Академия·ИБ

Особенности обработки персональных данных в государственных и муниципальных учреждениях

Дорошенко Руслан
директор АНО ДПО и ЭУ
«Академия Информационной Безопасности»

ЗАКОНОТВОРЧЕСТВО. ИСТОЧНИКИ

Академия·ИБ

Федеральный закон от 21.07.2014 N 242-ФЗ (ред. от 31.12.2014) "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях"

Постановление Правительства РФ от 19 августа 2015 г. N 857 "Об автоматизированной информационной системе "Реестр нарушителей прав субъектов персональных данных"

Проект Постановления Правительства Российской Федерации от 17.04.2015 «Об утверждении Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям законодательства Российской Федерации»

ОПРЕДЕЛЕНИЯ

Академия·ИБ

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

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно 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.

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.

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

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

«ТИХАЯ» СМЕНА ПРАВИЛ ИГРЫ

Академия·ИБ

Федеральный закон от 21.07.2014 N 242-ФЗ (ред. от 31.12.2014) "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях"

Внесение изменений в Федеральные законы:

ФЗ-152 «О персональных данных»;

ФЗ-294 «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;

ФЗ-149 «Об информации, информационных технологиях и о защите информации».

«ТИХАЯ» СМЕНА ПРАВИЛ ИГРЫ

Академия·ИБ

ФЗ-152 «О персональных данных»:

Статья 23. Уполномоченный орган по защите прав субъектов персональных данных
3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:
…
3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации

«ТИХАЯ» СМЕНА ПРАВИЛ ИГРЫ

Академия·ИБ

ФЗ-152 «О персональных данных»:

Статья 22. Уведомление об обработке персональных данных
Уведомление должно содержать следующие сведения:

…

10.1) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

РЕГУЛЯТОРЫ

Роскомнадзор

ФСТЭК России

ФСБ России

РЕГУЛЯТОРЫ

Академия·ИБ

ГОСУДАРСТВЕННАЯ ИНСПЕКЦИЯ ТРУДА В ЛИПЕЦКОЙ ОБЛАСТИ

Государственная инспекция труда (Роструд)

Прокуратура

РОСКОМНАДЗОР

Академия·ИБ

Виды деятельности:

- организация и проведение проверок;
- принятие мер по пресечению и устранению последствий выявленных нарушений;
- анализ и оценка состояния исполнения требований законодательства на основании представленных операторами документов и локальных актов;
- проведение мероприятий систематического наблюдения.

РОСКОМНАДЗОР

Академия·ИБ

Основания проведения внеплановых проверок (некоторые):

- истечение срока исполнения оператором выданного предписания ;

- поступление в Роскомнадзор информации, в том числе от СМИ о подтвержденных фактах нарушения законодательства РФ при обработке ПДн;

- нарушение оператором требований законодательства, выявленного в ходе систематического наблюдения

Не требуется согласования с Прокуратурой плановых и внеплановых проверок!!!

РОСКОМНАДЗОР

Академия·ИБ

Права должностных лиц РКН («цветочки»):

- запрашивать и получать от оператора информацию, документы и локальные акты связанные с обработкой ПДн;
- посещать и проводить обследования используемых оператором зданий, помещений, сооружений, ИСПДн, оборудования, а так же проводить необходимые исследования;
- выдавать обязательные для выполнения предписания об устранении нарушений;
- использовать технику и оборудование, принадлежащее Роскомнадзору;
- получать доступ к ИСПДн для оценки законности деятельности по обработке ПДн;
- проверять и оценивать принятые оператором меры для обеспечения обязанностей, предусмотренных законодательством;

Академия·ИБ

РОСКОМНАДЗОР

Права должностных лиц РКН («ягодки»):

- выдавать обязательные для исполнения требования о приостановлении или прекращении обработки ПДн, осуществляемых с нарушениями;
- выдавать обязательные для исполнения требования об уничтожении или блокировании недостоверных или полученных незаконным путем ПДн;
- Составлять протоколы об административном правонарушении в порядке, установленном законодательством РФ.

РОСКОМНАДЗОР

Академия·ИБ

Правонарушение	Нарушаемая статья законодательства	Наказание для должностных лиц	Наказание для юридических лиц
Нарушение требований к согласию	Ст. 9 ФЗ-152	10 – 20 тыс. руб.	15 – 75 тыс. руб.
Обработка ПДн без согласия	Ст. 6 ФЗ-152	5 - 10 тыс. руб.	30 - 50 тыс. руб.
~~Незаконная обработка спецкатегорий ПДн~~	~~Ст. 10 ФЗ-152~~	~~10 - 25 тыс. руб.~~	~~150 – 300 тыс. руб.~~
Неопубликование политики в области ПДн	Ст. 18.1 ФЗ-152	3 - 6 тыс. руб.	15 – 30 тыс. руб.
Отказ в предоставлении информации субъекту	Ст. 14, 20 ФЗ-152	4 – 10 тыс. руб.	25 – 40 тыс. руб.
~~Отказ в уничтожении или блокировании ПДн~~	~~Ст. 21 ФЗ-152~~	~~4 – 10 тыс. руб.~~	~~25 – 45 тыс. руб.~~
Нарушение правил хранения носителей ПДн	ПП – 687	4 – 10 тыс. руб.	25 – 50 тыс. руб.
Нарушение правил обезличивания (для гос.)	ПП-211 и приказ РКН 996	3 – 6 тыс. руб.	Не предусмотрено

ЧТО ДЕЛАТЬ?

Академия·ИБ

- аудит процессов автоматизированной и неавтоматизированной обработки персональных данных на соответствие требованиям законодательства РФ;
- критический взгляд на процессы сбора ПДн с использованием сети Интернет;
- при необходимости изменение архитектуры ИСПДн с обеспечением первичной записи и хранения данных на территории РФ;
- актуализация организационно-распорядительной документации по обработке и при необходимости защите ПДн;
- повышение осведомленности персонала, задействованного в процессах обработки ПДн, в вопросах требований законодательства.

КЛАССИФИКАЦИЯ ГИС

Академия·ИБ

Приказ ФСТЭК России №17 от 11.02.2013

«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Классификация ГИС проводится на основании определяемого уровня значимости и масштаба информационной системы.

ОПРЕДЕЛЕНИЕ УРОВНЯ ЗНАЧИМОСТИ

Академия·ИБ

Уровень значимости (УЗ) определяется степенью возможного ущерба для обладателя информации и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.

УЗ – высокий – в результате нарушения свойств безопасности возможны существенные негативные последствия в социальной , политической, экономической и иных областях деятельности и информационная система или оператор не могут выполнять своих функций. (УЗ 1)

УЗ – средний– в результате нарушения свойств безопасности возможны умеренные негативные последствия в социальной , политической, экономической и иных областях деятельности и информационная система или оператор не могут выполнять хотя бы одну из функций. (УЗ 2)

ОПРЕДЕЛЕНИЕ УРОВНЯ ЗНАЧИМОСТИ

Академия·ИБ

УЗ – низкий – в результате нарушения свойств безопасности возможны незначительные негативные последствия в социальной , политической, экономической и иных областях деятельности и информационная система или оператор могут выполнять свои функции, с привлечением дополнительных средств и сил. (УЗ 3)

УЗ 4 – не может быть определена степень ущерба, но требования по защите информации существуют.

КЛАССИФИКАЦИЯ

Академия·ИБ

Уровень значимости	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К 1	К 1	К 1
УЗ 2	К 1	К 2	К 2
УЗ 3	К 2	К 3	К 3
УЗ 4	К 2	К 3	К 4

На основании класса ГИС – К1, К2, К3, К4 - согласно

«Составу мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы»

определяются необходимые мероприятия по защите информации.

Академия·ИБ

Спасибо за внимание!

Дорошенко Руслан
директор АНО ДПО и ЭУ
Академия Информационной Безопасности