Защита персональных данных

В последнее время Операторы связи всё чаще получают запросы на приведение деятельности оператора связи в соответствие с требованиями законодательства в области персональных данных (в первую очередь – Федеральный закон № 152-ФЗ от 27.07.2006 "О персональных данных).

Связано это со вступлением с 1 июля 2017 г. в силу поправок в Кодекс РФ об административных правонарушениях, которые ощутимо расширяют ответственность операторов за несоблюдение условий обработки персональных данных. В 2019 году всё чаще территориальные управления Роскомнадзора проводят проверки Операторов на предмет защиты персональных данных. При этом, размер максимальной ответственности повысился с 10 000 до 75 000 рублей, минимальной с 1 до 15 тысяч рублей также выросло и количество возможных нарушений в этой области. Настоящая статья поможет небольшим операторам правильно выстроить систему защиты персональных данных

***

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (**субъекту персональных данных**). Наиболее распространённые виды – паспортные данные, место жительства, мобильный телефон и адрес электронной почты. Даже фамилия, имя и отчество сами по себе могут являться персональными данными (письмо Роскомнадзора от 20.01.2017 N 08АП-6054). Лица (как физические, так и юридические), которые обрабатывают персональные данные, являются **операторами персональных данных.**

В Российской Федерации обработка персональных данных (требования к обеспечению её безопасности, т.е. защита) регулируется государством. 27 июля 2006 года был принят **Федеральный закон "О персональных данных"** N 152-ФЗ.

Фактически, **обязательные требования содержатся не только в Законе** "О персональных данных", **но и в некоторых подзаконных актах**. В частности, иные важные требования к защите персональных данных содержатся в следующих нормативно-правовых актах:

1. Постановление Правительства РФ от 15.09.2008 N 687 (особенности обработки ПДн без средств автоматизации).
2. Постановление Правительства РФ от 01.11.2012 N 1119 (требования к обработке ПДн в информационных системах).
3. "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ 14.02.2008)
4. "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ 15.02.2008)
5. Приказ ФСТЭК России от 18.02.2013 N 21 (организационные и технические меры при обработке ПДн в информационных системах).

Требования к обеспечению безопасности при обработке персональных данных, установленные перечисленными актами, достаточно обширны, некоторые довольно сложны в техническом и организационном плане.

Ответственность за нарушение законодательства о персональных данных закреплена в Кодексе РФ об административных правонарушениях, в статье 13.11. Данная статья с 01 июля 2017 года насчитывает 7 составов правонарушений, размер наказаний за их совершение варьируется от 15 до 75 тыс. руб. административного штрафа. Более того, как раньше, так и после вступления в силу поправок в КоАП РФ, увеличивших штрафы и введших новые правонарушения, надзорный орган неоднократно привлекал к ответственности нарушителей законодательства в области персональных данных.

Требования законодательства в области персональных данных довольно обширны, сложны и неоднозначны, поэтому, в первую очередь, хочется узнать, **за что установлена ответственность**.

Ответ на данный вопрос даёт ст. 13.11. Кодекса Российской Федерации об административных правонарушениях:

Часть 1 статьи 13.11:

> "Обработка персональных данных в случаях, не преду-смотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных...", - штраф от 30 до 50 т.р. На что обратить внимание:

Персональные данные могут обрабатываться в следующих случаях (достаточно одного любого условия):

1. Есть согласие субъекта (НЕ ОБЯЗАТЕЛЬНО ПИСЬМЕННОЕ, т.е. "галочка" на сайте, вопрос по телефону – подойдут).
2. Вы заключили или собираетесь заключить договор с субъектом (даже если это оферта на веб-сайте и для заключения не нужна подпись). В таком случае даже согласия не нужно.
3. Вы обрабатываете персональные данные своих работников (из трудовых отношений). Здесь согласие также не нужно.
4. В иных специфических случаях, они указаны в Законе о персональ-ных данных и достаточно редки (ст. 6, ч. 1; к примеру: для защиты жизни, здоровья или иных жизненно важных интересов субъекта).

Штраф накладывают, если вы не смогли доказать, на каком основании вы обрабатываете конкретные персональные данные конкретного субъекта. Рекомендации: при сборе персональных данных на сайте необходимо перед отправкой субъектом своих данных предусмотреть, чтобы он обязательно поставил "галочку" под текстом вроде "Согласен на обработку моих персональных данных". Если данные обрабатываются в целях заключения договора и согласия нет – не обрабатывать нехарактерные для договора персональные данные (к примеру, по договору купли-продажи не стоит обрабатывать данные об образовании, профессии и воинской обязанности лица).

Часть 2 статьи 13.11:

> "Обработка персональных данных без согласия в пись-менной форме, … когда такое согласие должно быть получено … либо обработка персональных данных с нарушением … требований к составу сведений, включаемых в согласие в письменной форме …", - штраф от 15 до 75 т.р. На что обратить внимание:

Чтобы не получить штраф по данной статье необходимо придерживаться нескольких простых правил:

1. Нельзя публиковать или иным образом вносить в общедоступные источники персональные данные субъекта без его письменного согласия (для такого согласия предусмотрена особая форма).
2. Нельзя обрабатывать биометрические персональные данные или дан-ные, относящиеся к категории специальных, (медицинские данные, вероисповедание, философские взгляды) без письменного согласия.
3. Нельзя передавать персональные данные на территорию иностранных государств, которые не обеспечивают адекватную защиту прав субъектов (трансграничная передача) без письменного согласия лица.

Часть 3 статьи 13.11:

> "Невыполнение оператором предусмотренной законода-тельством Российской Федерации в области персональных данных обязанности по опуб-ликованию или обеспечению иным образом неограниченного доступа к документу, опреде-ляющему политику оператора в отношении обработки персональных данных, или сведе-ниям о реализуемых требованиях к защите персональных данных", - штраф от 15 до 30 т.р. На что обратить внимание:

Необходимо разместить на сайте Политику обработки персональных

Часть 4 статьи 13.11:

> "Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных", - штраф от 20 до 40 т.р. На что обратить внимание:

Административная ответственность наступает лишь в случае непредставления оператором информации по запросу субъекта персональных данных, оформленному в соответствии с указанными в законе требованиями. В данном случае комментарии излишни – учитывая, что запрос от субъектов персональных данных большая редкость – легче один раз ответить на письмо субъекта, чем заплатить 20-40 т.р.

Часть 5 статьи 13.11:

> "Невыполнение оператором в сроки … требования субъекта персональных данных или его представителя либо уполномоченного органа … об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки", - штраф от 25 до 45 т.р. На что обратить внимание:

Состав аналогичен части 4 ст. 13.11, т.е. сначала должно поступить требование субъекта / его представителя / Роскомнадзора, и если вы не исполните такое требование в срок – то только потом

наступает ответственность. Опять же – легче не разбираться в ситуации, удалить недостоверные данные, уведомить об этом в письменном виде субъекта персональных данных, а не выплачивать штраф.

Часть 6 статьи 13.11:

> "Невыполнение оператором … обязанности по соблюдению условий, обеспечивающих … сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния", - штраф от 25 до 50 т.р. На что обратить внимание:

Особенность данного состава в том, что штрафа не будет, если в результате нарушения не наступили какие-либо неблагоприятные последствия для субъекта персональных данных, к примеру – злоумышленник взломал базу данных вашей организации и опубликовал адреса всех сотрудников. Учитывая, что такая ситуация крайне редка для компаний среднего размера, а также то, что не всегда такие вещи может обнаружить Роскомнадзор – поводов для беспокойства мало.

На этом вся ответственность заканчивается. Более того, проверки проводит именно Роскомнадзор, как уполномоченный законом орган, а проверить технические моменты могут только ФСТЭК и ФСБ, которые по факту проверок не проводят (за очень редким исключением). Вся информация о плановых проверках содержится на сайте Роскомнадзора , включая организации, которые будут проверять в определённом году. Также за 3 дня Роскомнадзор дополнительно уведомляет о предстоящей проверке. Внеплановые же проводятся только при наличии достаточных оснований и при наличии жалобы конкретного лица (это может быть бывший работник, конкурент, просто клиент, который знает о своих правах). В таком случае Роскомнадзор уведомляет организацию за 24 часа до проверки. Исходя из этого – вероятность проверки крайне мала, а если она и есть – о проверке можно узнать заблаговременно.

Таким образом – ещё раз отмечу, что всё-таки нужно обеспечить для отсутствия претензий со стороны Роскомнадзора:

1. Должна быть опубликована Политика в отношении обработки персональных данных, а если сбор персональных данных осуществляется с помощью сайта – то Политика должна быть опубликована именно на этом сайте (прямое требование ст. 18 Закона о персональных данных).
2. Также под формой сбора персональных данных на сайте должно быть уведомление или "галочка" о том, что субъект согласен на обработку его персональных данных. В том случае, если ввод персональных данных субъектом подразумевает собой заключение договора (оферта) – то такой договор должен быть опубликован на сайте, согласие в этом случае не требуется. Договор предпочтительнее согласия.
3. Не стоит обрабатывать специальные категории персональных данных, биометрические персональные данные и передавать персональные данные клиентов и работников заграницу.
4. Всегда стоит отвечать на запросы и требования субъектов персональных данных (об уточнении, удалении, блокировании их данных). Это легче, чем оплатить штраф.
5. Также стоит подготовить минимально необходимые внутренние документы организации, которые необходимы исходя из требований законодательства и которые может затребовать Роскомнадзор как в рамках проверки, так и в рамках систематического наблюдения (мониторинга).

Стоит отметить, что перечисленные условия – это лишь необходимый минимум и в каждом конкретном случае оператору может потребоваться большая степень обеспечения безопасности обработки персональных данных.

Наконец, следует упомянуть о том, почему оферта лучше, чем согласие и что делать с уведомлением Роскомнадзора о начале обработки персональных данных. Согласно ст. 22 Закона о персональных данных оператор персональных данных до начала обработки обязан уведомить надзорный орган о своих намерениях обрабатывать персональные данные. На основании такого уведомления Роскомнадзор вносит оператора в Реестр операторов персональных данных. Это, в свою очередь, повысит требования к оператору (систематически обновлять сведения о себе и о своей деятельности в Реестре), а также риск попасть под плановую проверку. В ч. 2 ст. 22 Закона о персональных данных предусмотрены исключения, т.е. те условия, при которых можно и не подавать уведомление, не попасть в реестр. К таким исключениям законодатель относит следующие условия:

1. Персональные данные обрабатываются в соответствии с трудовым законодательством (данные работников)
2. Персональные данные обрабатываются в связи с заключением договора (персональные данные клиентов и потенциальных клиентов).
3. Персональные данные обрабатываются при непосредственном участии человека (без

использования средств автоматизации – биллинга и т.п.).
4. Некоторые специфические условия – персональные данные членов общественных объединений и религиозных организаций, только ФИО субъектов и т.д., см ч. 2 ст. 22 Закона о персональных данных.

Из указанного перечня следует, что если данные обрабатываются исключительно на основании согласия субъекта (даже не письменного) – то направлять уведомление в Роскомнадзор всё же следует. Так что если, к примеру, сайт вашей организации предусматривает две формы сбора персональных данных – заявка на подключение (ФИО, адрес подключения, паспортные данные), а также – форма обратной связи для вопросов рекомендуется осуществить следующие действия. По заявке на подключение – необходимо, чтобы на сайте была оферта, и таким образом – вводя свои персональные данные, потенциальный абонент уже заключает с вами договор. В форме обратной связи лучше всего будет оставить лишь два поля: электронный адрес и поле, куда непосредственно вводится вопрос лица: таким образом, сбор персональных данных осуществляться не будет.

С другой стороны – даже если не производить указанные выше действия и оставить согласие – сначала Роскомнадзор "любезно" пришлёт требование направить ему уведомление о начале обработки персональных данных. В ответ на него можно направить соответствующее уведомление, либо информационное письмо, в котором обосновать наличие исключений, позволяющих не "включаться" в Реестр операторов персональных данных.

В настоящее время нет большой разницы в действиях Роскомнадзора в зависимости от того, включена компания в Реестр или нет, так как требования законодательства в области персональных данных необходимо соблюдать в обоих случаях.

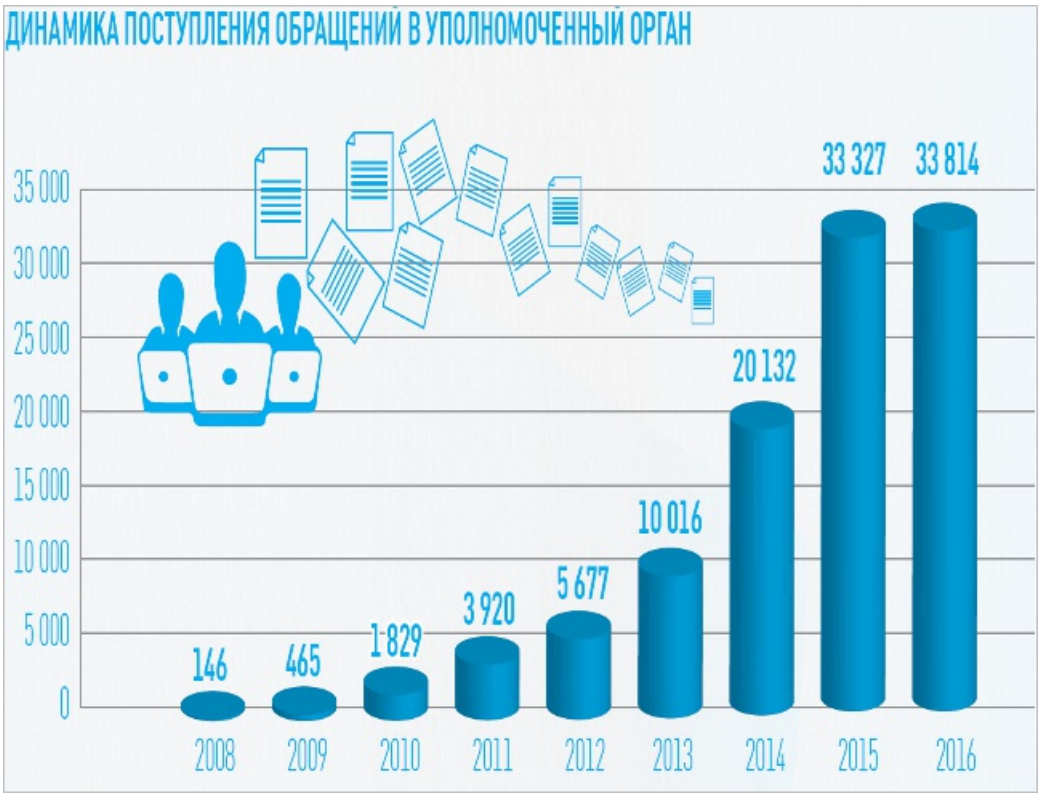
При выборе мер по обеспечению соблюдения требований законодательства в области персональных данных необходимо учитывать множество обстоятельств, включая размеры организации, качество внутренней документации и форм договоров, а также потенциальный уровень риска попасть в поле зрения надзорного органа.

В настоящее время контроль и надзор осуществляется административным органом в двух формах. **Во-первых, в виде проверки (плановой или внеплановой).** Плановые проверки проводятся в отношении лиц, сведения о которых содержатся в Реестре операторов персональных данных, который ведёт Роскомнадзор (далее – "Реестр"). Сведения об операторе заносятся в Реестр только после отправки таким оператором **уведомления о начале обработки персональных данных.** Вследствие того, что направление указанного уведомления существенно повышает риск попасть под проверку надзорного органа – мы не рекомендуем своим клиентам направлять уведомление, особенно ввиду того, что при грамотно составленной документации это абсолютно законно. Вместе с тем при наличии письменных запросов территориального управления Роскомнадзора, следует под угрозой штрафа включиться в Реестр.

Внеплановые проверки могут проводиться по нескольким основаниям, наиболее частым из которых, на сегодняшний день, является подача **жалобы клиентом и третьим лицом.**

Также возможны мероприятия систематического наблюдения, а именно: осмотр сайта на предмет соблюдения законодательства в области защиты персональных данных.

В нижеуказанной таблице отражены проверки Роскомнадзора по Персональным данным.



В 2018 уже проведено 832 плановых и 49 внеплановых проверок и 2118 мероприятий систематического наблюдения. По результатам: проверок выдано 768 предписаний, а по результатам наблюдений - 569 предписаний. За 2018 год Роскомнадзор направил в суды 6 419 протоколов об АП, **Сумма штрафов по которым 3, 971 миллионов рублей (из Публичного доклада Роскомнадзора за 2018 год).**

Очевидно, что чем больше клиентов, т.е. чем крупнее организация, тем больше шанс спровоцировать недовольство абонентов и вследствие этого получить жалобу. В этой связи необходимо выстроить наиболее эффективный и качественный процесс работы с физическими лицами, максимально соблюдать требования законодателя. Для таких организаций, которые работают с большим количеством абонентов, которые включены в Реестр, а также в отношении которых есть основания ожидать "интерес" со стороны административного органа, мы готовим стандартный пакет документов. В него входит ряд локальных, технических и публичных актов, которые позволяют минимизировать риски административных штрафов при **детальной документарной проверке** Роскомнадзора на предмет соблюдения законодательства в сфере персональных данных (список ниже).

Если шанс жалобы абонента на вашу организацию минимален и уведомление в Роскомнадзор о начале обработки персональных данных не подано – то вероятность плановой / внеплановой проверки Роскомнадзором вашей организации на порядок ниже. Зато есть большая вероятность попасть под **мероприятие систематического наблюдения** (мониторинг). При мониторинге у Роскомнадзора нет возможности ознакомиться с внутренним положением дел в организации, они смотрят лишь на внешнюю деятельность (в 99% случаев – веб-сайт, большинство штрафов и предписаний при мониторинге выносится за несоблюдение требований законодательства на сайте). Однако и за нарушения на сайте – выдают штраф **от 15 до 30 тысяч рублей** Более того, мало отделаться штрафом, Роскомнадзор также уже сейчас запрашивает у Оператора описание мер, предпринятых для устранения нарушения под угрозой штрафа в размере от **3 до 5 тысяч рублей** за не исполнение предписания по ст. 19.7 КоАП РФ.

Для отсутствия штрафов необходимо подготовить пакет документов, который позволит не допустить внешние нарушения законодательства.

Наиболее частыми нарушениями, выявленными Роскомнадзором за 2018 год являются:

- ОТСУТСТВИЕ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.
- НЕИЗДАНИЕ И/ИЛИ НЕОПУБЛИКОВАНИЕ ЮРИДИЧЕСКИМ ЛИЦОМ ДОКУМЕНТА, ОПРЕДЕЛЯЮЩЕГО ПОЛИТИКУ ОПЕРАТОРА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ; - НЕИЗДАНИЕ ЮРИДИЧЕСКИМ ЛИЦОМ ЛОКАЛЬНЫХ АКТОВ ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.
- НЕОСУЩЕСТВЛЕНИЕ ВНУТРЕННЕГО КОНТРОЛЯ/АУДИТА СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
- НЕОЗНАКОМЛЕНИЕ РАБОТНИКОВ ОПЕРАТОРА, НЕПОСРЕДСТВЕННО ОСУЩЕСТВЛЯЮЩИХ

ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, С ПОЛОЖЕНИЯМИ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ О ПЕРСОНАЛЬНЫХ ДАННЫХ, ДОКУМЕНТАМИ, ОПРЕДЕЛЯЮЩИМИ ПОЛИТИКУ ОПЕРАТОРА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ЛОКАЛЬНЫМИ АКТАМИ ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, И/ИЛИ НЕПРОВЕДЕНИЕ ОБУЧЕНИЯ УКАЗАННЫХ РАБОТНИКОВ.

Укажем минимально необходимые действия для обеспечения защиты персональных данных. Для начала следует разобраться с тем, что же представляют собой персональные данные. В упомянутом законе определено, что персональные данные, это **любая информация,** относящаяся к прямо или косвенно определённому физическому лицу. Довольно широкое понятие, охватывающее всю информацию, начиная с ФИО человека, его даты рождения и заканчивая религиозными убеждениями. Закон обязывает всех, кто обрабатывает персональные данные (операторов персональных данных) обеспечивать надлежащую безопасность такой обработки. Это выражается в предъявлении требований к операторам персональных данных относительно способов обработки, гарантий нераспространения и недопущения утечек персональных данных. Роскомнадзором могут проводиться проверки соблюдения таких требований, а в случае нарушения законодательства налагаться административная ответственность.

Что же необходимо, и что требует надзорный орган на практике? Во-первых, субъект, данные которого обрабатываются, должен быть осведомлён о подобной обработке, равно как и об условиях, на которых обрабатываются данные. Это выражается в **получении** однозначно определённого **согласия субъекта на обработку его персональных данных**…Нарушения в данной области легче всего выявляются и фиксируются, путём систематического наблюдения за ресурсами организации и наказываются штрафом 15-30 тысяч рублей. Учитывая постоянные изменения законодательства в области персональных данных очень важно размещать только актуальную версию документа, так как претензии предъявляются не только к наличию самого документа, но и к его качеству.

Во-вторых, обработка персональных данных внутри организации должна быть максимально безопасной. Это означает, что в случае обработки персональных данных с использованием информационных систем (читай – на любом электронном устройстве) необходимо разработать модель потенциальных угроз в отношении персональных данных. В соответствии с моделью необходимо все эти угрозы устранить или минимизировать. Здесь и встаёт вопрос о том, как доказать Роскомнадзору соблюдение установленных законодательством требований. Учитывая специфику проведения проверки (документарная) – необходимо максимально качественно составить комплект локальной и технической документации, который не оставит надзорному органу ни малейшего шанса придраться к оператору связи.

Основываясь на многолетнем опыте и профессионализме наших сотрудников, разработан, успешно применяется и систематически обновляется уникальный пакет документов, помогающих максимально соблюсти требования законодательства и успешно пройти проверку в любом регионе Российской Федерации.

В рамках подготовки соответствия Системы защиты персональных данных Оператора связи законодательству Российской Федерации, необходимо подготовить нижеследующие документы:

- Приказ о назначении комиссии по приведению в соответствие с требованиями законодательства в области Персональных данных.
- Положение о комиссии по приведению в соответствие с требованиями законодательства в области Персональных данных.
- План мероприятий по приведению в соответствие с требованиями законодательства в области Персональных данных.
- Приказ об утверждении списка лиц, имеющих доступ к обработке Персональных данных.
- Форма Обязательства о неразглашении Персональных данных.
- Приказ о проведении внутренней проверки в области Персональных данных.
- Перечень Персональных данных, подлежащих защите.
- Форма согласия абонента на обработку Персональных данных.
- Форма согласия сотрудника на обработку персональных данных.
- Приказ о выделении помещений для обработки Персональных данных.
- Перечень информационных систем Персональных данных.
- Технический паспорт информационных систем Персональных данных.
- Приказ о назначении ответственного администратора информационной безопасности.
- Инструкция администратора информационной безопасности.
- Приказ об утверждении Положений в области Персональных данных.
- Положение об обработке Персональных данных (Политика).
- Положение о защите Персональных данных.
- Положение о хранении Персональных данных.
- Приказ о классификации информационных систем Персональных данных.
- Акт классификации информационных систем Персональных данных.

- Приказ об утверждении Инструкции пользователя информационных систем Персональных данных.
- Инструкция пользователя информационных систем Персональных данных.
- Порядок резервирования и восстановления Персональных данных.
- План внутренних проверок в области Персональных данных.
- Регламент по реагированию на запросы субъектов Персональных данных.
- Инструкция о порядке обращения с носителями Персональных данных.
- Правила внутреннего контроля в области Персональных данных.