Институт мониторинга и оценки информационной безопасности

Учебный центр «АСТА-информ»

Февральская революция 2017 г. в персональных данных

Астахов Александр Геннадьевич
ГК «АСТА-информ»

ГРУППА КОМПАНИЙ «АСТА-информ»

ООО «МКЦ «АСТА-информ»

лицензия на деятельность по технической защите конфиденциальной информации ФСТЭК РФ № 1028 от 04.03.2010 (действует бессрочно);

лицензия на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств ФСБ РФ № 271 от 30.12.2014(действует бессрочно);

ЧОУ ДПО Учебный центр «АСТА-информ»

лицензия на право осуществления образовательной деятельности Министерства образования № 7549 от 30.01.2011(действует бессрочно);

ООО «Институт мониторинга и оценки информационной безопасности»

Защита персональных данных – наше главное дело:

на 17.03.2017г.

574 – проекта по защите персональных данных

302 – аттестовано ИСПДн и ГИС

34 – подготовлено к проверкам Роскомнадзора, ФСТЭК, ФСБ по персональным данным

41 – получили консультации перед проверками Роскомнадзора

16 415 – слушателей очно обучились по различным формам обучения

24 - региона России, где проведены работы и оказаны услуги по персональным данным

КЛЮЧЕВЫЕ МОМЕНТЫ В 2017 ГОДУ

1. Роскомнадзор наделен полномочием государственного контроля и надзора за соответствием обработки ПДн требованиям законодательства РФ в сфере персональных данных.

2. Федеральным законом приняты новые составы правонарушений в сфере персональных данных, которые вступят в силу с 1 июля 2017 года.

3. Роскомнадзор получил право возбуждать административные дела напрямую, минуя прокуратуру.

Штрафы, вводимые с 01.07.2017

№	Состав административного правонарушения	Наказание для должностных лиц (руководитель учреждения и ответственный за обработку ПДн)	Наказание для учреждения (оператора ПДн)
1.	Обработка персональных данных в случаях, не предусмотренных законодательством РФ, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи	5 – 10 тысяч рублей	30 – 50 тысяч рублей

- Фотография врача на сайте
- Личная фотография в Личном деле
- Данные пациента на форуме
- Дистанционное консультирование
- Амбулаторная карта больного на местном телевидении
- Статистический талон флюорографического обследования
- Согласие пациента по ОМС

Штрафы, вводимые с 01.07.2017

№	Состав административного правонарушения	Наказание для должностных лиц (руководитель учреждения и ответственный за обработку ПДн)	Наказание для учреждения (оператора ПДн)
2.	Обработка персональных данных без согласия в письменной форме субъекта персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством РФ требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных	10 – 20 тысяч рублей	15 – 70 тысяч рублей

- **6** случаев наличия обязательного письменного согласия
- А сколько у вас форм Согласий ?
- Ваши Согласия соответствуют ст. 9 152-ФЗ?

Штрафы, вводимые с 01.07.2017

№	Состав административного правонарушения	Наказание для должностных лиц (руководитель учреждения и ответственный за обработку ПДн)	Наказание для учреждения (оператора ПДн)
3.	Невыполнение оператором предусмотренной законодательством РФ обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, и сведениям о реализуемых требованиях к защите персональных данных	3 – 6 тысяч рублей	15 – 30 тысяч рублей

- **2** случая обязательного размещения Политики на официальном сайте
- Ваша форма обратной связи на сайте содержит персональные данные?

Штрафы, вводимые с 01.07.2017

№	Состав административного правонарушения	Наказание для должностных лиц (руководитель учреждения и ответственный за обработку ПДн)	Наказание для учреждения (оператора ПДн)
4.	Невыполнение оператором предусмотренной законодательством РФ обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	4 – 6 тысяч рублей	20 – 40 тысяч рублей

- **10** случаев получения информации пациентом (работником), предусмотренных п.7. ст.14 152-ФЗ

НО

Суд отклонил иск гражданина А., т.к. его письменный запрос не соответствовал п.3.ст.14

Штрафы, вводимые с 01.07.2017

№	Состав административного правонарушения	Наказание для должностных лиц (руководитель учреждения и ответственный за обработку ПДн)	Наказание для учреждения (оператора ПДн)
5.	Невыполнение оператором в сроки, установленные законодательством РФ, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных 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	4 – 10 тысяч рублей	25 – 45 тысяч рублей

- Как вы применяете нормы ст.21 152-ФЗ:
  - ваши действия в течение 3 дней?
  - ваши действия в течение 7 дней?
  - ваши действия в течение 10 дней?
  - ваши действия в течение 30 дней?

Штрафы, вводимые с 01.07.2017

6.	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством РФ 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	4 – 10 тысяч рублей	25 – 50 тысяч рублей

- Постановление Правительства РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

«Настольная книга»

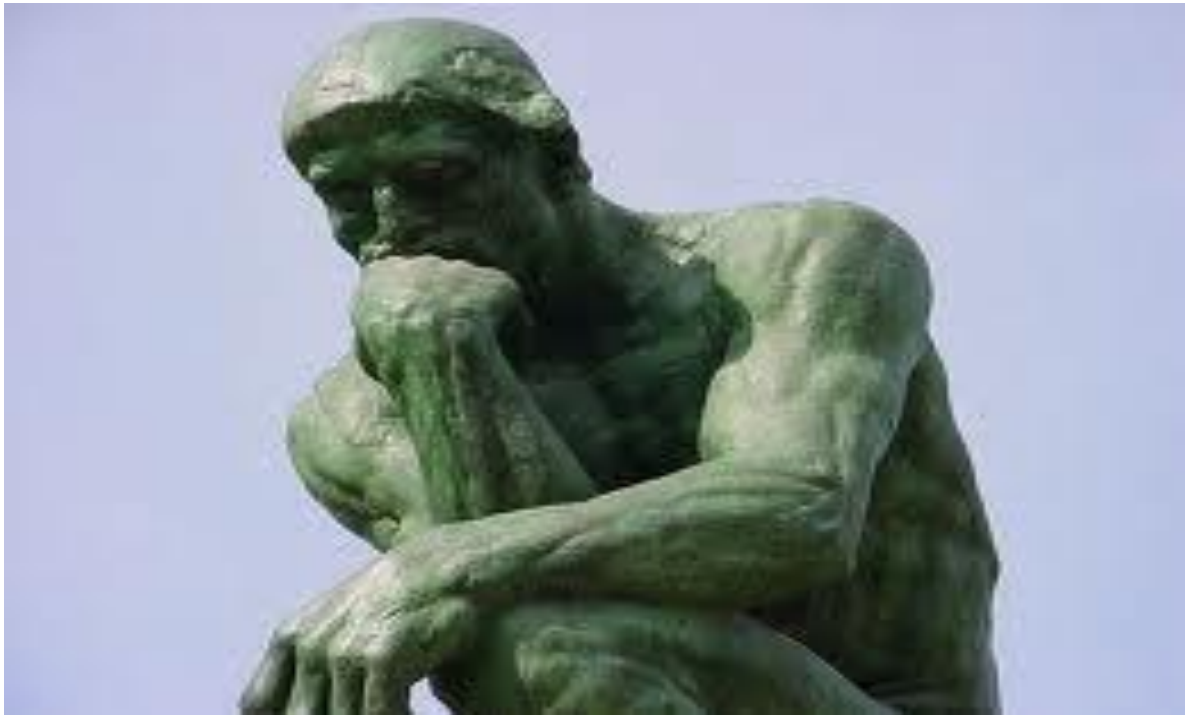
Ответственного за организацию обработки персональных данных

Штрафы, вводимые с 01.07.2017

№	Состав административного правонарушения	Наказание для должностных лиц (руководитель учреждения и ответственный за обработку ПДн)	Наказание для учреждения (оператора ПДн)
7.	Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством РФ обязанности по обезличиванию персональных данных, либо несоблюдение установленных требований или методов по обезличиванию персональных данных	3 – 6 тысяч рублей	3 – 6 тысяч рублей – только для должностных лиц

- Вы Управление здравоохранения?
- Вы обезличиваете персональные данные?
- Вы используете 4 метода обезличивания по Приказу Роскомнадзора № 996?
- Вы утвердили Правила обезличивания?
- У вас назначен ответственный за эти процедуры?

ЧТО ДЕЛАТЬ ВАМ, ЧТОБЫ НЕ ОКАЗАТЬСЯ «КРАЙНИМ» ?



Повышать осведомленность коллег

Требования законодательства к осведомленности сотрудников в сфере защиты ПДн

Статья	Требования
Федеральный Закон №152-ФЗ	Ст. 18.1 … 6) **ознакомление** работников, осуществляющих обработку ПДн, с положениями законодательства РФ, документами, определяющими политику оператора в отношении ПДн, локальными актами по вопросам обработки ПДн и **обучение** указанных работников
Постановление Правительства №211	е) осуществляет **ознакомление** служащих с положениями законодательства РФ, локальными актами по вопросам обработки ПДн и организует **обучение** указанных служащих

Статья	Требования
Постановление Правительства № 399 от 06.05.2016	…Организовать повышение квалификации специалистов и должностных лиц, ответственных за организацию защиты информации….
Приказ ФСТЭК №17	18.1 … **информирование** пользователей об угрозах безопасности информации, о правилах эксплуатации СЗИ, а также их **обучение**…
Приказ ФСБ №378	16. … назначение **ответственного** за обеспечение безопасности ПДн… 17. … назначение **обладающего достаточными навыками** должностного лица ответственным…

Статья	Требования
ГОСТ Р 51583 – 2014 Автоматизированная система в защищенном исполнении	6.13.2 … - **обучение персонала** АСЗИ и проверка его способности обеспечивать функционирование ЗИ … - **проверка и подготовка** специалистов структурного подразделения или должностного лица, ответственных за ЗИ в АСЗИ
ГОСТ РО 0043-004-2013 Программа и методики аттестационных испытаний	Д.3.5 **Проверка уровня подготовки** специалистов и распределения ответственности пользователей АС: - **оценка знания** инструкций по безопасности информации пользователями АС; - наличие системы **распределения ответственности** пользователей АС за выполнение требований безопасности информации

Спасибо за внимание!

e-mail: aag@asta74.ru

Астахов Александр Геннадьевич
ГК «АСТА-информ»