Российские дочки европейских компаний: нужно ли следовать Общему регламенту по защите персональных данных (GDPR)

10.07.2018 СТАТЬИ

Ковалева Наталья,

Директор направления по правовому обеспечению бизнеса АО СК «Альянс», к.ю.н, LLM

25 мая 2018 года стало очередной вехой в сфере правового регулирования и защиты

персональных данных. Это связано с началом применения Регламента (ЕС) 2016/679 Европейского Парламента и Совета «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ ЕС» (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. 2016. №4.5. P.119/1-119/88), или GDPR.

Ажиотаж, связанный с применением GDPR, объясняется не только и не столько желанием компаний защитить персональные данные своих клиентов, работников, пользователей, сколько желанием минимизировать риски возложения на компании штрафных санкций за нарушение Регламента. Такое желание вполне понятно и обоснованно: за нарушение GDPR установлен максимальный штраф до 4% от глобального оборота или 20 млн. евро.

GDPR – документ прямого действия, подлежит прямому применению в государствах-членах Евросоюза. Однако и страны не-члены ЕС могут быть вовлечены в орбиту Регламента в силу его экстерриториального принципа действия. В связи с этим перед многими российскими компаниями, являющимися частью европейских групп компаний, встает вопрос о применимости к их деятельности GDPR.

Сам Регламент не дает четкого ответа на этот вопрос. Статья 3 говорит, что GDPR применяется к лицам, образованным вне территории ЕС, в случае если:

1. осуществляется обработка персональных данных в контексте деятельности подразделения контролера или обработчика персональных данных в ЕС. При этом не имеет значения, осуществляется ли такая обработка на территории ЕС или вне территории ЕС;

2. осуществляется обработка персональных данных находящихся на территории ЕС субъектов персональных данных контролером или обработчиком, не имеющим

подразделения в ЕС, и при этом такая обработка связана с:
а) предложением товаров или услуг находящимся на территории ЕС субъектам персональных данных, или
б) мониторингом поведения находящихся на территории ЕС субъектов персональных данных при условии, что такое поведение имеет место на территории ЕС.

Столь размытое определение экстерриториального принципа действия GDPR оставляет больше вопросов, нежели дает ответы и рекомендации. Если по предложению товаров/услуг и мониторингу есть некоторые разъяснения в преамбуле GDPR (ст.23 и ст.24 соответственно), позволяющие понять сущность указанных формулировок, то по деятельности подразделения таких разъяснений нет.

Так, в соответствии со ст.23 Преамбулы GDPR если обработка персональных данных связана с предложением товаров и услуг, то для применения Регламента недостаточно, чтобы у субъекта персональных данных в ЕС был доступ к вебсайту иностранного лица (в нашем случае – российского лица) или возможность отправлять такому лицу сообщения. Необходимо установить, что иностранное лицо имело явную цель сделать таких субъектов своими клиентами. Чтобы понять, имеет ли место таргетирование субъектов персональных данных в ЕС, следует учитывать такие факты как: предложение товаров и услуг на языке страны ЕС, прием для оплаты валюты страны ЕС, возможность размещать заказы на языке страны ЕС.

Если компания не попадает под критерии ст.23 Преамбулы GDPR, проверяем ее на критерии ст.24 Преамбулы GDPR. По общему правилу, Регламент применяется, если обработка персональных данных связана с мониторингом поведения субъекта персональных данных. Мониторинг имеет место, когда компания отслеживает физических лиц в Интернете и используют полученные данные для того, чтобы составить «профиль» физического лиц, а затем использовать эти данные для принятия решений в отношении такого лица или предсказывания его личных предпочтений, поведения и привычек. Если следовать букве GDPR, то, к примеру, любой банк или провайдер услуг сотовой связи, находящиеся на

территории России и выпускающие продукты для российских потребителей, становятся субъектами GDPR, как только потребитель их услуг/продуктов выехал на территорию ЕС. Это связано с тем, что неотъемлемой частью услуг/продуктов в названных сферах является мониторинг местонахождения потребителя. Так, например, как только клиент оператора сотовой связи пересек границу РФ, ему в автоматическом режиме поступает сообщение о роуминге, тарифном плане с определением страны пребывания, что свидетельствует о мониторинге со стороны телекоммуникационной компании места нахождения такого клиента. Если клиент снимает денежные средства в банкомате страны ЕС, в реестре банковских операций автоматически фиксируется факт снятия наличных с указанием места нахождения банкомата, что также говорит о мониторинге со стороны кредитной организации места нахождения клиента.

Однако если следовать духу GDPR, то описанный выше подход будет неверен, потому что мониторинг поведения субъектов персональных данных в Интернете должен быть целью деятельности компании, основным видом ее деятельности, а не частью ее услуги/продукта.

Наконец, попробуем разобраться с подразделением контролера или обработчика персональных данных. Не вызывает сомнений, что ситуация, когда российская компания является материнской по отношению к европейской дочерней структуре, либо, когда у российской компании имеются филиалы/представительства в ЕС, подпадает под действие GDPR, поскольку все находящиеся в ЕС юридические лица, независимо от их организационно-правовой формы, являются субъектами GDPR. Однако если развернуть ситуацию и рассмотреть материнскую компанию в ЕС и дочернюю компанию в РФ, то применение для последней положений GDPR не является очевидным.

Ранее действовавшая Директива 95/46/ ЕС в области защиты персональных данных (Data Protection Directive) также оперировала понятием «подразделение». На основании анализа ряда судебных дел, Рабочая группа (Article 29 Working Party) по применению указанной директивы высказала позицию о том, что понятие «подразделение» должно толковаться широко, и законодательство ЕС в части защиты персональных данных может применяться

даже тогда, когда подразделение в ЕС в обработку персональных данных не вовлечено, но существует неразрывная связь между деятельностью такого подразделения и обработкой персональных данных.

Если применить указанную позицию Рабочей группы для рассматриваемой ситуации, то получится следующее. Обработка персональных данных происходит в российской дочерней компании, материнская компания в обработку персональных данных не вовлечена. Но поскольку между материнской и дочерней компанией существует неразрывная связь по определению, то в качестве частного случая проявления такой связи следует рассматривать связь между деятельностью материнской компании в ЕС и обработкой персональных данных, которая осуществляется в ее дочерней структуре в РФ. Исходя из этого, российская дочка европейской материнской компании подпадает под действие GDPR.

Поскольку такой вывод неочевиден и вытекает из логического толкования ранее действовавшей практики применения законодательства в области защиты персональных данных, попробуем поискать более убедительные аргументы применения GDPR к российским дочкам европейских компаний.

На мой взгляд, одним из таких аргументов может являться механизм обязательных корпоративных правил (Binding Corporate Rules (BCR), закрепленный в GDPR. Что это такое? BCR это заложенная в Регламенте возможность для европейских компаний, ведущих совместный бизнес с другими компаниями, в том числе и не находящимися в ЕС, определить единые правила игры для всех участников такой группы. Ст. 47 GDPR определяет требования к содержанию обязательных корпоративных правил. Так, BCR должны устанавливать структуру группы компаний; категории персональных данных, тип обработки и их цели, тип затронутых субъектов персональных данных; общие принципы защиты данных; права субъектов персональных данных; порядок рассмотрения жалоб; проведения аудита и отчетности перед надзорными органами. Для того, чтобы BCR стали обязательными для всех участников группы компаний, обязательные корпоративные правила должны быть, во-первых, разработаны для целей конкретной группы компаний; во-вторых, утверждены

надзорным органом в области защиты персональных данных той страны, где находится материнская компания; и, наконец, они должны быть подписаны всеми участниками группы компаний.

Иными словами, любая европейская компания, представляющая собой группу компаний, в которую входят неевропейские юридические лица, вправе использовать механизм обязательных корпоративных правил для того, чтобы определить единые правила и принципы обработки персональных данных для всех участников группы. Уверена, что добросовестная материнская компания воспользуется механизмом BCR, иначе она не сможет взаимодействовать со своими неевропейскими структурами даже в части трансграничной передачи сведений о сотрудниках, обмена информацией о клиентах, что является неотъемлемой частью информационного взаимодействия внутри любой группы компаний. Соответственно если европейская материнская компания озаботилась защитой персональных данных и соблюдением требований GDPR через использование механизма BCR, то дочерняя компания, присоединившись к обязательным корпоративным правилам, становится обязанной соблюдать GDPR.

Однако применение GDPR для российской дочерней структуры будет усеченным. Что это означает? Во-первых, дочерние структуры не должны назначать своих представителей в ЕС для отчетности об исполнении GDPR, эту функцию берет на себя материнская компания. У дочерней компании остается обязанность перед материнской своевременно уведомлять об инцидентах, связанных с персональными данными. Во-вторых, штрафы за нарушение GDPR невозможно применить к российским компаниям в силу отсутствия действенного механизма исполнения решений судов иностранных государств. Наконец, положения GDPR вполне соответствуют требованиям Федерального закона №152 от 27.07.2006 г. «О персональных данных». Если российская компания следует российскому законодательству в области защиты персональных данных, то она уже в какой-то мере соответствует и GDPR. Здесь необходимо провести анализ процессов по обработке персональных данных, пересмотреть существующие локальные нормативные акты компании, понять, какие новые, специфичные

для GDPR процессы, документы и инструменты, связанные с обработкой персональных данных, следует внедрить. То есть не нужно начинать все с чистого листа, нужно лишь «подкрутить» процессы, документы, инструменты до требуемого Регламентом состояния.

По данным KPMG, 14 из 30 российских компаний попадают под действие GDPR. Практика показывает, что следование GDPR и внедрение требуемых инструментов и процедур оказывает положительное влияние на репутацию российской компании и повышает ее конкурентоспособность. Когда компании, особенно входящие в европейские или международные группы компаний, оценивают возможности сотрудничества, то они анализируют степень соответствия претендента на сотрудничество в части защиты персональных данных не только по локальному (российскому) законодательству, но и по стандартам GDPR.

Таким образом, если материнская компания находится в Европе, то российская дочерняя структура должна соответствовать Регламенту в усеченном виде с изъятиями и ограничениями, о которых я указала выше, при условии принятия обязательных корпоративных правил через подписание внутригруппового договора или иного аналогичного документа. В целом же, учитывая тот факт, что GDPR не противоречит Федеральному закону №152 от 27.07.2006 г. «О персональных данных», а ставит разумные и справедливые задачи по защите персональных данных, ценность которых возрастает с каждым годом цифровой эры, считаю, что применение российскими компаниями GDPR принесет им репутационные бонусы, с одной стороны, и позволит шагнуть чуть дальше и глубже, чем того требует российское законодательство в области защиты персональных данных, с другой стороны.

СТАТЬИ