

СЛОЖНОСТИ И СПОРНЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

Романов Илья | CISA, CISM

Заместитель руководителя Отдела консалтинга

АО «ДиалогНаука»

ДиалОГНаука

- ❖ Создана в 1992 году СП «Диалог» и Вычислительным центром РАН.
- ❖ Первые продукты – ревизор ADinf, антивирусы Aidstest и Dr. WEB.
- ❖ В настоящее время – системный интегратор в области информационной безопасности.

Направления деятельности

В соответствии с требованиями нормативных документов и стандартов:

- ❖ 152-ФЗ,
- ❖ СТО БР ИББС,
- ❖ PCI DSS,
- ❖ 382-П,
- ❖ ISO 27001,
- ❖ АСУ ТП,
- ❖ Коммерческая тайна,
- ❖ Сведения ДСП,
- ❖ Защита ГИС.



О компании «ДиалогНаука»: ключевые клиенты



Транснефть
ГИПРОТРУБОПРОВОД
АКЦИОНЕРНОЕ ОБЩЕСТВО
-ИНСТИТУТ ПО ПРОЕКТИРОВАНИЮ
МАГИСТРАЛЬНЫХ ТРУБОПРОВОДОВ-



СКЦ РОСАТОМА



ГАЗПРОМБАНК

Кредит ЕвропаБанк



БАШНЕФТЬ
АКЦИОНЕРНАЯ НЕФТЯНАЯ КОМПАНИЯ

ГНИВЦ
ФНС РОССИИ



НАЦИОНАЛЬНЫЙ
РАСЧЕТНЫЙ
ДЕПОЗИТАРИЙ
ГРУППА МОСКОВСКАЯ БИРЖА



Ростелеком



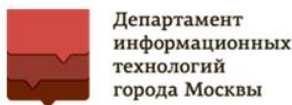
Правительство Санкт-Петербурга
Комитет по градостроительству и архитектуре



ПЕНСИОННЫЙ ФОНД
РОССИЙСКОЙ ФЕДЕРАЦИИ



ТПК
Топливная
Процессинговая
Компания



Тинькофф Банк



НПФ СБЕРБАНК
Негосударственный пенсионный фонд



НАСЛЕДИЕ
негосударственный пенсионный фонд



СТРАХОВАНИЕ
ЦЕНТРАЛЬНЫЙ ТЕЛЕГРАФ
ОСНОВАН В 1852 ГОДУ



Космическая связь



ТРАСТ

РОСБАНК
SOCIETE GENERALE GROUP



СБЕРБАНК ЛИЗИНГ

НОРНИКЕЛЬ

СОГЛАСИЕ
страхование



Запсибкомбанк

Альфа-Банк

ЦБДДМО

Nordea

Транснефть
АО «Транснефть – Прикамье»

МТС Ты знаешь, что можешь!

ГАЗПРОМ
НЕФТЬ
ООО «Газпромнефть-Центр»

МОЭСК

НАЦИОНАЛЬНАЯ
СЛУЖБА
ВЗЫСКАНИЯ

РусГидро

МОСКОВСКИЙ ГОРОДСКОЙ ФОНД
ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО
СТРАХОВАНИЯ
ОБЪЕДИНЕННАЯ ЭНЕРГЕТИЧЕСКАЯ КОМПАНИЯ

- Особенности получения письменных согласий на обработку ПДн
- Сбор ПДн с использованием интернет-сайтов
- Актуальность уведомления об обработке ПДн
- Проверки Роскомнадзора, ФСБ и ЦБ РФ
- Европейский регламент по защите ПДн (GDPR)

Проверки Роскомнадзора

- Вышли из под действия 294-ФЗ (о защите прав при проверках):
 - продление сроков проверки, задержка с выдачей акта;
 - нет возможности оспорить результат (только через суд).
- Большие запросы (требуют свыше 50 справок и официальных ответов).
- Детально смотрят и «бумажные» документы и информационные системы, особое внимание – сайтам.
- Неохотно идут на обсуждение спорных вопросов.



Типичные нарушения

- Нарушения, связанные с сайтами:
 - нет Политики,
 - обработка данных посетителей без согласия,
 - некорректные типовые формы (см. ПП-687).
- Незаконная обработка ПДн:
 - обработка без согласия,
 - согласие не соответствует требованиям,
 - обработка (хранение) по достижению целей.
- Нарушение конфиденциальности:
 - передача третьим лицам.
- Неактуальное уведомление об обработке ПДн.



Письменные согласия на обработку ПДн

- 152-ФЗ:
 - Согласие на обработку ПДн может быть дано в любой позволяющей подтвердить факт его получения форме.
 - В отдельных случаях – только письменное согласие, содержащее **ЦЕЛЬ** обработки персональных данных.
- ТК РФ
 - Не сообщать ПДн работника третьей стороне без **письменного** согласия работника.

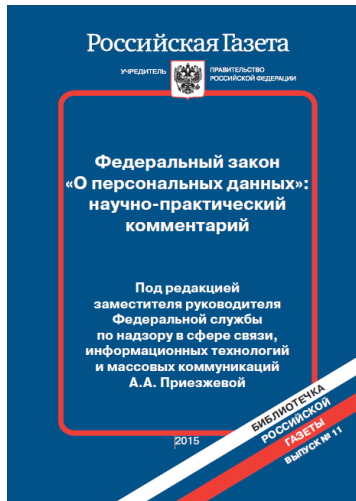


Цель может быть только одна

- 152-ФЗ:
 - Согласие на обработку ПДн может быть дано в любой позволяющей подтвердить факт его получения форме.
 - В отдельных случаях – только письменное согласие, содержащее **ЦЕЛЬ** обработки персональных данных.
- ТК РФ
 - Не сообщать ПДн работника третьей стороне без **письменного** согласия работника.
- Вывод
 - В случае передачи ПДн работников (за рамками ТК) нужны **отдельные** письменные согласия под каждую цель (зарплатный проект, турагентства, ДМС и т.д.).
 - Аналогично и для других субъектов ПДн.



Суды придерживаются такой позиции Роскомнадзора.



...отсутствует однозначное понимание того, в каких случаях собираемые и обрабатываемые данные будут относиться к персональным, а в каких — нет.

...если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать ПДн, даже если они не включают в себя данные документов, удостоверяющих личность.

- Обработка ПДн с использованием счетчиков посещаемости сайтов:
 - IP-адрес компьютера, страна, дата и время посещения, тип браузера, тип операционной системы, модель мобильного устройства, тип мобильного устройства.
- Требуется согласие:
 - в отдельных случаях достаточно «галочки»,
 - в других – обязательна публичная оферта на сайте.

Типовые формы (электронных) анкет на сайте должны соответствовать ПП-687:

- Обработка ПДн **не может быть** признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн либо были извлечены из нее.
- **Формы на сайте** должны содержать цель, сроки обработки, перечень действий, отметку о согласии и т.д.



Отсутствие в Реестре Операторов

Операторов вправе без уведомления осуществлять обработку ПДн в соответствии с трудовым законодательством.

При этом как только работодатель выходит за рамки ТК, он обязан подавать уведомление. Примерами могут служить:

- 1) оформление полисов ДМС
- 2) передача ПДн сторонним организациям для осуществления пропускного режима

Позиция РКН:

В подавляющем большинстве случаев у Операторов нет оснований не подавать уведомление в реестр Операторов ПДн.

Актуальность записи в Реестре Операторов

- Не учтены отдельные категории субъектов ПДн:
 - родственники работников (карточка Т-2);
 - посетители сайтов.
- Не учтены отдельные категории ПДн, например, сведения, содержащиеся в свидетельстве о браке, в удостоверении офицера и паспорте моряка.
- Неполные сведения о правовых основаниях обработки ПДн.

Позиция РКН:

Для граждан наличие Компании в Реестре свидетельствует о легитимности обработки ПДн.

Последствия проверок РКН



- Блокировка интернет-сайтов
- Предписания (срок исполнения – 3 месяца)
- Штрафы

**В подавляющем большинстве случаев
Операторам не удастся оспорить результаты
проверок в суде.**

- Как называется: Обследование помещений, зданий, сооружений, участков местности и транспортных средств.
- Основания:
 - ФЗ «Об оперативно-розыскной деятельности» (144-ФЗ),
 - внутренний план?
- Порядок проведения:
 - приходят без предупреждения,
 - смотрят документы,
 - смотрят оборудование и информационные системы.



Что проверяет ФСБ:

- назначение ответственных лиц (допуск к ПДн, защита ПДн),
- учет машинных носителей ПДн,
- наличие сертифицированных СЗИ и СКЗИ,
- модель угроз и совокупность предположений о нарушителе,
- определение уровня защищенности и требуемого класса СКЗИ.



Результаты:

- штрафы (ч. 6, ст. 13.12 КоАП РФ) – от 10 000 рублей
- представления об устранении причин и условий (срок – 1 месяц в соответствии со ст. 29.13 КоАП РФ)

На основании ст. 22.2, ч.1 ст. 29.9 и в соответствии со ст.29.10 КоАП РФ об административных правонарушениях,

ПОСТАНОВИЛ:

Признать юридическое лицо _____ в лице его законного представителя – директора _____ виновным в совершении административного правонарушения, выразившегося в нарушении законодательства о защите персональных данных, ответственность за которое предусмотрена ч. 6 ст. 13.12 КоАП РФ в виде административного штрафа от десяти тысяч до пятнадцати тысяч рублей.

ФЕДЕРАЛЬНАЯ
СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)

Директору _____

УПРАВЛЕНИЕ

ПРЕДСТАВЛЕНИЕ

об устранении причин и условий, способствовавших совершению административного правонарушения

Руководствуясь статьёй 29.13 Кодекса об административных правонарушениях Российской Федерации, _____ ФСБ России по

Центральный Банк является регулятором в отношении

- Кредитных организаций – банков и НКО.
- Некредитных финансовых организаций – страховых, НПФ, МФО, БКИ, участников рынка ценных бумаг, ломбардов и др.



Запрашивается в рамках проверки процессов обработки и защиты ПДн:

- Аттестат и (или) иной документ, подтверждающий соответствие требованиям по безопасности.
- Приказы о назначении ответственных лиц и утверждении документов.
- Модель угроз, техническое задание и технический проект на создание ИСПДн, сведения о средствах защиты информации
- Сведения об обеспечении защиты информации при ее обработке, хранении и передаче сертифицированными средствами защиты.
- Сведения, документы и справки о выполнении требований по защите (ПП-1119, ФСТЭК-21)



Запрашивается в рамках проверки процессов обработки и защиты ПДн:

- Аттестат и (или) иной документ, подтверждающий соответствие требованиям по безопасности.
- Приказы о назначении ответственных лиц и утверждении документов.
- Модель угроз, техническое задание и технический проект на создание ИСПДн, сведения о средствах защиты информации
- Сведения об обеспечении защиты информации при ее обработке, хранении и передаче сертифицированными средствами защиты.
- Сведения, документы и справки о выполнении требований по защите (ПП-1119, ФСТЭК-21)



Штрафы и санкции в области ПДн

- 13.11 КоАП РФ. Нарушение законодательства в области ПДн (7 составов правонарушения)
- 19.7 КоАП РФ. Непредставление сведений (например, уведомление в реестр операторов)
- 13.12 КоАП РФ. Нарушение правил защиты информации (пример с ФСБ)
- Блокировка Интернет-сайта
- Предписания



General Data Protection Regulation (GDPR)



- General Data Protection Regulation (GDPR) – европейский регламент по защите ПДн.
- Вступает в действие 25 мая 2018.

Действие регламента распространяется на

- Компании, учрежденные в ЕС (например, дочерние структуры).
- Компании, учрежденные в иных государствах, которые:
 - а) предлагают товары или услуги субъектам в ЕС (например, онлайн-сервисы, банки, телеком-операторы);
 - б) осуществляют мониторинг действий, поведения субъектов, находящихся в ЕС (например, любой интернет-сайт).



- Вместо Операторов ПДн – контролеры и обработчики
- Простое и понятное согласие
- Отозвать согласие должно быть также просто, как и получить
- Право субъекта на перенос данных
- Обязанность уведомления регулятора и субъектов ПДн об инцидентах
- Назначение представителя в ЕС
- Обязанность проведения оценки нарушения конфиденциальности (DPIA)

Штрафы и санкции за невыполнение GDPR

- Штрафы до 20 млн евро или 4% годовой выручки компании
- Требование оповещения субъектов об инцидентах, требования ограничения обработки ПДн, или уничтожения ПДн
- Нарушение доступности веб-сайта для субъектов ПДн в ЕС, задействованного в сборе ПДн
- Репутационные риски

Приведение в соответствие GDPR и 152-ФЗ

1. **Проведение обследования, выявление несоответствий**
2. **Актуализация процессов обработки ПДн, проектирование системы защиты**
3. **Внедрение процессов обработки ПДн и средств защиты информации**
4. **Мониторинг и контроль, сопровождение при проверке регуляторов**

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

<http://www.DialogNauka.ru>

e-mail: info@DialogNauka.ru

