РЕКОМЕНДАЦИИ
по соблюдению некоммерческими организациями требований
Федерального закона «О персональных данных» №152-ФЗ от 27 июля 2006 года
(с последующими изменениями)

Любая организация, независимо от форм собственности или организационно-правового статуса (за исключением филиалов и представительств иностранных некоммерческих неправительственных организаций), обрабатывает персональные данные своих сотрудников, контрагентов, добровольцев и т.д., то есть, согласно Федеральному закону «О персональных данных» (далее - Закон), является оператором персональных данных. В связи с этим, у операторов закономерно возникает вопрос: как соблюсти все требования Закона при обработке персональных данных, чтобы не быть привлеченным к ответственности за их нарушения? Ответственность за нарушения законодательства в области обработки персональных данных достаточно серьезна хотя бы для того, чтобы постоянно держать ее в уме (об этом ниже). Разработать единые рекомендации по соблюдению требований Закона представляется крайне сложным, поскольку цели, объем, категории обрабатываемых персональных данных в каждой организации разнятся, однако мы постараемся составить примерный перечень действий и мер, необходимых для каждой организации – оператора. Несмотря на то, что мы постараемся «простым» языком изложить все необходимые требования законодательства, операторам персональных данных, все же, придется вникнуть в тексты нормативно-правовых актов, регулирующих данную сферу, ссылки на нормативно-правовые акты будут приведены в тексте рекомендаций.

Прежде всего, необходимо определить, какая информация относится к персональным данным и какие существуют категории персональных данных. Согласно последним изменениям в Законе, формулировка понятия «персональные данные» приведена в еще более общем и пространном виде, чем было ранее: «персональные данные – любая информация, относящаяся к прямо или косвенно определенному и определяемому физическому лицу (субъекту персональных данных)». Подобная «размытость» понятия «персональные данные» отнюдь не способствует правильному толкованию норм Закона и позволяет трактовать в качестве персональных данных практически любую информацию (вплоть до абсурда). Каких-либо разъяснений на этот

Данные рекомендации подготовлены Филиалом Международного центра некоммерческого права в РФ и Некоммерческим партнерством «Юристы за гражданское общество» в рамках Программы правовой поддержки гражданского общества. Январь 2012 года.

счет, в том числе со стороны контролирующих органов, нет. Однако, целесообразно руководствоваться следующим правилом: какую информацию Роскомнадзор включает в уведомление об обработке персональных данных, то и следует считать таковыми (о функциях Роскомнадзора и об уведомлении об обработке персональных данных будет подробно изложено далее в тексте настоящих рекомендаций). Существуют также специальные категории персональных данных (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья или интимной жизни), а также биометрические персональные данные (характеризующие физиологические особенности человека, на основе которых можно установить его личность). Условия обработки разных категорий персональных данных различаются (об этом также будет изложено ниже).

Важно обозначить перечень государственных органов – регуляторов в области обработки персональных данных:

- основные контрольные функции делегированы Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор). Данная служба, в соответствии с Законом, является уполномоченным органом по защите прав субъектов персональных данных, составляет и ведет реестры операторов персональных данных, рассматривает обращения субъектов персональных данных, привлекает операторов к административной ответственности за нарушения и т.д.;

- Федеральная служба по техническому и экспортному контролю (далее – ФСТЭК) осуществляет надзорные функции за применением технических средств защиты информации, сертифицирует такие технические средства и лицензирует деятельность по защите информации;

- Федеральная служба безопасности РФ (далее – ФСБ) контролирует использование криптографических (шифровальных) средств защиты информации, сертифицирует такие средства и лицензирует деятельность по защите информации с использованием криптографических средств;

- органы прокуратуры РФ, на которые возложена обязанность по надзору за соблюдением законодательства в целом («око государево»);

- Федеральная инспекция труда также обладает определенными полномочиями по контролю в данной сфере, ведь обязанности работодателя по хранению и использованию персональных данных закреплены трудовым законодательством (Глава 14 Трудового кодекса РФ), а нарушения положений трудового законодательства подведомственны именно Федеральной инспекции труда.

Итак, какие же именно действия и меры обязан принимать каждый оператор персональных данных, чтобы соблюсти требования Закона?

Во-первых, оператор обязан провести классификацию своих информационных систем персональных данных, определить какие категории персональных данных обрабатываются, виды обработки персональных данных, какой класс защиты информации

требуется. Классификация проводится в соответствии с требованиями совместного Приказа ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года №55/86/20. Оператором выносится приказ о назначении комиссии по классификации информационных систем персональных данных. Процедура классификации заканчивается составлением соответствующего акта. Особенности автоматизированной или неавтоматизированной обработки персональных данных регулируются Постановлением Правительства РФ от 17 ноября 2007 года №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и Постановлением Правительства РФ от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». После проведения классификации в организации должно быть разработано и утверждено Положение об обработке персональных данных с обязательным ознакомлением сотрудников организации с требованиями данного Положения. Далее организация своим приказом назначает лицо, ответственное за обработку персональных данных. Помимо этого, во исполнение требований Закона и Постановлений Правительства РФ, организация – оператор обязана разработать и утвердить еще ряд локальных (внутренних) актов, а также приобщить документы от поставщиков средств защиты информации (далее – СЗИ): приказ о допуске к обработке персональных данных (список лиц) и о допуске к работе с СЗИ, приказ о допуске в помещения или приказ о контролируемой зоне (территории), модель угроз, техническое задание на СЗИ, документы по поставке и программное обеспечение СЗИ, лицензии и сертификаты на используемые СЗИ, приказ о вводе системы в эксплуатацию, декларирование готовности и соответствия, инструкция по антивирусному обеспечению, инструкция администратору безопасности, документы по прохождению обучения сотрудников требованиям обеспечения безопасности персональных данных, акты уничтожения персональных данных после достижения цели их обработки, журнал поэкземплярного учета СЗИ, журнал учета проверок, журнал учета обращений субъектов персональных данных, журнал учета носителей информации и т.д. И это лишь примерный перечень документов, которые обязан разработать оператор. При этом, конкретных образцов необходимых документов нет ни в Законе, ни в Постановлениях Правительства, оператор разрабатывает их самостоятельно.

Во-вторых, следует напомнить, что по Закону оператор обязан принимать необходимые организационные и технические меры по обеспечению безопасности персональных данных, при этом достаточность таких мер определяется в ходе осуществления государственного контроля и надзора, то есть в ходе проверок. Что касается использования технических средств защиты информации (СЗИ), то, теоретически, Закон допускает их самостоятельную разработку оператором персональных данных, однако для этого необходимо получить соответствующие лицензии ФСБ и ФСТЭК (деятельность по защите информации подлежит обязательному лицензированию,

осуществление такой деятельности без лицензии расценивается как незаконное предпринимательство со всеми вытекающими из этого последствиями административного или даже уголовного характера), создать опытную лабораторию для испытаний разрабатываемых средств, получить в установленном порядке сертификаты на разработанные средства защиты информации и прочее. Поскольку данный путь является чрезвычайно затратным и трудоемким, представляется сомнительным, что организация, не специализирующаяся на защите информации, может самостоятельно разработать собственные средства защиты информации. Выход у организаций – операторов персональных данных остается только один: обратиться в компанию, специализирующуюся на защите информации, за построением системы информационной безопасности и внедрением СЗИ. Перечень организаций, предоставляющих услуги по защите информации весьма широк и разброс цен на эти услуги также велик. При выборе компании для построения системы информационной безопасности нужно руководствоваться, прежде всего, следующим: имеет ли компания необходимые лицензии ФСБ и ФСТЭК на осуществление деятельности по защите информации, имеются ли необходимые сертификаты тех же ФСБ и ФСТЭК на применяемые СЗИ, как давно компания работает в сфере защиты информации, отзывы организаций, воспользовавшихся услугами данной компании, успешное прохождение этими организациями проверок Роскомнадзора. На рынке услуг по защите информации действует довольно много посредников, которые самостоятельно такие услуги не оказывают, а лишь необоснованно завышают цены, при этом сами обращаются к непосредственным производителям СЗИ. Для сокращения излишних расходов, организации – оператору персональных данных необходимо таких посредников отсеять.

Следующий важный момент касается направления оператором уведомления об обработке персональных данных в Роскомнадзор. Все операторы, еще до начала обработки персональных данных, обязаны направить соответствующее уведомление в Роскомнадзор. Вместе с тем, Закон содержит исчерпывающий перечень случаев обработки персональных данных, когда оператор вправе не направлять такое уведомление. Ко всем этим исключениям нужно подходить крайне осторожно, поскольку, например, если оператор осуществляет обработку персональных данных только в соответствии с трудовым законодательством, то он вправе не направлять уведомление в Роскомнадзор, однако, могут быть случаи, когда работник по решению суда или в добровольном порядке отчисляет алименты на содержание детей или пожилых родителей, и эти алименты из заработной платы работника отчисляет именно работодатель. Для отчисления таких алиментов работодатель обрабатывает персональные данные их получателей (детей, супругов, родителей работника), и причислить такую обработку к трудовым отношениям довольно затруднительно, тем более доказать это при проверке Роскомнадзора. Еще одним распространенным примером выхода за рамки трудовых правоотношений, в соответствии с разъяснениями Роскомнадзора, является передача персональных данных работников третьим лицам при оформлении зарплатной карты в

рамках договора с кредитным учреждением. То есть, если заработная плата в организации не выдается на руки (что в настоящее время уже редкость), а начисляется на банковскую карту, то уведомление в Роскомнадзор подавать нужно. Если проверкой будет выявлено, что оператор при обработке персональных данных вышел за пределы предусмотренных случаев, когда нет необходимости в направлении уведомления в Роскомнадзор, то у оператора возникает серьезный риск быть привлеченным к административной ответственности. Направление уведомления об обработке персональных данных в Роскомнадзор, автоматически влечет за собой включение организации в реестр операторов, и, соответственно, в список плановых проверок (план проверок на текущий год размещен в свободном доступе на официальном сайте Роскомнадзора www.rsoc.ru). Вместе с тем, нельзя забывать о том, что Роскомнадзор имеет право проводить и внеплановые проверки, в частности, по обращениям субъектов персональных данных о нарушении их прав, поэтому ненаправление уведомления в Роскомнадзор не может обезопасить оператора персональных данных от проверок. Сведения, которые должны содержаться в уведомлении, четко регламентированы в тексте Закона, бланк уведомления содержится на официальном сайте Роскомнадзора. Процедура направления уведомления довольно проста: на сайте Роскомнадзора заполняется соответствующий бланк, которому присваивается регистрационный номер, второй и третий зарегистрированные экземпляры распечатываются, после чего один хранится у оператора, а другой почтовой связью направляется в Роскомнадзор. При этом датой направления уведомления считается его регистрация на сайте службы.

Вызывает определенные трудности механизм получения согласия субъекта на обработку его персональных данных. Согласно последним изменениям в Законе, субъект персональных данных или его представитель может дать свое согласие на обработку его персональных данных в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. При этом, обязанность предоставить доказательство получения такого согласия возлагается на оператора. В тексте Закона прямо указаны требования к письменному согласию субъекта персональных данных. Поэтому, для исключения каких бы то ни было проблем с получением согласия субъекта персональных данных, представляется целесообразным в каждой организации разработать письменную форму (с учетом требований Закона, конечно) согласия субъекта персональных данных, в которой последнему будет необходимо собственноручно указать необходимые сведения и поставить подпись. В организации нужно взять за правило заполнять такую форму письменного согласия при заключении трудовых и иных гражданско-правовых договоров с сотрудниками, контрагентами, добровольцами и т.д. То есть такая форма фактически будет являться приложением к договорам, когда возникает необходимость в обработке персональных данных. Можно также внести согласие субъекта на обработку его персональных данных отдельным пунктом в сам текст соответствующего договора. Как уже упоминалось выше, передача персональных данных работника в кредитные учреждения для начисления зарплаты на банковскую карту также

требует его письменного согласия. Обработка специальных категорий персональных данных и биометрических персональных данных возможна только с письменного согласия субъекта персональных данных, за исключением случаев, установленных федеральным законом. Много споров вызвал вопрос о том, является ли фотоизображение гражданина биометрическими персональными данными. Каких-либо разъяснений и на этот счет нет, однако, исходя из положений Закона, фотоизображения все же следует считать таковыми, поскольку они характеризуют физиологические особенности человека и позволяют определить его личность. Многие организации имеют свои сайты в информационно-телекоммуникационной сети Интернет, а на сайтах зачастую размещаются фото руководителей, сотрудников организации, партнеров, фотоотчеты с мероприятий и т.д. Так вот, во избежание ненужных проблем с контролирующими органами, при размещении фотоизображений в сети Интернет, оператору все же следует запастись письменным согласием лица, изображенного на фото, на такое публичное размещение его биометрических персональных данных, фактически делающее его биометрические данные общедоступными. Что же касается групповых фото, то тут уже придется получать согласие всех изображенных на фото лиц. На официальном сайте Роскомнадзора в разделе «Новости» была размещена информация о том, что конкретная организация была оштрафована за обработку биометрических персональных данных без письменного согласия субъекта, а факт нарушения заключался в том, что в организации хранились копии паспортов работников, в которых, как известно, присутствуют фотоизображения владельцев. Таким образом, фотографии все же являются биометрическими персональными данными и их обработка требует соблюдения норм Закона. Напомним, что обязанность доказывания наличия согласия субъекта персональных данных возложена на оператора, в связи с чем существует такая практика (это, прежде всего, касается различных СМИ и информационных агентств): при получении информации, включающей в себя персональные данные, из открытых источников в сети Интернет, делаются скрин-шоты соответствующих страниц, а, поскольку теоретически возможна подделка таких скрин-шотов, то производится еще и их нотариальное заверение. Несмотря на сложность такого подхода, это позволяет доказать общедоступность персональных данных, а, соответственно, и законность их обработки.

Анализ правоприменительной практики показывает, что нередки случаи, когда организации (даже несмотря на то, что формально все требования по обеспечению безопасности персональных данных соблюдены и все необходимые документы в организации разработаны) подвергаются административному наказанию за то, что хранят у себя документы, содержащие персональные данные субъектов, с которыми организацию ранее связывали гражданско-правовые отношения, но цели обработки персональных данных давно достигнуты и дальнейшее их хранение не требуется. Во избежание подобных эксцессов, организациям следует порекомендовать провести ревизию всех документов организации, содержащих персональные данные субъектов, и те персональные данные, цели обработки которых достигнуты и их хранение в соответствии

с бухгалтерским учетом, налоговым или трудовым законодательством не требуется, необходимо уничтожить с составлением соответствующего акта (Закон предоставляет тридцатидневный срок для уничтожения персональных данных после достижения или утраты целей их обработки). Те же персональные данные, хранение которых требуется в соответствии с налоговым или иным законодательством, но у самой организации необходимости в них нет, можно сдать в различные архивы и «забыть» про них. Если у органов государственной власти (например, налоговых) возникнет необходимость в данных документах, то они могут самостоятельно, без участия организации, затребовать их в соответствующих архивах. Сдача документов в архив позволит организации – оператору персональных данных обезопасить себя от претензий Роскомнадзора, поскольку Закон не распространяется на архивные документы в соответствии с законодательством об архивном деле в РФ.

Теперь о том, что касается трансграничной (то есть за пределы РФ) передачи персональных данных. В данной части Закон содержит в себе положения, которые непонятны и спорны. Например, перед трансграничной передачей персональных данных оператор обязан убедиться, что принимающей стороной обеспечивается их «адекватная» защита. При этом содержание понятия «адекватности» защиты персональных данных в Законе не раскрывается, в связи с чем у операторов возникают опасения, что ту защиту принимающей стороны, которую оператор посчитает «адекватной», контролирующие органы вовсе не обязательно сочтут таковой. И опять же возникает риск привлечения оператора к ответственности. Выхода тут у операторов персональных данных может быть два: трансграничная передача персональных данных может осуществляться при наличии согласия в письменной форме субъекта на такую передачу его персональных данных, либо же, если трансграничная передача персональных данных осуществляется в целях исполнения договора, стороной которого является субъект персональных данных. Поэтому, во избежание проблем при трансграничной передаче персональных данных, оператору следует запастись письменным согласием субъекта персональных данных.

Существуют следующие виды ответственности за нарушения в сфере обработки персональных данных:

- практически любое нарушение законодательства о персональных данных может быть квалифицировано по статье 13.11 Кодекса РФ об административных правонарушения (Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);

- ненаправление уведомления в Роскомнадзор об обработке персональных данных, в случае, когда оно должно было быть направлено, квалифицируется по статье 19.7 КоАП РФ (Непредставление сведений (информации);

- как уже упоминалось ранее, обязанности работодателя по хранению и использованию персональных данных сотрудников закреплены в главе 14 Трудового кодекса РФ, в связи с чем их нарушение может быть истолковано как административное

правонарушение, предусмотренное статьей 5.27 КоАП РФ (Нарушение законодательства о труде и об охране труда);

- ни в коем случае не следует использовать несертифицированные в установленном порядке средства защиты информации и не осуществлять деятельность по защите информации без соответствующей лицензии под угрозой привлечения к административной ответственности по статьям 13.12 КоАП РФ (Нарушение правил защиты информации), 13.13 КоАП РФ (Незаконная деятельность в области защиты информации), 14.1 КоАП РФ (Осуществление предпринимательской деятельности без государственной регистрации или без специального разрешения (лицензии) или даже уголовного преследования по ст. 171 Уголовного кодекса РФ (Незаконное предпринимательство);

- сотрудники организации, непосредственно осуществляющие обработку персональных данных, могут быть привлечены к административной ответственности по статье 13.14 КоАП РФ (Разглашение информации с ограниченным доступом);

- при обработке персональных данных также существует риск привлечения к уголовной ответственности по статье 137 Уголовного кодекса РФ (Нарушение неприкосновенности частной жизни), но это, все же, в большей мере относится к деятельности различных СМИ.

При всем этом, нарушения в сфере обработки персональных данных могут подпадать и под иные составы преступлений или административных правонарушений. Таким образом, в руках государства есть достаточное количество «рычагов» воздействия на нарушителей законодательства в области персональных данных.

Конечно, Закон содержит в себе много нестыковок, чрезмерно жестких и трудновыполнимых требований к операторам персональных данных, однако следует помнить, что сфера обработки такой конфиденциальной информации как персональные данные – это сфера публичных интересов, и государство будет защищать ее вне зависимости от желания самих субъектов персональных данных.