Практические аспекты выполнения действующего законодательства в области ПДн

Проведение внутреннего аудита

Левиев Дмитрий Олегович

эксперт
НОУ «Академия Информационных Систем»

Основные понятия и определения в области обработки Персональных данных

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

До 25 июля 2011:

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Основные понятия и определения в области обработки Персональных данных

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Основные понятия и определения в области обработки Персональных данных

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Основные понятия и определения в области обработки Персональных данных

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

до 25.07.2011

Обработка ПДн в ИСПДн считается не автоматизированной, если такие действия с ПДн, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Основные понятия и определения в области обработки Персональных данных

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

До 25 июля 2011:

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Основные понятия и определения в области обработки Персональных данных

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Основные понятия и определения в области обработки Персональных данных

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Основные понятия и определения в области обработки Персональных данных

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Основные понятия и определения в области обработки Персональных данных

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Основные понятия и определения в области обработки Персональных данных

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

До 25.07.2011:

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств

Основные понятия и определения в области обработки Персональных данных

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Законодательство Российской Федерации в области обработки персональных данных

- Конституция РФ
- Трудовой кодекс
- Федеральный закон «О персональных данных» №152-ФЗ с изменениями и дополнениями
- Иные федеральные законы РФ определяющие случаи и особенности обработки ПДн

Уведомление Роскомнадзора

- Уведомление должно содержать следующие сведения:
  - наименование (фамилия, имя, отчество), адрес оператора
  - цель обработки персональных данных
  - категории персональных данных
  - категории субъектов, персональные данные которых обрабатываются;
  - правовое основание обработки персональных данных;
  - перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
  - описание мер, предусмотренных статьями 18.1 и 19 152-ФЗ, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
  - фамилия, 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;
  - дата начала обработки персональных данных;
  - срок или условие прекращения обработки персональных данных;
  - сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
  - сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

Внесение изменений в реестр операторов персональных данных

- В случае изменения сведений, указанных уведомлении, а также прекращения обработки оператор обязан уведомить об изменениях Роскомнадзор в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Обязанности оператора

- Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 статьи 18 152-ФЗ, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

  1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

  2) цель обработки персональных данных и ее правовое основание;

  3) предполагаемые пользователи персональных данных;

  4) Установленные Федеральным законом права субъекта персональных данных;

  5) источник получения персональных данных.

Обязанности оператора

- Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 статьи 18 152-ФЗ, в случаях, если:

  1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

  2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

  3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

  4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

  5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 статьи 18 152-ФЗ, нарушает права и законные интересы третьих лиц.

Обязанности оператора

- Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено 152-ФЗ или другими федеральными законами.

Обязанности оператора

- К принимаемым мерам могут, в частности, относиться:

  1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

  2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

  3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 152-ФЗ;

Обязанности оператора

- К принимаемым мерам могут, в частности, относиться:

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

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

Обязанности оператора

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

Обязанности оператора

- Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети

Обязанности оператора

- Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами

Обязанности оператора

- Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных

Обязанности оператора

- Обеспечение безопасности персональных данных достигается, в частности:

  1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

  2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

  3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

  4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

Обязанности оператора

- Обеспечение безопасности персональных данных достигается, в частности:

  5) учетом машинных носителей персональных данных;

  6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

  7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

  8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

  9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

Виды электронных подписей:

- простая электронная подпись;
- усиленная электронная подпись (различаются ***усиленная неквалифицированная электронная подпись*** и ***усиленная квалифицированная электронная подпись***).

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

Простая электронная подпись - электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Федеральный закон Российской Федерации от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности"

Федеральный закон регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности.

Федеральный закон Российской Федерации от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности"

Лицензированию подлежат следующие виды деятельности:

- разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (крипто графических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

Федеральный закон Российской Федерации от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности"

Лицензированию подлежат следующие виды деятельности:

- разработка и производство средств защиты конфиденциальной информации;
- деятельность по технической защите конфиденциальной информации.

Меры по обеспечению безопасности персональных данных при их обработке

- Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии со статьей 19 152-ФЗ, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

Защита персональных данных

- Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с статьей 19 152-ФЗ, при обработке персональных данных в государственных информационных системах персональных данных осуществляются ФСБ России и ФСТЭК России в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных

Защита персональных данных

- ФСБ России и ФСТЭК России решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с статьей 19 152-ФЗ, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных

ТЗКИ. Определение конфиденциальной информации для лицензирования

- Конфиденциальная информация для целей лицензирования – информация, не содержащая сведения, составляющие государственную тайну, но защищаемая в соответствии с законодательством Российской Федерации (согласно ПП79)

ТЗКИ. Лицензируемые виды работ и услуг

- Контроль защищенности конфиденциальной информации по техническим каналам в:
  - средствах и системах информатизации;
  - технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;
  - помещениях со средствами (системами), подлежащими защите;
  - помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения).

ТЗКИ. Лицензируемые виды работ и услуг

- Контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.
- Сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

ТЗКИ. Лицензируемые виды работ и услуг

- Аттестационные испытания и аттестация на соответствие требованиям по защите информации:
  - средств и систем информатизации;
  - помещений со средствами (системами) информатизации, подлежащими защите;
  - защищаемых помещений.

ТЗКИ. Лицензируемые виды работ и услуг

- Проектирование в защищенном исполнении:
  - средств и систем информатизации;
  - помещений со средствами (системами) информатизации, подлежащими защите;
  - защищаемых помещений.

ТЗКИ. Лицензируемые виды работ и услуг

- Установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

ТЗКИ. Требования к персоналу

- Наличие в штате (штатном расписании) не менее двух специалистов имеющих:
  - высшее профессиональное образование в области технической защиты информации
  - либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации

ТЗКИ. Требования к помещению (защищенное помещение)

- Наличие помещения для осуществления деятельности принадлежащего лицензиату на праве собственности или на другом законном основании (договоре аренды) и имеющий аттестат соответствия техническим нормам и требованиям по технической защите информации, установленные ФСТЭК России

ТЗКИ. Требования к АС

- Использование аттестованных в установленном порядке АС для обработки конфиденциальной информации (3Б, 2Б, 1Г)
- Использование средств защиты информации сертифицированных в установленном порядке по требованиям защиты информации для защиты конфиденциальной информации
- Использование ПО для лицензионной деятельности на основании договора с правообладателем (4 часть ГК РФ)

ТЗКИ. Требования к наличию контрольно-измерительного оборудования

- Наличие на любом законном основании (право собственности/аренды/лизинга) производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию
- Перечень оборудования определяется ФСТЭК России.
- Необходимо для работ и услуг:
  - контроль защищенности от утечки по техническим каналам
  - сертификационные испытания
  - аттестационные испытания
  - установка, монтаж, испытания, ремонт СЗИ

ТЗКИ. Требования к наличию средств контроля защищенности по НСД

- Наличие на праве собственности или на ином законном основании средств контроля защищенности информации от несанкционированного доступа, сертифицированных по требованиям безопасности информации
- Перечень средств определяется ФСТЭК России.
- Необходимо для работ и услуг:
  - контроль защищенности от НСД
  - сертификационные испытания
  - аттестационные испытания

ТЗКИ. Требования к наличию нормативно-методической базы

- Наличие технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг по вопросам технической защиты информации в соответствии с перечнем, установленным ФСТЭК России
- Перечень опубликован на официальном сайте ФСТЭК России на странице http://www.fstec.ru/_razd/_ispo.htm
  - 15 нормативно правовых актов
  - 28 нормативно-методических и методических документов (часть ДСП)
  - 44 стандарта

ТЗКИ. Требования к системы производственного контроля

- Наличие системы производственного контроля в соответствии с установленными стандартами (для сертификационных испытаний)

ТЗКИ. Проверки

- Плановые проверки проводятся через 1 год после получения лицензии и через 3 (три) года после последней плановой проверки
- Проверки проводятся документарном виде (без выезда к лицензиату) и выездные.
- Внеплановые проверки проводятся совместно с Прокуратурой РФ.
- Основание внеплановой проверки – окончания срока предписания об устранении нарушений.
- Проведение внеплановой проверки не отменяет плановую проверку.

ТЗКИ. Нарушения лицензионных требований

- Грубое нарушение:
  - Отсутствие в штате сотрудников, отвечающих лицензионным требованиям
  - Отсутствие необходимого оборудования
  - Отсутствие необходимых средств контроля защищенности (НСД)
  - Отсутствие или окончание срока действия аттестата на АС
  - Использованием нелицензионного ПО
  - Отсутствие системы производственного контроля (только для сертификации)

Лицензирование в области работы с криптографическими средствами

- Виды лицензий:
  - Техническое обслуживание шифровальных (криптографических) средств (тип Х, ФСБ России)*
  - Оказание услуг по шифрованию информации (тип У, ФСБ России)*
  - Распространение шифровальных (криптографических) средств (тип Р, ФСБ России)*

  * *С 3 ноября 2011 должна выдаваться одна лицензия на СКЗИ, однако до сих пор нет соответствующего Постановления Правительства.*
- Общие нормативные документы:
  - Приказ №66 от 09.02.2005 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»
  - Приказ ФАПСИ № 152 от 13.06.2001 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Порядок обработки ПДн при передаче их во внешнюю организацию

- Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора).

Порядок обработки ПДн при передаче их во внешнюю организацию

- Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные 152-ФЗ.

Порядок обработки ПДн при передаче их во внешнюю организацию

- В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 152-ФЗ.

При оформлении отношений с Третьей стороной, оператор должен:

- Издать документ, определяющий политику обработки ПДн;
- Подготовить поручение Третьей стороне;
- Внести изменения в договор с Третьей стороной;
- Заключить с Третьей стороной соглашение о конфиденциальности;
- Организовать контроль обработки ПДн у Третьей стороны.

Поручение Оператора на обработку ПДн должно содержать:

- Цель обработки и состав ПДн, подлежащих обработке;
- Перечень действий (операций) Третьей стороны с ПДн;
- Уровень защищенности ПДн, подлежащий обеспечению;
- Требования к защите обрабатываемых ПДн;
- Порядок уничтожения ПДн по завершении их обработки;
- Порядок оценки эффективности принятых мер защиты ПДн.

Изменения в Договоре с Третьей стороной:

- Обязанность соблюдения законных принципов обработки ПДн;
- Обязанность обеспечения безопасности ПДн;
- Обязанность не раскрывать третьим лицам и не распространять ПДн;
- Обязанность выполнять технические и организационные меры, указанные в техническом заднии, яляющимся обязательнм приложением к доворору;
- Обязанность установить правила доступа к ПДн;
- Обязанность провести оценку эффективности мер защиты ПДн;
- Право оператора осуществлять проверку порядка обработки ПДн;
- Санкции за нарушение порядка обработки ПДн.

Лица, ответственные за организацию обработки персональных данных в организациях

- Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.
- Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.
- Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 152-ФЗ.

Лица, ответственные за организацию обработки персональных данных в организациях

- Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:
- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Примерный список запрашиваемых документов при проверке Роскомнадзором Оператора персональных данных

- учредительные документы Оператора;
- копия уведомления об обработке персональных данных;
- положение о порядке обработки персональных данных;
- положение о подразделении, осуществляющем функции по организации защиты персональных данных;
- должностные регламенты лиц, имеющих доступ к персональным данным;
- план мероприятий по защите персональных данных;
- план внутренних проверок состояния защиты персональных данных;
- приказ о назначении ответственных лиц по работе с персональными данными;
- типовые формы документов, предполагающие или допускающие содержание персональных данных;

Примерный список запрашиваемых документов при проверке Роскомнадзором Оператора персональных данных

- журналы, реестры, книги, содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях;
- договоры с субъектами персональных данных, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных; выписки из ЕГРЮЛ, содержащие актуальные данные на момент проведения мероприятия по контролю (надзору);
- приказы об утверждении мест хранения материальных носителей персональных данных;
- письменное согласие субъектов персональных данных на обработку их персональных данных (типовая форма);
- распечатки электронных шаблонов полей, содержащие персональные данные; справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка персональных данных;

Примерный список запрашиваемых документов при проверке Роскомнадзором Оператора персональных данных

- заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке (проверяется только наличие данных документов);
- приказ о создании комиссии и акты проведения классификации информационных систем персональных данных (проверяется только наличие данных документов);
- журналы (книги) учета обращений граждан (субъектов персональных данных);
- акт об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения цели обработки);
- иные документы, отражающие исполнение Оператором требований законодательства Российской Федерации в области персональных данных.

Проведение внутренних проверок

- Ежегодный план проверочных мероприятий, утвержденный руководителем организации
- Проверки организует Ответственный за организацию обработки персональных данных
- Обязательные пункты плана:
  - Проверка законности обработки
  - Проверка наличия документов и их актуальность
  - Проверка выполнения требований по защите персональных данных
  - Проверка уничтожения данных
  - Своевременность передачи данных на архивное хранение

Примеры ситуаций Внутриобъектовый режим

- Положение о внутриобъектовом режиме
- Инструкция по разграничению доступа в отдельные помещения
- Договор с ЧОП
- Инструкция по пропускному режиму
- Порядок идентификации субъекта для прохода на территорию, в том числе без представления подтверждающих документов
- Форма журнала учета посетителей
- Инструкция по ведения журнала учета посетителей
- Требования к сотруднику ЧОП (охраннику)
- Согласованные особенности эксплуатации технических средств ЧОП

Примеры ситуаций
Обращение с медицинской документацией

- Классы клиентов:
  - Пациенты возраста от 0 до 14 лет
  - Пациенты возраста от 14 до 16 лет
  - Пациенты возраста от 16 до 18 лет
  - Пациенты возраста старше 18 лет
  - Частично недееспособные пациенты
  - Недееспособные пациенты

Примеры ситуаций
Обращение с медицинской документацией

- Контроль выдачи медицинской документации
- Места хранения медицинской документации
- Контроль целостности медицинской документации
- Выполнение требований к носителям медицинской документации
- Использование технических мер для контроля перемещения медицинской документации (RFID-метки)

Предоставление копий медицинской документации пациенту

- ЛПУ обязано предоставлять безвозмездно копии медицинской документации пациенту в **доступной форме**
- Изготовление копий путем фотокопирования (ксерокс) является автоматизированной обработкой ПДн, т.к. копировальные аппараты являются средствами вычислительной техники.
- При использовании электронных карт (документов) должны использоваться средства защиты от изменения содержимого документа и подтверждения авторства – квалифицированная усиленная электронная подпись

Контакты

Левиев Дмитрий Олегович
Эксперт
Академия Информационных Систем
Тел./факс +7 495 231-3049
E-mail dleviev@infosystem.ru
http://www.infosystems.ru