О защите персональных данных

Эльвира Данилова
Менеджер, Юридические услуги
Компания МАЗАР

Александр Волков
Менеджер, ИТ Аудит Компания МАЗАР

В современном обществе информационных технологий вопрос защиты персональных данных имеет особую важность. Для многих компаний работа с персональными данными является неотъемлемым элементом развития бизнеса. О том, что должны учитывать компании при построении внутренних процессов при работе с персональными данными, мы поговорили со специалистами компании Mazars: Эльвирой Даниловой, менеджером юридической группы Департамента налоговых и юридических услуг и Александром Волковым, менеджером группы ИТ-аудита Департамента аудита.

Коллеги, добрый день. Благодарим вас за возможность пообщаться на такую важную тему, как построение внутренних процессов компании по работе с персональными данными. В последнее время наблюдается повышенный интерес к данному вопросу, даже в тех компаниях, которые ранее не уделяли этой теме должного внимания. С чем, на ваш взгляд, это связано?

Изменения в правовом регулировании защиты персональных данных происходят как в нашей стране, так и за рубежом.

В России с 1 июля 2017 года существенно ужесточается ответственность за правонарушения в области обработки персональных данных. Так, компании смогут быть привлечены к административной ответственности по шести видам составов правонарушений в области работы с персональными данными с наложением штрафа от 15 тыс. руб. до 75 тыс. руб. При этом для более оперативного привлечения к ответственности Роскомнадзор получит полномочия по возбуждению дел об административных правонарушениях и передаче материалов в суд без обращения в прокуратуру.

В Евросоюзе также произошли существенные изменения регулирования данной сферы. С 25 мая 2018 года вступают в силу новые европейские правила защиты персональных данных «Общеевропейский регламент защиты персональных данных» (General Data Protection Regulation, GDPR). Особенность данного документа заключается в его экстратерриториальном

действии: положения GDPR при определенных обстоятельствах могут быть обязательны для соблюдения компаниями, учрежденными за пределами Евросоюза, но обрабатывающими данные резидентов Евросоюза с коммерческой целью (предложение товаров или услуг, мониторинг поведения для определения предпочтений в товарах и т.д.). Штраф за нарушение GDPR может достигать 20 млн евро или 4% годового оборота компании. Хотя надо отметить, что вопрос соблюдения GDPR российскими компаниями — это очень объемная тема для отдельной беседы.

Действительно, это очень важный повод позаботиться о соблюдении законодательства и привести в порядок существующие документы, а в некоторых случаях и разработать их с нуля. Давайте тогда сегодня поговорим о том, что ближе к нашей действительности — о требованиях российского законодательства. Различаются ли требования к внутреннему комплаенсу в области персональных данных в зависимости от объема обрабатываемых персональных данных?

С точки зрения законодательства о защите персональных данных, не имеет значения, обрабатывает ли компания небольшой объем персональных данных своих сотрудников в целях трудового законодательства, либо оперирует массивами персональных данных клиентов в коммерческих целях: базовые ключевые требования законодательства (наличие определенной документации и систем защиты данных) применяются без исключений или послаблений. Но конечно на практике наполнение документов и подход к системе защиты может различаться в зависимости от того, в каких объемах, в каких целях и при каких обстоятельствах компании обрабатывают персональные данные.

Как компании следует выстраивать работу с персональными данными? На что следует особо обратить внимание, чтобы защитить себя на случай проверок Роскомнадзора?

Закон о персональных данных не устанавливает исчерпывающего перечня мер, которые компания обязана реализовывать для обеспечения защиты персональных данных. Определение достаточности мер относится к ответственности компании, обрабатывающей персональные данные. При этом хотелось бы особо отметить, что соблюдение законодательства о персональных данных не ограничивается только получением согласия работника на обработку его персональных данных и выполнением требования о локализации процессов обработки персональных данных.

Меры, направленные на соблюдение законодательства в области защиты персональных данных, можно условно разделить на три группы: юридические меры, организационно-технические меры и меры внутреннего

контроля.

Конкретный набор документов и их наполнение следует определять каждой компании индивидуально, в зависимости от специфики своей работы с персональными данными. В частности, если в компании имеет место трансграничная передача персональных данных, вопросу регламентации данного процесса важно уделить особое внимание.

Юридические меры включают себя принятие компанией ряда локальных актов (политика обработки персональных данных; положения об обработке персональных данных, иных локальных актов и приказов), в которых должен быть зафиксирован подход компании к обработке данных (цели, способы, ответственные лица и т.д.).

К организационно-техническим мерам относится осуществление ряда мероприятий в области обеспечения информационной безопасности, которые позволят компании обеспечивать режим конфиденциальности персональных данных и предотвращать незаконный доступ к ним (в частности, обеспечение определенного уровня технической защиты персональных данных и безопасности информационных систем).

Меры внутреннего контроля — это внедрение набора мероприятий, необходимых для поддержания режима защиты персональных данных в компании на постоянной основе (проведение тренингов, периодические внутренние проверки с фиксацией проведенных мероприятий в журналах и т.д.).

Расскажите, пожалуйста, более подробно про техническую сторону вопроса. Какие технические мероприятия и решения желательно внедрять компаниям для обеспечения безопасности работы с персональными данными? На что компании следует полагаться, чтобы определить достаточный для себя набор технических мер.

Круг нормативных актов, регламентирующих техническую сторону вопроса, достаточно широк. Это Постановления Правительства, Приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК), ФСБ, Минкомсвязи и Роскомнадзора.

Практическая реализация технических мер по защите зависит от многих факторов, в том числе от того, какие бизнес-процессы компании включают в себя обработку персональных данных, каковы объемы и каков состав обрабатываемых персональных данных, с участием каких информационных систем происходит обработка и т.д.

Меры по защите хорошо знакомы специалистам по информационной безопасности и включают в себя ограничение логического доступа к информационным системам, резервное копирование, антивирусная защита, физическая защита серверов и рабочих станций и т.д.

Однако для того чтобы понять, какие меры, где и в каком объеме нужно внедрять, необходимо, помимо прочего, также выяснить, какие подразделения компании принимают участие в обработке персональных данных, какие категории субъектов передали свои персональные данные для обработки и какие меры уже внедрены. Результатом подобной оценки обычно становится набор документов, относящихся к проектированию систем защиты персональных данных. Обязательные среди них документы — «Модель угроз» и «План мероприятий по обеспечению безопасности персональных данных».

В действительности получается, что процедура комплаенса в области персональных данных — процесс трудоемкий. Насколько сложно на практике проходить проверки Роскомнадзора и как к ним подготовиться?

Прежде всего хотелось бы отметить, что компания может быть проверена Роскомнадзором как в ходе плановой проверки (о чем будет известно заранее), так и в ходе внеплановых проверок. В частности, Роскомнадзор вправе принять решение о проведении внеплановой проверки по заявлению физических лиц (например, бывших работников) или юридических лиц (например, конкурентов).

По статистике Роскомнадзора до 70% проверок завершаются с вынесением замечаний. Это является косвенным признаком того, что компании уделяют вопросу комплаенса в области работы с персональными данными недостаточно внимания.

Для успешного прохождения проверки необходимо иметь качественный пакет документов, регламентирующих процесс работы с персональными данными, внедрить ряд технических мер по защите персональных данных, а также обеспечить доказательства того, что за формальными документами действительно стоит непрерывный процесс защиты персональных данных.

Соблюдение законодательства о персональных данных — это комплекс мер, реализация которых должна поддерживаться в компании на постоянной основе. Важно не только фиксировать во внутренних актах комплекс таких мер и способы их реализации, но также в действительности их реализовывать. Важно поддерживать внедрение и реализацию мер на постоянной основе и иметь доказательства того, что меры не являются декларативными и существующими только на бумаге.

Практика проведения мероприятий, направленных на приведение организаций к соответствию требованиям законодательства о персональных данных показывает, что их предпочтительнее осуществлять до появления информации о плановой проверке, так как работа в авральном режиме стоит дороже и не всегда эффективна.