Проверки НКО Роскомнадзором: правовое пространство

СЕРИЯ МАТЕРИАЛОВ

- **Проверки НКО.** Рамки правового пространства
- **Проверки НКО Министерством юстиции:** правовое пространство
- **Налоговые проверки НКО:** правовое пространство
- **Проверки НКО Роскомнадзором:** правовое пространство
- **Проверки НКО трудовыми инспекциями:** правовое пространство
- **Проверки НКО Госпожнадзором:** правовое пространство
- **Проверки НКО органами прокуратуры:** правовое пространство

Проверки НКО Роскомнадзором: правовое пространство

Авторы: Анатолий Арсенихин, Екатерина Васютина, Максим Дмитрук,
Юлия Дробот, Татьяна Захаркова, Елена Исаева, Елена Макей,
Дарья Милославская, Игорь Михайлов, Василий Романец и Александра Сазонова.
Под редакцией Дарьи Милославской.

Проверки НКО. Рамки правового пространства / Дарья Милославская и др. – Москва.

В сборнике материалов под общим названием «Проверки НКО. Рамки правового пространства» Вы познакомитесь с правовыми основаниями проведения проверок некоммерческих организаций различными государственными органами, в том числе Министерством юстиции, органами прокуратуры, Государственной инспекцией труда, Федеральной налоговой службой и др., а также получите общие рекомендации по подготовке к проверкам и поведению руководителя некоммерческой организации в ходе проверок.

Материалы адресованы руководителям, юристам и бухгалтерам некоммерческих организаций.

Корректор: Ольга Зюзина
Дизайн и верстка: Ирина Мячина

НАШИ ОБОЗНАЧЕНИЯ:

 – Федеральные законы | Документы

 – Официальные сайты

 – Важные советы

Нормативно-правовые акты приведены
по состоянию на 21 декабря 2018 г.

Подготовлено юристами Ассоциации «Юристы за гражданское общество»
ISBN 978-5-905823-67-1

ОГЛАВЛЕНИЕ

Вопрос-ответ

1. Кто проверяет/кто принимает документы?

Должностные лица Роскомнадзора, указанные в распоряжении о проведении проверки.

2. Достаточно ли удостоверения, чтобы прийти в организацию и посмотреть документы?

Нет, обязательно распоряжение о проведении проверки.

3. Что проверяют?

Соблюдение требований законодательства об обработке и защите персональных данных (ПД).

4. Какие документы имеют право запрашивать?

Документы, которые НКО обязана иметь в соответствии с законодательством о персональных данных (положение об обработке ПД, приказ о назначении ответственного за обработку ПД лица, модель угроз, документы об установке средств защиты информации, письменные согласия на обработку ПД и др.).

5. Можно ли документы исправлять в процессе прохождения проверки?

Четких ограничений нет. Анализ практики показывает, что Роскомнадзор зачастую допускает исправление документов в процессе проверки.

6. Кто должен представлять (показывать/отвозить) документы?

Лицо, назначенное ответственным за обработку ПД (приказ по организации).

7. Какие могут найти нарушения и чем это грозит?

Наиболее распространенными нарушениями являются: ненаправление в Роскомнадзор уведомления об обработке ПД, обработка ПД без согласия субъекта ПД, непринятие организационных и технических мер по защите ПД и др. За эти нарушения грозит административная, а в некоторых случаях – даже уголовная ответственность.

Краткое содержание раздела

НКО редко защищают персональные данные

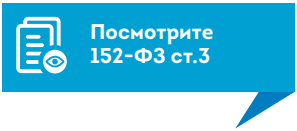
Практика общения с представителями некоммерческих организаций показывает, что уровень их осведомленности о требованиях законодательства в области обработки и защиты персональных данных чрезвычайно низок. В связи с этим в деятельности некоммерческих организаций возникает потенциальная возможность нарушения закона и как следствие – неблагоприятный исход проверки.

Основные вопросы, возникающие в сфере обработки персональных данных, можно разделить на следующие основные группы:

- вопросы, связанные с получением согласия на обработку персональных данных и его правильного оформления;
- вопросы, возникающие в связи с неавтоматизированной (бумажной) обработкой персональных данных. Требования закона в части хранения материальных носителей персональных данных (не путать с бухучетом и архивным делом!) определены специальным постановлением Правительства РФ;
- технические меры, а именно: применение технических средств защиты персональных данных при их автоматизированной (с использованием компьютера) обработке, определение модели угроз, выбор поставщика средств защиты информации;
- подача/неподача в Роскомнадзор уведомления об обработке персональных данных.

Общие рекомендации по поведению при проведении проверок

Любая организация, независимо от форм собственности или организационно-правового статуса, обрабатывает персональные данные своих сотрудников, контрагентов, добровольцев и т.д., то есть, согласно Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон), является оператором персональных данных.



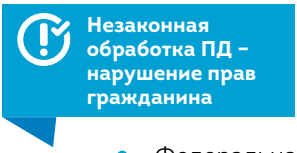
Закон определяет понятие **«персональные данные»** следующим образом: «персональные данные – любая информация, относящаяся к прямо или косвенно определенному и определяемому физическому лицу (субъекту персональных данных)». Подобная «размытость» термина позволяет трактовать в качестве персональных данных практически любую информацию о конкретном физическом лице (субъекте персональных данных), в связи с чем, во избежание возможных рисков привлечения к ответственности, следует понимать данное понятие максимально расширительно (начиная с фамилии и заканчивая банковским счетом физического лица и сведениями о его профессиональных навыках или образовании).

Существуют специальные, а также биометрические персональные данные

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).

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.;

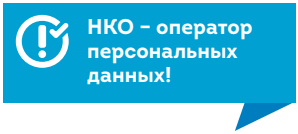


- органы прокуратуры РФ, осуществляющие надзор за соблюдением законов и соблюдением прав и законных интересов граждан;
- Федеральная служба по техническому и экспортному контролю (далее – ФСТЭК) осуществляет надзорные функции за применением технических средств защиты информации, сертифицирует такие технические средства и лицензирует деятельность по защите информации;
- Федеральная служба безопасности РФ (далее – ФСБ) контролирует использование криптографических (шифровальных) средств защиты информации, сертифицирует такие средства;
- Государственная 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 ТК РФ), а нарушения положений трудового законодательства подведомственны именно Государственной инспекции труда.

Работодатель всегда обрабатывает персональные данные

Обязанности оператора персональных данных (ПД)

Обязанности оператора персональных данных (любой организации) можно разделить на две основные части: организационные и технические.

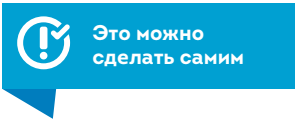


Организационные моменты включают в себя:

- разработку и принятие внутренних (локальных) актов организации;
- определение лиц, ответственных за обработку персональных данных;
- получение согласия на обработку персональных данных от граждан;
- организацию хранения материальных (бумажных) носителей персональных данных (определение помещений для хранения и порядка доступа к ним);
- ведение журнала учета обращений субъектов персональных данных и т.д.

Техническая сторона состоит в применении специальных технических средств защиты информации.

Организационные меры соблюдения законодательства о ПД



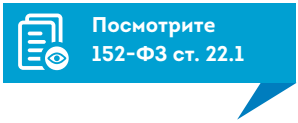
К организационным мерам, в частности, относятся:

- **назначение лица,** ответственного за обработку персональных данных;
- **определение видов,** объема персональных данных, способов их обработки;
- **разработка внутреннего положения** об обработке персональных данных (данное положение должно распространяться на всех субъектов персональных данных, а не только на сотрудников организации, что является распространенной ошибкой) и ознакомление с ним всех сотрудников организации, а также размещение его для ознакомления неограниченным кругом лиц (в свободном доступе в офисе организации и на своем сайте в сети Интернет);

У каждой НКО свои модели угроз

- **разработка модели угроз** в соответствии с нормативными актами;
- **определение уровней защищенности** персональных данных в информационных системах;
- **определение поставщика средств защиты информации** и разработка технического задания на их поставку и установку, приобщение документов по поставке программного обеспечения средств защиты информации (СЗИ), лицензий и сертификатов на используемые СЗИ, вынесение приказа о вводе системы в эксплуатацию, декларирование готовности и соответствия;

- **определение списка сотрудников,** допущенных к обработке персональных данных и организация их обучения по вопросам обработки персональных данных;



- **определение места хранения** материальных носителей персональных данных и порядка допуска лиц в помещения организации;

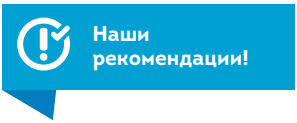
- **разработка инструкций для администратора безопасности,** пользователей, а также по антивирусному обеспечению;

- **ведение необходимых журналов учета:** СЗИ, обращений субъектов ПД, материальных носителей ПД, приема посетителей, проверок и др.

- **составление актов уничтожения** персональных данных после достижения цели их обработки.

Согласие на обработку ПД

На практике у некоммерческих организаций вызывает определенные трудности механизм получения согласия субъекта на обработку его персональных данных. Согласно Закону, 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.

Теоретически, можно также внести согласие субъекта на обработку его персональных данных отдельным пунктом в сам текст соответствующего договора, однако в этом случае в тексте

договора должна быть предусмотрена специальная графа для подписи субъекта ПД непосредственно под согласием, а при проверке законности обработки ПД контролирующим органом необходимо будет представить договор целиком.

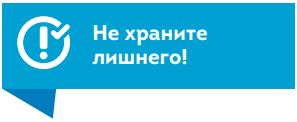
Правильно:
получить письменное согласие на обработку ПД от всех сотрудников

Несмотря на то, что трудовые правоотношения не требуют получения письменного согласия субъекта на обработку персональных данных, передача персональных данных работника в кредитные учреждения для начисления зарплаты на банковскую карту выходит за рамки трудовых правоотношений и требует его письменного согласия. Также за рамки трудовых отношений выходит и отчисление алиментов в добровольном порядке или по решению суда.

Обработка ПД

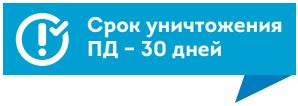
Обработка специальных категорий персональных данных и биометрических персональных данных возможна только с письменного согласия субъекта персональных данных, за исключением случаев, установленных федеральным законом. Следует отметить, что фото- и видеоизображения расцениваются как биометрические персональные данные, т.е. требуют наличия письменного согласия соответствующего субъекта. Это же относится и к случаям размещения фото- и видеоизображений субъектов персональных данных на сайтах организаций в сети Интернет.

Исключение составляют фото- и видеоизображения, полученные на открытых публичных мероприятиях (статья 152.1 Гражданского кодекса РФ), где получение согласия не требуется.



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 законодатель-

ством не требуется, уничтожить с составлением соответствующего акта. Закон предоставляет тридцатидневный срок для уничтожения персональных данных после достижения или утраты целей их обработки.



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.

Можно воспользоваться архивом, но подготовить документы по специальным требованиям трудно

Трансграничная передача ПД

Трансграничная передача данных (то есть за пределы РФ) также урегулирована законом. 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.

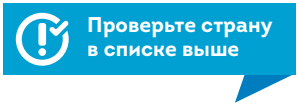
Отдельно следует указать, что адекватной признается защита в странах, подписавших «Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

Оператору, осуществляющему трансграничную передачу персональных данных, необходимо руководствоваться законодательством иностранного государства, на территорию которого осуществляется передача персональных данных, законодательством Российской Федерации в области защиты прав субъектов персональных данных, а также международными нормативными актами, в том числе Конвенцией о защите прав физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. ETS № 108 с учетом перечня стран, подписавших и ратифицировавших данную Конвенцию. Это Австрия, Бельгия, Болгария,

Важно для НКО, занимающихся международным сотрудничеством

Дания, Великобритания, Венгрия, Германия, Греция, Ирландия, Испания, Италия, Латвия, Литва, Люксембург, Мальта, Нидерланды, Польша, Португалия, Румыния, Словакия, Словения, Финляндия, Франция, Чехия, Швеция, Эстония. Вторая группа, которая может претендовать на статус стран, обеспечивающих адекватную защиту персональных данных, это страны, имеющие общенациональные нормативные правовые акты в области защиты персональных данных и уполномоченный надзорный орган по защите прав субъектов персональных данных. Это Андорра, Аргентина, Израиль, Исландия, Канада, Лихтенштейн, Норвегия, Сербия, Хорватия, Черногория, Швейцария, Южная Корея, Япония.

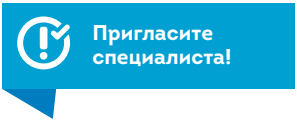
В случае необходимости передачи персональных данные в другие страны у оператора, согласно Закону, есть два способа:



1) трансграничная передача персональных данных может осуществляться при наличии согласия в письменной форме субъекта на такую передачу его персональных данных,

2) 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.

Технические меры соблюдения законодательства о ПД

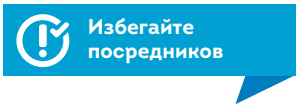


Что касается использования технических средств защиты информации (СЗИ), то, теоретически, Закон допускает их самостоятельную разработку оператором персональных данных, однако для этого необходимо получить соответствующие лицензии ФСБ и ФСТЭК (деятельность по защите информации подлежит обязательному лицензированию, 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.

Разработка технических СЗИ требует особой подготовки

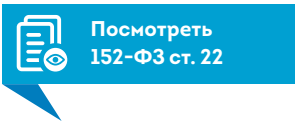
Необходимые технические средства защиты определяются при разработке модели угроз. Перечень организаций, предоставляющих услуги по защите информации, весьма широк и разброс цен на эти услуги также велик. При выборе компании для построения системы информационной безопасности нужно руководствоваться, прежде 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.



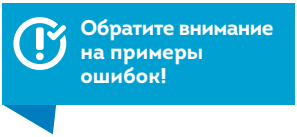
На рынке услуг по защите информации действует довольно много посредников, которые самостоятельно такие услуги не оказывают, а лишь необоснованно завышают цены, при этом сами обращаются к непосредственным производителям СЗИ. Для сокращения излишних расходов организации – оператору персональных данных необходимо таких посредников отсеять.

Уведомление об обработке ПД



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 такого уведомления.

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 зарплат-



ной 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.

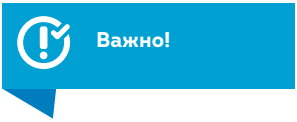
Направление уведомления об обработке персональных данных в Роскомнадзор автоматически влечет за собой включение организации в реестр операторов и, соответственно, в список плановых проверок.

rkn.gov.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.

Обращение субъекта персональных данных – основание для проверки

Порядок проведения проверок



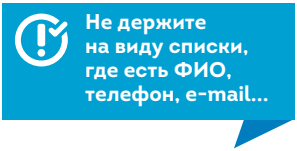
С 1 сентября 2015 года положения Федерального закона от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» при осуществлении контроля и надзора за обработкой персональных данных не применяются.

Несмотря на отмену распространения положений 294-ФЗ на осуществление контроля и надзора за обработкой персональных данных, **порядок и сроки проведения проверочных мероприятий Роскомнадзора** (Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, утвержденный приказом Минкомсвязи России от 14.11.2011 № 312) изменений не претерпели (по состоянию на октябрь 2017 года).

Срок проверки не может превышать 20 рабочих дней

Проверки Роскомнадзора могут быть плановыми и внеплановыми, которые, в свою очередь, подразделяются на документарные и выездные. Срок проверки не может превышать 20 рабочих дней (в исключительных случаях – может быть продлен еще не более чем на 20 рабочих дней).

Проверки проводятся на основании распоряжения (приказа) руководителя подразделения Роскомнадзора, результаты проверок оформляются актом, а копии распоряжения и акта проверки вручаются представителю проверяемой организации.



В случае проведения документарной проверки, у НКО будут запрошены следующие документы:

- внутренние документы (приказы, положения и др.);
- сведения, содержащиеся в уведомлении (ответственное лицо, сведения об организации и т.д.).

В случае проведения выездной проверки у НКО могут запросить:

- те же документы, что и при документарной проверке;
- информацию, находящуюся в компьютерах, в режиме выборки;
- правила хранения персональных данных на материальных носителях;
- применение СЗИ.

Ответственность

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

- **практически любое нарушение законодательства о персональных данны**х может быть квалифицировано по статье 13.11 Кодекса РФ об административных правонарушениях (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);

За несертифицированные СЗИ грозит ответственность

- ни в коем случае **не следует использовать несертифицированные в установленном порядке средства защиты информации** и 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 в большей мере относится к деятельности различных СМИ.

Важно для 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.

Список основных нормативно-правовых актов

Список основных нормативно-правовых актов:

- Федеральный закон от 27.08.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»;

- Приказ Федеральной службы по техническому и экспортному контролю России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008 года;

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15 февраля 2008 года;

- Приказ ФСБ от 10 июля 2014 г. N 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Если Вам нужна более подробная информация

- Если Ваша организация все-таки оказалась в плане проверок, а в этой тетради Вы не нашли ответов на все интересующие Вас вопросы,

- если Вы не знаете, что ответить сотруднику Роскомнадзора на его просьбу/требование представить документы,

- если Вам просто интересно узнать больше о проверках, которые проводит Роскомнадзор,

Вы можете написать Василию Романцу (romanets@lawcs.ru) **и Александре Сазоновой** (sazonova@lawcs.ru)

Если Вам понравились наши материалы и Вы задумались о правовой безопасности Вашей организации, мы будем рады предложить Вам:

- правовой аудит внутренней документации для минимизации рисков Вашей деятельности;
- внесение изменений в учредительные документы;
- составление любых видов документов и договоров;
- юридическое сопровождение ведения внутренней документации;
- консультирование о полномочиях контролирующих органов при проведении ими проверок;
- правовую экспертизу любых заключаемых договоров;
- подготовку аналитических справок и заключений;
- консалтинговые услуги бухгалтерского сопровождения;
- проведение информационно-просветительских встреч в любом городе России.

Связаться с нами и уточнить условия Вы можете, написав Владимиру Харченко по эл. почте: kharchenko@lawcs.ru или позвонив по телефону: 8 (495) 966-06-31.