

Основные ошибки в политиках обработки персональных данных медицинских организаций

Размещение политики об обработке Пдн на сайте оператора

▶ п.2. ст.18.1 ФЗ о Пдн: 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. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, **обязан опубликовать в соответствующей информационно-телекоммуникационной сети**, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети "Интернет", с использованием которых осуществляется сбор персональных данных, 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.



Статистика



Типичные ошибки на примере 10 клиник (разместившие политику)

Нет перечня субъектов, чьи Пдн обрабатываются	Нет цели обработки	Не указаны способы обработки
Не указан порядок уничтожения Пдн	Нет сроков обработки Пдн	Нет перечня обрабатываемых Пдн
Нет контактных данных оператора для связи по вопросам обработки Пдн	Соблюдение законодательства, Устава - как правовое основание обработки Пдн	Соблюдение законодательства и Устава - как цель обработки Пдн

Ответственность

Коап

ч.3 ст.13.11 КоаП: **Невыполнение оператором** предусмотренной законодательством Российской Федерации в области персональных данных обязанности **по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора** в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных -

влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до трех тысяч рублей; на должностных лиц - от шести тысяч до двенадцати тысяч рублей; на индивидуальных предпринимателей - от десяти тысяч до двадцати тысяч рублей; на **юридических лиц - от тридцати тысяч до шестидесяти тысяч рублей.**

Ответственность

<https://52.rkn.gov.ru/news/news341221.htm>

Нарушения российского законодательства в области персональных данных

*«нарушения ч. 2 ст. 18.1 Закона (43%) - в документе, регламентирующем политику в отношении обработки персональных данных, **не перечислены все обрабатываемые оператором категории персональных данных** в рамках каждой из категорий субъектов персональных данных, не указаны все **категории субъектов** персональных данных, чьи персональные данные обрабатываются отдельно в рамках обозначенных целей обработки, а также **правовых оснований** обработки персональных данных (отсутствует структура целеполагания); **документ**, регламентирующий политику в отношении обработки персональных данных, **не размещен** на каждой странице сайта, с использованием которой осуществляется сбор персональных данных».*

Судебная практика

- Суд **оштрафовал** общество за то, что оно **не опубликовало на сайте документ, согласно которому обрабатывает и защищает персональные данные.**

- Роскомнадзор обнаружил, что общество не опубликовало на сайте или другим способом не обеспечило неограниченный доступ к документу, который определяет политику оператора в отношении обработки персональных данных, или к сведениям о реализуемых требованиях к защите персональных данных.
- Мировой суд привлек общество к ответственности **по статье 13.11 КоАП (30-60 т.р. для юридических лиц).**

- Областной **суд не принял во внимание доводы общества о том, что оно не имело возможности определять граждан с помощью формы на сайте.** «... идентифицировать физическое лицо по одному имени, без других данных (фамилия, отчество, адрес, заполнение которых в форме обратной связи не предусмотрено), не представляется возможным. К тому же в графе "Ваше имя" в форме заполнения данной формы имя не обязательно может быть настоящим. Остальные элементы заполнения формы обратной связи (тема сообщения, сообщение) также не являются персональными данными»
- *(постановление Тамбовского областного суда от 04.10.2016 по делу № 4А-288/2016)».*

Оформление политики обработки персональных данных

В документе, определяющем политику оператора в отношении обработки персональных данных, рекомендуется отражать следующее:

- ❑ Информация об операторе (наименование или Ф.И.О., ИНН), **контактная информация**;
- ❑ **Цели обработки** персональных данных, **категории и перечень** обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, **способы, сроки их обработки и хранения, порядок уничтожения** персональных данных при достижении целей их обработки или при наступлении иных законных оснований;
- ❑ **Правовые основания** обработки персональных данных;
- ❑ Перечень **мер, принимаемых оператором** и направленных на обеспечение выполнения оператором обязанностей, предусмотренных Законом о персональных данных;
- ❑ Информация **о передаче оператором персональных данных третьим лицам** с указанием правового основания, цели, состава передаваемых персональных данных (при осуществлении);
- ❑ Сведения об осуществлении **трансграничной передачи** персональных данных с указанием стран, на территорию которых передаются персональные данные (при осуществлении);
- ❑ **Способы связи с оператором** для реализации прав субъектов персональных данных (адрес электронной почты, почтовый адрес и т.д.).

Рекомендации РКН по составлению политики (вебинар от 27.07.2023)

► Содержание

Содержание документа, определяющего политику оператора в отношении обработки персональных данных



п.2 ч.1 ст.18.1
№152-ФЗ

«... Для **каждой цели** обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований... Не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности.»

- ✗ ОТСУТСТВИЕ ДАННОЙ ИНФОРМАЦИИ ЛИБО ЕЁ НЕСООТВЕТСТВИЕ ФАКТИЧЕСКОЙ ОСУЩЕСТВЛЯЕМОЙ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРА ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА САЙТЕ
- ✗ ПОЛНОЕ ДУБЛИРОВАНИЕ В ПОЛИТИКЕ КОНФИДЕНЦИАЛЬНОСТИ ПОЛОЖЕНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА №152-ФЗ

Рекомендации РКН по составлению политики (вебинар от 27.07.2023)

► Образец оформления

1. ЦЕЛЬ: оформление онлайн-заказа на сайте

1. 1. категории и перечень
обрабатываемых
персональных данных

- Имя, фамилия
- Номер телефона
- Адрес электронной почты
- Адрес доставки

1. 2. категории субъектов,
персональные данные
которых обрабатываются

- Посетители сайта
- Клиенты

1. 3. сроки их обработки и
хранения

- В течение 3 [трех] лет с момента оформления онлайн-заказа либо до истечения указанного срока в случае отзыва субъектом персональных данных согласия на обработку его персональных данных.

1. 4. способы обработки и
хранения

- Автоматизированная

1. 5. порядок уничтожения
персональных данных при
достижении целей их
обработки или при
наступлении иных законных
оснований

Уничтожение персональных данных субъекта осуществляется комиссией, созданной на основании приказа ООО «Оператор». Документальной фиксацией уничтожения персональных данных субъекта является оформление соответствующего акта о прекращении обработки персональных данных. После утверждения акта персональные данные подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.

2. ЦЕЛЬ: рассылка рекламных сообщений и предложений

1. 1. категории и перечень
обрабатываемых
персональных данных

- Имя
- Дата рождения
- Адрес электронной почты

Рекомендации РКН по составлению политики (вебинар от 27.07.2023)

▶ Рекомендации оформления политики конфиденциальности

Рекомендации по содержанию документа, определяющего политику оператора в отношении обработки персональных данных



- ✓ ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ (НАИМЕНОВАНИЕ ИЛИ ФИО, ИНН), ЕГО КОНТАКТНАЯ ИНФОРМАЦИЯ
- ✓ ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ И ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ, СПОСОБЫ, СРОКИ ИХ ОБРАБОТКИ И ХРАНЕНИЯ, ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ИХ ОБРАБОТКИ ИЛИ ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ
- ✓ ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
- ✓ ПЕРЕЧЕНЬ МЕР, ПРИНИМАЕМЫХ ОПЕРАТОРОМ И НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОПЕРАТОРОМ ОБЯЗАННОСТЕЙ, ПРЕДУСМОТРЕННЫХ ФЕДЕРАЛЬНЫМ ЗАКОНОМ №152-ФЗ
- ✓ ИНФОРМАЦИЯ О ПЕРЕДАЧЕ ОПЕРАТОРОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ С УКАЗАНИЕМ ПРАВОВОГО ОСНОВАНИЯ, ЦЕЛИ, СОСТАВА ПЕРЕДАВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ (ПРИ ОСУЩЕСТВЛЕНИИ)
- ✓ СВЕДЕНИЯ ОБ ОСУЩЕСТВЛЕНИИ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ С УКАЗАНИЕМ СТРАН, НА ТЕРРИТОРИЮ КОТОРЫХ ПЕРЕДАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПРИ ОСУЩЕСТВЛЕНИИ)
- ✓ СПОСОБЫ СВЯЗИ С ОПЕРАТОРОМ ДЛЯ РЕАЛИЗАЦИИ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ (АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ, ПОЧТОВЫЙ АДРЕС И Т.Д.)

Спасибо за внимание!

+79265900373
<https://lukash.info>