменил и заменил собой ранее действующую Директиву № 95/46/EC, лежащую в основе европейского регулирования в сфере персональных данных на протяжении более 20 лет.

В связи с тем, что Регламент представляет собой сложный нормативно-правовой акт с обилием технических правил и экстерриториальным принципом действия, компаниям-нерезидентам Европейского союза, услуги которых, тем не менее, ориентированы на европейский рынок, настоятельно рекомендуется детально проанализировать и тщательно проработать положения Регламента.

ОСНОВНЫЕ ПОНЯТИЯ РЕГЛАМЕНТА

Ниже в схематичном виде представлены действующие лица процесса обработки ПДн согласно терминологии Регламента.



«Контролер» определяет цели и способы обработки ПДн, которую он может осуществлять как самостоятельно, так и с привлечением третьего лица, а «обработчик» обрабатывает ПДн от имени контролера и действует в строгом соответствии с инструкциями контролера.

АНАЛИЗ

1.1 Общий обзор ключевых требований Регламента

Соблюдение прав субъектов ПДн, в частности, информирование субъектов о деталях обработки их ПДн; предоставление доступа к этим данным; исправление и уничтожение указанных данных; соблюдение ограничений обработки указанных данных; обеспечение переносимости данных (то есть право субъекта ПДн получить относящиеся к нему ПДн в структурированном, универсальном и машиночитаемом формате и в дальнейшем беспрепятственно передать их другому контролеру); учет возражений против хранения ПДн, а также против принятия в отношении субъекта решений, которые основаны исключительно на автоматизированной обработке ПДн.

Уведомление надзорного органа об утечке ПДн[1]. В случае утечки ПДн в течение **72 часов**, после того как контролеру стало известно об утечке, контролер должен уведомить об этом компетентный надзорный орган. Необходимо задокументировать любую утечку, а также все относящиеся к утечке факты, последствия утечки и принятые корректирующие меры.

Прозрачность обработки ПДн[2]. Любую информацию о целях, методах и объемах обработки ПДн следует излагать максимально доступно и просто.

Согласие на обработку ПДн[3] должно быть выражено в форме утверждения или в форме четких активных действий субъекта. Согласие на обработку ПДн будет недействительно, если у субъекта не было выбора или не было возможности отозвать свое согласие без ущерба для самого себя.

Передача данных[4]. В соответствии с Регламентом передача ПДн за пределы Европейского союза разрешена только входящим в группу лицам или третьим лицам-контрагентам, находящимся за пределами Европейской экономической зоны, только в том случае, если страна, в которой находится получатель таких ПДн, обеспечивает надлежащий уровень защиты ПДн.

Учетные сведения об обработке данных[5]. Каждый контролер и, если применимо, представитель контролера должны вести учет любой деятельности, связанной с обработкой ПДн, которая находится в сфере его ответственности.

Назначение представителя[6]. Если контролер или обработчик с местом нахождения за пределами Европейского союза обрабатывает ПДн находящихся в Европейском союзе субъектов, и деятельность такого контролера или обработчика по обработке ПДн связана с предложением товаров или услуг или связана с мониторингом активностей субъектов ПДн в Европейском союзе, то контролер или обработчик должен в письменной форме назначить представителя[7]. Вместе с тем, назначение такого представителя не влияет на ответственность контролера или обработчика в соответствии с Регламентом. К лицу, назначенному представителем, могут применяться меры воздействия в случае нарушения контролером или обработчиком требований Регламента.

---

[1] Статья 33 Регламента
[2] Статьи 5, 6, 9, 10, 85 и 89 Регламента
[3] Пункт 32 Преамбулы Регламента, статья 7 Регламента
[4] Статьи 44 – 50 Регламента
[5] Статья 30 Регламента
[6] Статья 27 Регламента
[7] Если только (i) обработка данных не носит эпизодического характера, (ii) не включает обработку в большом объеме специальных категорий ПДн или ПДн, относящихся к приговорам по уголовным статьям или уголовным правонарушениям, (iii) и не должна привести к возникновению риска для прав и свобод физических лиц, принимая во внимание характер, контекст, объем и цели обработки данных, или если контролером является государственное учреждение.

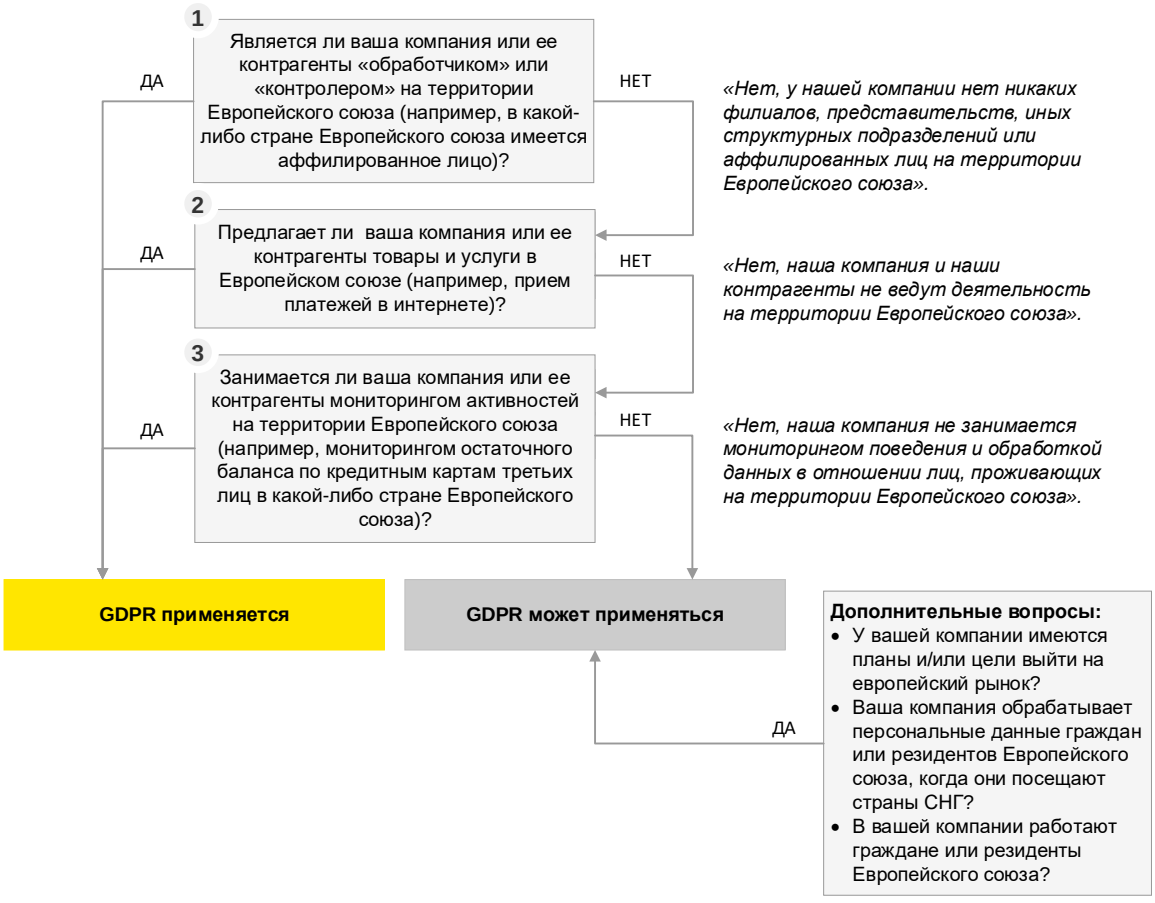
Документальное оформление процесса обработки. Принятие и оформление политики в области защиты и хранения ПДн (включая порядок действий в случае утечки данных), уведомлений об обработке ПДн (в том числе покупателей, клиентов, работников и т.д.), формы согласий субъекта ПДн. Данный перечень не является исчерпывающим.

1.2 Экстерриториальное действие GDPR – применяется в том числе за пределами Европейского союза

По общему правилу действие Регламента распространяется на любые операции по обработке ПДн в контексте присутствия на территории Европейского союза их контролера или обработчика, при этом независимо от места (страны), в которой фактически такая обработка производится.

Однако Регламент также имеет экстерриториальное действие и применяется ко всем компаниям, которые обрабатывают ПДн резидентов и граждан Европейского союза, при этом независимо от территориального местонахождения (регистрации) такой компании и вне зависимости от условий такой обработки.

Ниже в справочных целях приведен алгоритм определения применимости требований Регламента к деятельности компании:



Одним из риск-сценариев может стать, в том числе, наличие веб-сайта, переведенного на один или несколько официальных языков стран-участниц Европейского союза, возможность приема оплаты

услуг в одной из официальных валют Европейского союза, упоминание потребителей или пользователей, которые находятся в Европейском союзе.

Регламент также применяется к обработке ПДн контролером, который расположен за пределами Европейского союза, но находится под юрисдикцией страны-участницы Европейского союза в соответствии с международным правом (например, дипломатическое представительство, консульства) – иными словами, если компания поручила обработку ПДн или передала ПДн на территорию стран-участниц Европейского союза.

Примеры применимости Регламента

В практическом плане GDPR распространяется на любые компании, которые «ориентированы» на рынок стран Европейского союза в качестве потенциального рынка сбыта своей продукции или рынка предоставления услуг. Например, производитель товаров находится (зарегистрирован) в одной из стран СНГ, но реализует продукцию гражданам Европейского союза через интернет-сайт, который имеет версии на европейских языках и позволяет оплачивать банковскими картами приобретаемые через интернет-магазин товары, в том числе в иностранной валюте.

Другим примером может являться наличие у компании, зарегистрированной в одной из стран СНГ, дочернего предприятия на территории страны Европейского союза. Например, казахстанский банк имеет на территории Европейского союза свое дочернее подразделение, которое осуществляет коммерческие операции на территории Европейского союза и с участием граждан Европейского союза. Очевидно, что в таком случае дочернее подразделение казахстанского банка должно соблюдать требования Регламента. Однако если между дочерним подразделением казахстанского банка и казахстанским банком происходит передача ПДн граждан Европейского союза, которые будут обрабатываться и храниться в казахстанском банке, то и сам казахстанский банк также подпадет под требования Регламента.

Еще одним примером является мониторинг активностей субъекта ПДн на территории Европейского союза путем отслеживания геопозиции пользователя через мобильное приложение в целях предложения ему рекламы мероприятий в соответствующей локации. Компания-владелец мобильного приложения будет подпадать под требования Регламента даже в том случае, если она находится (зарегистрирована) за пределами Европейского союза.

1.3 Последствия несоблюдения требований Регламента компаниями-нерезидентами Европейского союза

Меры ответственности

В качестве мер ответственности за нарушение положений Регламента предусмотрены штрафные санкции и иные меры юридического характера, которые могут применяться по отдельности или в совокупности.

В зависимости от типа нарушения Регламент предусматривает два пороговых значения размеров штрафов:

- Штраф до 20 млн евро или до 4% об общего годового оборота (в зависимости от того, какая сумма больше)
- Штраф до 10 млн евро или до 2% об общего годового оборота (в зависимости от того, какая сумма больше)

При определении конечного размера штрафа подлежат учету различные факторы, например, характер, тяжесть и продолжительность правонарушения, меры, предпринятые контролером или обработчиком для смягчения ущерба, полученного субъектами ПДн, а также факты предыдущих нарушений контролера или обработчика.

Следует отметить, что подать жалобу в надзорный орган или обратиться за средством судебной защиты вправе любой субъект ПДн, который сочтет, что его/ее права по Регламенту были нарушены в результате обработки его/ее ПДн.

Ниже приведены некоторые примеры привлечения к ответственности за нарушение положений Регламента:

В ходе проверки деятельности одного лечебного заведения в Португалии был выявлен факт неограниченного доступа персонала к данным пациентов. Лечебное заведение было оштрафовано за внутреннюю политику, которая в недостаточной степени ограничивала доступ к ПДн пациентов. Размер штрафа составил 400 000 евро, однако впоследствии был оспорен.

Немецкая компания была оштрафована на 20 000 евро, когда при расследовании утечки данных в результате хакерской атаки выяснилось, что компания не применяла технические средства защиты (шифрования) данных.

Другая немецкая компания была оштрафована на 50 000 евро за сбор излишних ПДн, которые не требовались для оказания услуг.

Далее, за использование видеонаблюдения и недостаточное уведомление об этом субъектов ПДн была оштрафована австрийская компания на сумму 4 800 евро.

Репутационные риски

Учитывая размеры предусмотренных штрафов за нарушение требований Регламента, случаи их применения с большой долей вероятности привлекут внимание СМИ и, следовательно, повлияют на репутацию компании и отношение к ней, ее продуктам и услугам как текущих, так и потенциальных клиентов и контрагентов. Следовательно, в этой связи компании-резиденты Европейского союза в значительной степени будут мотивированы ориентироваться только на тех иностранных партнеров, которые готовы обеспечить соответствие своих бизнес-процессов требованиям GDPR.

Кроме того, обращаем ваше внимание, что любые решения уполномоченного по защите ПДн находятся в свободном доступе и размещаются на его интернет-сайте в полном объеме.

1.4 Возможное влияние GDPR на национальное законодательство о ПДн в странах СНГ

На страны-участницы Европейского союза возложена обязанность «трансформировать» свое национальное право к требованиям Регламента. Учитывая развитые экономические связи с бизнесом Европейского союза, мы предполагаем, что законодательство о ПДн в странах СНГ возможно пойдет по пути устранения наиболее критичных коллизий между действующими законодательными требованиями и нормами Регламента. При этом, подобная гармонизация может потребовать внесение значительных изменений в национальное законодательство стран СНГ.

В практическом плане для компаний стран СНГ, деятельность которых связана со сферой ПДн, ориентированных на пользователей из и в Европейском союзе, вступивший в силу Регламент означает дополнительное обременение по учету европейского регулирования, наряду с соблюдением требований национального законодательства.

1.5 Рекомендуемый подход компании к GDPR (привлечение заинтересованных сторон: бизнес, ИТ, комплаенс)

GDPR является законодательным актом, который на 75% состоит из технических требований и в этой связи предполагает комплексную перестройку и значительный апгрейд всех систем компании, так или иначе связанных с работой с ПДн.

Для оценки масштаба воздействия требований Регламента на деятельность компании, приводим примерный чек-лист необходимых мероприятий:

- Определение процессов и систем, в которых используются ПДн граждан Европейского союза
- Составление реестра операций и учет всей деятельности, связанной с обработкой ПДн (учетные сведения должны включать в том числе контактные сведения контролера и обработчика, категории ПДн, субъектов ПДн, обработки, сведения о трансграничной передаче, общее описание технических и организационных мер безопасности и т.д.)
- Оценка рисков нарушения конфиденциальности для критичных процессов обработки ПДн
- Оценка несоответствий требованиям Регламента: выявление процессов и систем, требующих изменений для соответствия Регламенту (GAP-анализ / аудит соответствия требованиям Регламента)
- Подготовка программы внедрения Регламента, включающей обзор действующих процедур и документов, касающихся отношений с клиентами, сотрудниками, а также с третьими лицами, с которыми первые могут обмениваться ПДн и (или) предоставлять к ним доступ
- Определение необходимости назначения ответственного за защиту данных и организация внутренней системы управления защитой ПДн

Самостоятельное построение системы защиты ПДн, соответствующей всем требованиям GDPR, потребует существенных финансовых и временных инвестиций. При этом, мероприятия можно проводить как своими силами, так и посредством привлечения третьих лиц (аутсорсинг), что может частично снять нагрузку с компании. Для формирования и реализации технических решений в рамках исполнения требований Регламента целесообразно обращаться к консультантам, имеющим подобный опыт, и международным вендорам, имеющим технологии и сервисы, включая технологии информационной безопасности, защиты конфиденциальности данных и предотвращения их утечек, в наиболее полной мере удовлетворяющие требованиям Регламента. Передача ряда технических функций по обработке ПДн третьему лицу («обработчику» в терминологии Регламента) не освободит от ответственности самого оператора («контролера» в терминологии Регламента), но снизит операционные риски последнего и обеспечит возможность более полного соответствия требованиям Регламента.

Ограничения и использование

Выводы, содержащиеся в настоящем документе, основаны на нашем понимании и интерпретации положений Регламента № 2016/679 Европейского Парламента и Совета Европейского союза, а также опубликованных официальных инструкциях и рекомендациях к нему. Указанные акты могут быть изменены в любой момент времени. Очевидно, что мы не можем предвидеть ни время, ни суть таких изменений, однако в настоящее время мы, тем не менее, не располагаем информацией о подготовке таких изменений, которые могут существенно повлиять на наши выводы.

Мы не будем пересматривать выводы, изложенные в настоящем документе, в случае подобных изменений, если только нам не будет направлено специальное предложение это сделать.

Настоящие комментарии подготовлены исключительно для использования Microsoft Kazakhstan, и никакое другое физическое или юридическое лицо не может на них полагаться.