Как соблюсти требования о защите персональных данных

Персональные данные личности являются конфиденциальной информацией, и ее оборот осуществляется в рамках жесткой правовой процедуры. Принятый шесть лет назад Закон о персональных данных регулирует отношения, связанные с обработкой персональных данных. Однако большинство норм подзаконных актов в отношении требований по обработке персональных данных размыто и в них сложно ориентироваться. Расскажем о том, как привести деятельность компании в соответствие с данными требованиями на примере типичных ошибок, совершаемых операторами при работе с персональными данными.

Правовую основу регулирования отношений в сфере персональных данных составляет Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон) и принятые в соответствии с ним нормативные правовые акты.

Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Субъектом персональных данных может быть только физическое лицо.

Таким образом, персональные данные — это любая информация, с помощью которой лицо можно определить (идентифицировать), например: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, биометрическая информация, данные о супруге, детях, других членах семьи, индивидуальные средства коммуникации (номер телефона, адрес электронной почты, персональный сайт или иной личный ресурс в Интернете, например блог или страница в социальной сети), сведения о событиях и обстоятельствах жизни лица, позволяющие его идентифицировать, в том числе аудио- и видеофайлы, и т.д. Перечень сведений, которые могут быть отнесены к персональным данным, является открытым.

Любые действия или операции с персональными данными называются обработкой персональных данных.

Государственный или муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими 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, называются операторами персональных данных.

Обязанности оператора

Закон обязывает оператора принимать меры по защите персональных данных, но при этом перечень таких мер он вправе определять сам. Закон называет лишь примерный перечень мер. К ним, в частности, отнесены:

1) назначение ответственного за организацию обработки персональных данных;

2) издание документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) ознакомление работников с положениями законодательства РФ о персональных данных, в том числе с требованиями о защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и (или) обучение указанных работников.

При этом оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях о защите персональных данных.

Оператор обязан представить указанные документы и локальные акты и (или) иным образом подтвердить принятие указанных мер по запросу Роскомнадзора.

Таким образом, можно выделить основные обязанности оператора:

- принятие локального нормативного акта, регулирующего вопросы защиты персональных данных;
- назначение работника, ответственного за организацию обработки персональных данных.

Также до начала обработки персональных данных оператор обязан направить уведомление в территориальное отделение Роскомнадзора по месту своего нахождения. Форма бланка и рекомендации по его заполнению утверждены приказом Роскомнадзора от 19.08.2011 № 706.

Оператор не обязан уведомлять Роскомнадзор в случаях, когда персональные данные:

1) обрабатываются в соответствии с трудовым законодательством;

2) получены оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) сделаны субъектом персональных данных общедоступными;

4) включают в себя только фамилии, имена и отчества субъектов персональных данных;

5) необходимы в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

6) обрабатываются без использования средств автоматизации.

Роскомнадзор в течение 30 дней с даты поступления уведомления об обработке персональных данных вносит сведения об операторе в реестр операторов. Сведения, содержащиеся в этом реестре, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

обратите внимание

Операторы, осуществлявшие обработку персональных данных до 1 июля 2011 г., обязаны не позднее 1 января 2013 г. представить в Роскомнадзор следующие сведения:

- *правовое основание обработки персональных данных;*
- *фамилию, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;*
- *сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;*
- *сведения об обеспечении безопасности персональных данных в соответствии с требованиями о защите персональных данных, установленными Правительством РФ.*

Согласие на обработку персональных данных

По общему правилу обработка персональных данных осуществляется с согласия субъекта персональных данных. Согласие на обработку может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме.

Случаи, когда согласия не требуется, предусмотрены в ст. 6 Закона.

Обязанность представить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на оператора. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в любой момент.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя данные, указанные в п. 4 ст. 9 Закона.

Ответственность

В Законе статья об ответственности сформулирована лаконично: «Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность».

В настоящее время меры ответственности за нарушение законодательства о защите персональных данных разбросаны по различным отраслям законодательства — административному, уголовному, гражданскому, трудовому.

Наиболее часто применяется административная ответственность за нарушение ст. 13.11 КоАП РФ. В качестве типичных можно выделить следующие нарушения:

- обработку персональных данных без согласия субъекта персональных данных;
- несоответствие содержания письменного согласия субъекта на обработку его персональных данных требованиям Закона о персональных данных;
- нарушение требований конфиденциальности при обработке персональных данных.

Ответственность наступает в виде предупреждения или наложения административного штрафа на на должностных лиц — от 500 до 1000 руб., на юридических лиц — от 5000 до 10 000 руб.

Однако есть предложение увеличить размер штрафов (соответствующий законопроект проходит сейчас согласовательные процедуры). Например, штраф за нарушение порядка обработки персональных данных для юридических лиц — до 500 000 руб.

Моральный вред, причиненный субъекту персональных данных, подлежит возмещению в соответствии с ГК РФ. Его возмещение осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Также виновные в нарушении требований законодательства несут дисциплинарную и уголовную ответственность. Однако привлечение к уголовной ответственности является крайне редким явлением.

Борис Пупко,
юрист группы технологий и инвестиций VEGAS LEX

к сведению

Советы, как привести деятельность компании в соответствие с требованиями законодательства

Сотрудники Роскомнадзора уделяют большое внимание документам, которые закрепляют политику в отношении персональных данных, вопросы их обработки и защиты. С одной стороны, в нормативных актах установлены определенные требования к оформлению и содержанию этих документов, с другой — эти требования размыты по многочисленным нормативным актам, поэтому операторам сложно в них сориентироваться.

Большинство замечаний Роскомнадзора относится к тому, что необходимые документы, касающиеся персональных данных, часто носят формальный характер, повторяя содержание статей Закона о персональных данных. В разъяснениях Роскомнадзор выделяет типичные ошибки, которые допускают операторы:

1. Не указываются конкретные нормы Закона, на основании которых оператор ведет обработку персональных данных. Роскомнадзор говорит о том, что в документах следует четко перечислить соответствующие пункты и статьи конкретных нормативных актов, регламентирующих осуществляемый вид деятельности оператора и касающихся обработки персональных данных.

2. Под целью обработки персональных данных операторы ошибочно указывают саму обработку персональных данных или действия, совершаемые с персональными данными (сбор, хранение, использование и др.). Однако здесь следует перечислить конкретную цель обработки персональных данных.

3. Категории персональных данных указываются не полностью, часто вместо закрытого перечня операторы пишут фразы «и др.», «и т.п.», «другая информация». Необходимо перечислять все обрабатываемые категории персональных данных. Перечень должен быть закрытым.

4. Перечисляются лишь общие характеристики используемых оператором способов обработки персональных данных, а также порядок передачи информации. Однако оператору следует указать лишь те из них, которые он фактически совершает, например сбор, систематизацию, хранение, уточнение, использование и передачу.

5. Не указываются конкретные меры, которые оператор обязуется осуществлять при обработке персональных данных и для обеспечения их безопасности.

6. Отсутствует список лиц, имеющих доступ к персональным данным, обрабатываемым в информационной системе. Такой список следует утвердить приказом оператора.

Это наиболее типичные ошибки операторов, хотя Роскомнадзор отмечает и другие. Например, отсутствие листа ознакомления работников оператора под личную подпись с Положением о защите персональных данных, а также документа, подтверждающего факт информирования лиц о том, что они осуществляют обработку персональных данных без использования средств информатизации. Подобный документ должен содержать категории персональных данных, а также особенности и правила осуществления обработки.