БелИнфоНалог

Памятка для специалистов, которые отвечают за работу с персональными данными

## Это база.

# Как выполнить требования Федерального закона N 152-ФЗ «О персональных данных»

Для ИП и юрлиц

БелИнфоНалог

# Введение

Компании и ИП, у которых есть сотрудники и клиенты обязаны соблюдать требования Федерального закона N 152-ФЗ "О персональных данных". С момента поиска кандидата на должность и его оформления в штат, а также в момент оформления договора с клиентом - наступает требования закона. Не у всех организаций есть специалист по информационной безопасности, который будет ответственным за обработку персональных данных. Многие компании наделяют этими функциями работников, которые не подозревают об ответственности. Предлагаем разобраться вместе.

**Роман Беседин**

*ведущий специалист по информационной безопасности компании «БелИнфоНалог»*

***С 30 мая 2025 года** многократно вырастают штрафы за ненадлежащее исполнение и за нарушение требований Федерального закона N 152-ФЗ "О персональных данных", в том числе за неуведомление Роскомнадзора о том, что организация является оператором персональных данных.*

БелИнфоНалог

# Немного вводных данных

Предлагаем разобраться в теории и обратиться к закону. Разберемся в основных терминах, о которых пойдет речь в этой памятке.

**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.

**Согласие на обработку персональных данных** - письменное разрешение субъекта персональных данных, дающее право заинтересованной организации получать, собирать, обрабатывать, использовать и хранить законным способом личные сведения о себе. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

БелИнфоНалог

# Что именно относится к персональным данным?

**ФИО + любые прочие сведения, например:**

Дата и место рождения, адрес, контактные данные, телефон, паспортные данные, СНИЛС, ИНН и любая прочая информация, которая относится к физическому лицу.

**Фото, видео, сканы документов**

– это персональные данные.
Любую информацию, относящуюся к человеку могут признать персональными данными.

**Данные из соцсетей и других сервисов**

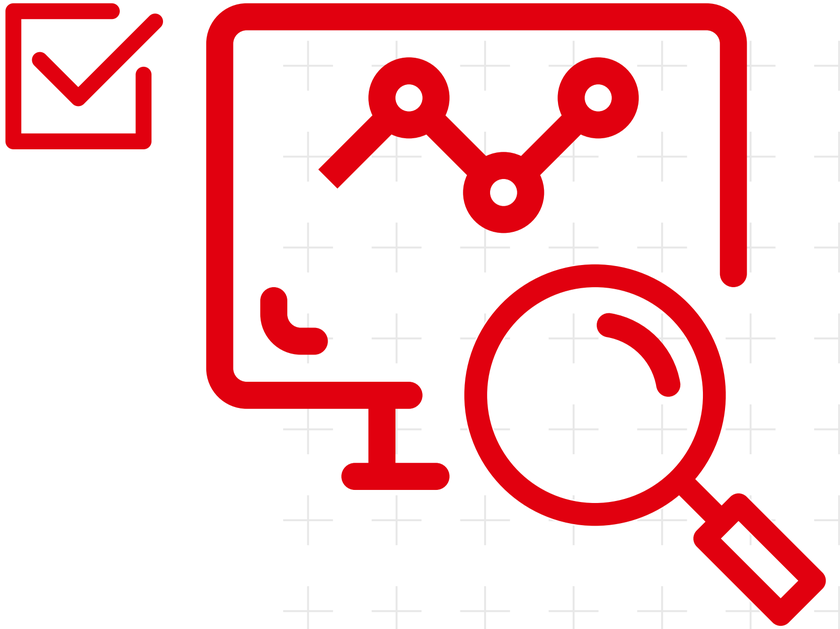
Например, если у человека на странице в соцсети будет указан номер телефона для связи, то нельзя его добавить в базу потенциальных клиентов и отправлять ему смс-уведомления о проводимых акциях.

**Электронная почта**

По мнению Роскомнадзора, электронная почта даже без дополнительной информации может считаться персональными данными.

БелИнфоНалог

# Как собираете персональные данные, как обрабатываете и храните?



У каждой организации свои бизнес-процессы, но мы постараемся выделить самые частые случаи, когда данные сотрудников или клиентов хранятся в электронном виде.

| Где? | + | - |
|---|---|---|
| **Локально на компьютере, например в текстовых документах или таблицах** | Очень распространено у ИП и малого бизнеса, потому что доступно, бесплатно и не требуется дополнительных навыков и обучения (как в работе с CRM-системами) | Риск копирования и утечки данных из файла. Кто угодно может использовать этот файл в своих целях.<br>Риск потери базы данных клиентов и сотрудников (удалили файл, стерли информацию и пр.) |
| **Облачные сервисы для работы онлайн-документами, например Яндекс или Google (опасно!)** | Аналогично локальным документам, к которым прибавляется доступ к файлу с любого устройства, которое подключено к интернет | Запрещено собрать и хранить персональные данные на серверах, которые находятся за пределами РФ (относится к Google и другим иностранным сервисам) |
| **CRM-системы** | Многие популярные CRM-системы обновляют свой функционал и интерфейс под требования законодательства, например, можно подгрузить файл согласия на обработку персональных данных в систему и хранить скан документа. | Если вы пользуетесь облачной CRM-системой, то нужно убедиться, что серверы находятся на территории РФ и система отвечает всем требованиям законодательства. |

БелИнфоНалог

# Какие нарушения бывают и какая за них ответственность

Для начала нужно понять, какие конкретно данные поступают к вам в работу, для чего они используются и как обрабатываются. Мы рекомендуем отнестись к этому серьезно, т.к. с каждым годом всё больше внимания уделяется защите информации для предотвращения инцидентов.

«Законотворцы» стремятся сделать «токсичными» любые персональные данные, обработка которых не требуется по закону (например, для оформления трудовых отношений), стремятся к тому, чтобы как можно меньше персональных данных обрабатывалось организациями

**Инцидент –** это утечка данных (целенаправленный слив или случайность). Можно выделить три вида инцидентов.

*Согласно 152-ФЗ если произошел инцидент с персональными данными, то оператор (организация) обязан сообщить об этом в Роскомнадзор в течение 24 часов. За сокрытие предусмотрен штраф – 1-3 млн. руб для ИП и юрлиц.*

| Взлом и кража данных | Случайный человеческий фактор | Технический сбой |
|---|---|---|
| Злоумышленники получили несанкционированный доступ к персональным данным через фишинг, DDOS-атаку и пр. | Ошибочная отправка персональных данных, утрата документов или порча оборудования, где хранится база данных | Сбой в работе технических систем, использование уязвимых, неактуальных версий ПО, отсутствие средств защиты |

БелИнфоНалог

# Ответственность и штрафы

**С 30 мая 2025 года значительно увеличатся штрафы за утечку персональных данных и другие нарушения при работе с ними**

**Обработка персональных данных, которая не предусмотрена законом**

| ИП, физлица | Должностные лица | Юрлица |
|---|---|---|
| 10-15 тыс. руб. за первичное | 50-100 тыс. руб. за первичное | 150-300 тыс. руб. за первичное |
| 15-30 тыс. руб. за повторное | 100-200 тыс. руб. за повторное | 300-500 тыс. руб. за повторное |

**Несвоевременное сообщение или несообщение в Роскомнадзор о работе с персональными данными.**

- Неуведомление о работе с персональными данными. Штраф вырастит для должностных лиц до 30-50 тыс. руб, для ИП и компаний – до 100-300 тыс. руб. Проверьте, зарегистрированы ли вы в реестре операторов персональных данных. Если не знаете, как проверить или отправить данные в Роскомнадзор, то свяжитесь с нашими специалистами;
- Несвоевременное уведомление или неуведомление Роскомнадзора об утечке персональных данных. Штраф для должностных лиц составит 400-800 тыс. руб, а для ИП и компаний – 1-3 млн. руб.

**Утечка или незаконная передача персональных данных**

**1 000-10 000 чел.**

| ИП, физлица | Должностные лица | Юрлица |
|---|---|---|
| 400-600 тыс. руб. за первичное нарушение | 800 тыс. – 1,2 млн руб. за первичное нарушение | 3-5 млн руб. |
| 100-200 тыс. руб. за повторное | 200-400 тыс. руб. за повторное | |

**Утечка специальных категорий персональных данных**

| ИП, физлица | Должностные лица | Юрлица |
|---|---|---|
| 500-800 тыс. руб. за первичное нарушение | 1-2 млн руб. за первичное нарушение | 10-15 млн руб. |
| 300-400 тыс. руб. за повторное | 400-600 тыс. руб. за повторное | |

**10000-100000 чел.**

| ИП, физлица | Должностные лица | Юрлица |
|---|---|---|
| 400-600 тыс. руб. за первичное нарушение | 1-2 млн руб. за первичное нарушение | 10-15 млн руб. за первичное нарушение |
| 300-400 тыс. руб. за повторное | 400-600 тыс. руб. за повторное | |

**Утечка биометрических персональных данных**

| ИП, физлица | Должностные лица | Юрлица |
|---|---|---|
| 500-800 тыс. руб. за первичное нарушение | 1-2 млн руб. за первичное нарушение | 15-20 млн руб. за первичное нарушение |
| 400-500 тыс. руб. за повторное | 1,3-1,5 млн руб. за повторное | |

**Уголовная ответственность за утечку данных**

Незаконный сбор, передача и хранение персональных данных предусматривает наказание вплоть до уголовной ответственности ( № 421-ФЗ и статья 272.1 УК РФ): штраф до 300 000 руб., принудительные работы до 4 лет, лишение свободы до 4 лет.

Если персональные данные касаются несовершеннолетних или биометрии, то наказание ужесточается: штраф до 700 000 руб., лишение свободы на срок до 5 лет.

В случае если персональные данные переданы в другие страны, то штраф может составить 2 млн руб. и лишение свободы до 8 лет (например, за занесение персональных данных в Google-таблицу).

БелИнфоНалог

# Что необходимо сделать компаниям, чтобы избежать штрафов за нарушения обработки персональных данных?

*БелИнфоНалог является интегратором в части обеспечения информационной безопасности. Наши специалисты успешно реализовывают проекты по всей России по обеспечению кибербезопасности для бизнеса и госорганизаций.*

1. Проверить, уведомлен ли Роскомнадзор, что **ваша организация (или ИП) является оператором персональных данных.** Сделать это можно на сайте Роскомнадзора https://pd.rkn.gov.ru/ Проверьте свою компанию по ИНН и если данных в реестре нет, то рекомендуем как можно быстрее оформить уведомление. Обратитесь в БелИнфоНалог, чтобы правильно подготовить документы и оперативно отправить их в Роскомнадзор.

2. Проверить, актуализировать, либо разработать **формы согласий на обработку персональных данных** и использовать их в своей работе.
Этот этап очень важен, т.к. согласие на обработку персональных данных в подавляющем большинстве (99%) является единственным законным основанием для обработки.

3. Разработать **организационно-распорядительную документацию**, в т.ч. разработать инструкции, назначить ответственных, составить планы работ, провести контрольные мероприятия.

4. Обеспечить **техническую защиту персональных данных согласно требованиям:**
Федерального закона "О персональных данных" от 27.07.2006 N 152-ФЗ,
Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
Приказа ФСТЭК России от 18 февраля 2013 г. N 21
«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

5. Провести оценку эффективности принимаемых мер по обеспечению безопасности персональных данных.

6. Регулярно проводить **мероприятия по обеспечению безопасности обработки персональных данных** и выполнять требования по информационной безопасности.

БелИнфоНалог

# БелИнфоНалог специализируется на информационной безопасности

Наши специалисты успешно реализовали проекты по всей России по обеспечению кибербезопасности для бизнеса и госорганизаций.


8 800 511-82-81

@belinfonalog

belinfonalog.ru
belinfonalog.market