**Семинар по вопросам защиты персональных данных**

**Тема доклада:** «Соблюдение законодательства о персональных данных: обязанности оператора персональных данных. Типичные нарушения требований законодательства»

Начальник отдела по защите прав субъектов персональных данных и надзора в сфере информационных технологий Управления Роскомнадзора по Ярославской области Лысова Маргарита Александровна

**Дата** 16.06.2016

**Время** 09:40-10:00

Необходимость обеспечения безопасности персональных данных в настоящее время объективная реальность. С трудом можно представить деятельность хоть какой-либо организации, а уж тем более органа власти, без обработки информации о человеке. В любом случае орган государственной власти и местного самоуправления обрабатывает персональные данные служащих, их родственников, физических лиц, обращающихся за предоставлением услуг.

Защита персональных данных – это требование законодательства.

Понимая важность и ценность информации о человеке, а также заботясь о соблюдении прав своих граждан, государство требует от операторов обеспечить надежную защиту персональных данных.

Вероятно поэтому Интернет пестрит заголовками «Поможем избежать штрафов при проверке Роскомнадзора. Подготовим документы, избавим от изучения 152-ФЗ». По-моему, весьма сомнительное предложение.

Знакомство с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» - первое, с чего необходимо начать тем, кто имеет дело с информацией о человеке.

Рассчитывая на то, что все-таки сегодня для вас не первая «встреча» с ФЗ «О персональных данных», напомню, персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных); а оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Не смотря на конкретность данного в ФЗ «О персональных данных» определения «оператора», некоторые юридические лица, в том числе государственные и муниципальные органы не причисляют себя к таковым, ссылаясь на отсутствие непосредственного доступа к персональным данным граждан, содержащихся в различных информационных системах, например, в сферах образования, здравоохранения, социальной защиты населения, а также ссылаясь на осуществление обработки персональных данных исключительно в рамках исполнения трудовых отношений.

Но, возвращаясь к определению, выделю ключевое слово «организующие», которое рушит вышеизложенную позицию операторов.

Все-таки, надо понимать, что оператор может не осуществлять обработку персональных данных, т.е. не собирать их, не накапливать, не хранить, не использовать и т.д., а лишь организовывать этот процесс, да и цели обработки персональных данных в указанном определении не фигурируют. Т.е. если даже юридическое лицо осуществляет обработку персональных данных только своих сотрудников и только в целях исполнения трудовых отношений, этого уже достаточно, чтобы быть оператором.

Как я уже сказала, защита персональных данных – это требование закона. В чем именно оно выражается?

Во-первых, каждый оператор должен придерживаться принципов обработки данных, а это значит, что необходимо:

- определить законное основание обработки персональных данных; конкретную и законную цель обработки; содержание и объем персональных данных, в соответствии с целью сбора персональных данных; срок хранения персональных данных;

- исключить избыточность персональных данных;

- обеспечить точность персональных данных, их достаточность, актуальность по отношению к целям обработки.

Во-вторых, определить условия обработки персональных данных, которые закреплены в ч. 1 ст. 6 ФЗ «О персональных данных». Т.е. оценить следующие обстоятельства: обработка персональных данных обусловлена требованиями закона, договора или есть необходимость получения согласия на обработку персональных данных. Определиться, при каком условии обработка персональных данных будет легитимной.

В-третьих, соблюдать конфиденциальность персональных данных, а именно не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Как гласит народная мудрость «кто раскрывает тайну, тот теряет всякое доверие». Очевидно, что, нарушая режим конфиденциальности, оператор несет не только репутационные риски, но и может быть привлечен к ответственности.

Статьей 13.11 КоАП РФ предусмотрено, что нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа, сумма которого может достигать десяти тысяч рублей.

Кроме того, не стоит забывать про иные виды ответственности, предусмотренные российским законодательством, в том числе уголовную.

В-четвертых, оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Что это значит?

Статьей 18.1 ФЗ «О персональных данных» установлено, что оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Указанная статья содержит примерный перечень мер, который фактически является необходимым минимумом. С реализации следующих мер необходимо начать:

1) назначить лицо, ответственное за организацию обработки персональных данных.

Именно это лицо будет осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных; доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных; организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов, а также исполнять другие обязанности, которые предусмотрит оператор.

2) разработать документы, определяющих политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Нас часто спрашивают какие именно это должны быть документы? Сколько их? Что они должны содержать?

Однако, конкретный перечень этих документов законом не регламентирован, содержание, естественно, тоже.

Но, если обратиться к иным нормативным правовым актам, можно придти к выводу о том, что это должен быть документ, устанавливающий цели, задачи деятельности по обработке персональных данных, перечень действий, категории персональных данных, категории субъектов персональных данных, способы обработки, сроки хранения, правила доступа, места хранения, порядок уничтожения персональных данных для каждой из целей.

3) применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 ФЗ «О персональных данных»;

4) осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценить вред, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;

6) ознакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Вниманию государственных и муниципальных органов. В отличие от юридических лиц, которым дана некая свобода в определении состава мер, направленных на соблюдение законодательства о персональных данных, операторы, являющиеся государственными или муниципальными органами, обязаны принимать конкретные меры, предусмотренные Постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами». Данный документ является некой инструкцией, которая содержит действия государственного или муниципального органа по организации процесса обработки персональных данных.

Не мало важен тот факт, что оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

Обеспечить неограниченный доступ – значит не стеснять субъекта персональных данных таким обстоятельством, как, например – регистрация на сайте для ознакомления с данным документом.

Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать указанный документ в соответствующей информационно-телекоммуникационной сети, а также обеспечить возможность доступа к нему с использованием средств соответствующей информационно-телекоммуникационной сети.

Для государственных и муниципальных органов и здесь есть особенность - документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

Еще одна обязанность операторов – регистрация в Реестре операторов, осуществляющих обработку персональных данных, и что не мало важно - поддержание представленной информации в актуальном состоянии.

Осуществление указанных действий – это не только еще один шаг к исполнению закона, но и гарант добросовестности, прозрачности деятельности по обработке персональных данных - для граждан, особенно это касается организаций, оказывающих услуги в сфере жилищно-коммунального хозяйства.

Есть все основания полагать, что ряд притязаний граждан ушел бы на второй план, в случае если бы, обратившись к поиску в Реестре операторов, осуществляющих обработку персональных данных на сайте Роскомнадзора и его территориальных органов, можно было бы увидеть информацию о всех управляющих компаниях, товариществах собственников жилья, информационно – расчетных центрах.

Безусловно, что все государственные и муниципальные органы должны быть зарегистрированы в Реестре, и я не знаю ни одного, который бы подпадал под исключения, предусмотренные ФЗ «О персональных данных».

При этом иные категории операторов – медицинские организации, образовательные учреждения и другие – это и ваша обязанность тоже.

Вместе с тем, одним из типичных нарушений как раз является нарушение требований ч. 3 ст. 22 ФЗ «О персональных данных» - представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения.

Это свидетельствует о недостаточном внимании к заполнению Уведомлений об обработке (намерении осуществлять обработку) персональных данных и последующих Информационных писем о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных, а также непредставлении информации, равно как и несвоевременном предоставлении информации, при возникновении изменений в деятельности оператора, например – появилась новая категория персональных данных, сменился ответственный за организацию обработки персональных данных и т.д. Напоминаю, у оператора, согласно ч. 7 ст. 22 ФЗ «О персональных данных» есть 10 рабочих дней для того, чтобы в случае изменения сведений, указанных в ч. 3 ст. 22 ФЗ «О персональных данных», а также в случае прекращения обработки персональных данных, уведомить Роскомнадзор, а точнее его ТУ.

Призываю присутствующих руководителей проанализировать информацию, содержащуюся в Реестре операторов, осуществляющих обработку персональных данных, и обратить внимание на необходимость предоставления сведений о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации в соответствии с п. 10.1 ч. 3 ст. 22 ФЗ «О персональных данных», вступившим в законную силу с 1 сентября 2015 г.

Обращаю внимание, что формы Уведомлений и Информационных писем, а также порядок их заполнения размещены не только на портале персональных данных Роскомнадзора, но и на «Едином портале государственных и муниципальных услуг (функций)» ([www.gosuslugi.ru](http://www.gosuslugi.ru)), которым я рекомендую пользоваться в связи с очевидными преимуществами.

Достаточно один раз пройти процесс регистрации на Портале для создания «Личного кабинета», в котором Вы сможете подать заявление на оказание любой государственной услуги, передав все необходимые документы в электронном виде. Это освобождает от необходимости лично приезжать, в данном случае, в Управление, тем самым Вы экономите свое время.

Общаясь с операторами, осуществляющими обработку персональных данных на территории Ярославской области, я часто слышу вопрос, и он для них первостепенный «велики ли штрафы за нарушение обязательных требований законодательства о персональных данных?».

У меня на это есть один простой ответ - проверка закончится, штраф оператор заплатит, а требования закона в любом случае придется исполнять.