OVODOV
CyberSecurity

Персональные данные 2023

Александр Оводов

О КОМПАНИИ

OVODOV CyberSecurity

- Компания «Ovodov CyberSecurity» - ведущий системный интегратор решений в области обеспечения информационной безопасности, работающий на рынке информационных технологий с 2001 года.

- В октябре 2021г. компания выступила организатором крупнейшего в регионе форума по информационной безопасности **CyberSecurity SABANTUY.**

Защищаем персональные данные ваших работников и клиентов от утечек и несанкционированного доступа

Защищаем коммерческую тайну, техническую и производственную информацию, управленческий учет от конкурентов

Внедряем информационные системы контроля сотрудников, помогаем повысить производительность труда, выявить лентяев, инсайдеров и саботажников

Подготавливаем к прохождению проверок РОСКОМНАДЗОРа, ФСТЭК и ФСБ

РЕЗУЛЬТАТЫ НАШЕЙ РАБОТЫ

- Выполненные проекты - 5 173 шт.
- Точек на обслуживании - 3 461 шт.
- Аттестованных рабочих мест - 4 195 шт.
- Пройденных проверок Роскомнадзора - 152 шт.
- Пройденных проверок ФСБ, ФСТЭК- 41 шт.
- Внедрённые средства от несанкционированного доступа - 5 574 лицензий
- Внедрённые межсетевые экраны - 9095 лицензий
- Внедрённые антивирусы - 12 347 лицензий
- Внедрённые средства криптографической защиты - 9 189 лицензий

О спикере

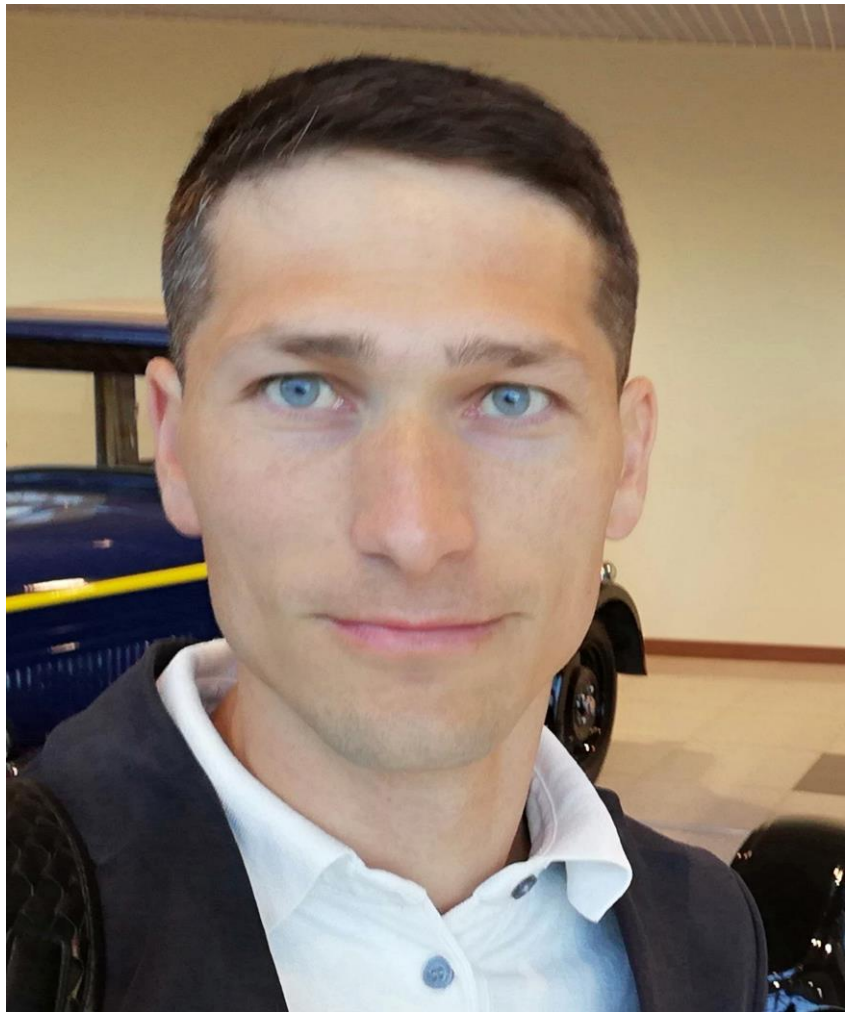
В области защиты персональных данных с 2010 года

Судебная практика

- Приостановление деятельности через отсутствие лицензии на ТЗКИ у коммерческой организации – выиграно;
- 6 протоколов об административном правонарушении с одного акта проверки – сведено к предупреждению;

Подготовка клиентов к проверкам и участие в них

- Роскомнадзор – более 40 проверок. Все без штрафов, 2 с предписаниями исполненным в течение 5-ти дней после окончания проверки.
- ФСБ – 12 проверок пройдено. Две без нарушений. Одна с минимальными нарушениями



OVODOV
CyberSecurity

Сделать ведение бизнеса в цифровой среде безопасным!

В конечном итоге мы хотим чтобы все с кем взаимодействуем оставались успешными!

Ключевые изменения

- Теперь требования 152-ФЗ распространяются и на иностранные юридические и физические лица, обрабатывающие ПДн на основании договора или согласия

- НПА ОГВ и ОМСУ, локальные и правовые акты не могут содержать ограничения для операторов и подлежат обязательному согласования с РОСКОМНАДЗОР если касаются обработки ПДН специальных категорий персональных данных, биометрических персональных данных, персональных данных несовершеннолетних, предоставлением, распространением персональных данных, полученных в результате обезличивания.

Ключевые изменения

OVODOV CyberSecurity

- Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных

Проверить условия договора с субъектами персональных данных

Ключевые изменения

OVODOV CyberSecurity

В поручении оператора должны быть определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные к защите ПДн, обязанность по запросу оператора ПДн в течение срока действия поручения оператора, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 настоящего Федерального закона, в том числе требование об уведомлении оператора о инцидентах.

Внести изменения в поручение обработки персональных данных. Определить формат и порядок работы с документами подтверждающими принятие мер защиты персональных данных

Ключевые изменения

OVODOV CyberSecurity

- В случае, если оператор поручает обработку персональных данных иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом персональных данных за действия указанных лиц несет оператор и лицо, осуществляющее обработку персональных данных по поручению оператора.

- Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.

Проверить согласия на обработку персональных данных и уточнить

Ключевые изменения

OVODOV CyberSecurity

- Требования по обработке персональных данных, разрешенных субъектом персональных данных для распространения больше не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.

Ключевые изменения

OVODOV CyberSecurity

- Предоставление биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных частью 2 статьи 11 152-ФЗ. Оператор не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным.

В случае использования биометрических персональных данных в СКУД необходимо иметь возможность пропустить в обход системы, если субъект не подпишет согласие (если у вас СКУД не предусмотрен законодательно)

Ключевые изменения

- Изменение порядка трансграничной передачи
- Сокращение сроков рассмотрения запросов субъектов ПДн до 10 рабочих дней. Сведения в ответе должны быть представлены тем же способом что использовать субъект при обращении. Состав предоставляемых данных по запросу расширен на:

9.1) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 настоящего Федерального закона

Подготовка и подача отдельных уведомлений о трансграничной передаче

Пересмотр правил ответов на запросы субъектов ПДн в части сроков и состава

Ключевые изменения

- Если в соответствии с федеральным законом предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку
- При получении ПДн не от субъекта ПДн Оператор обязан до начала обработки предоставить субъекту следующую информации:

Дополнено - 2.1) перечень персональных данных

Изменить форму разъяснения юридических последствий отказа предоставить ПДн

Изменить форму уведомления субъекта о составе полученных ПДн от третьих лиц

Ключевые изменения

- Политика и локальные акты должны содержать для каждой цели категории и перечень обрабатываемых ПДн, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.
- Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов ПДн, а также возлагающие на операторов не предусмотренные законодательством РФ полномочия и обязанности

Внести изменения в Политику обработки персональных данных, в Положение об обработке персональных данных или Правила обработки персональных данных

Ключевые изменения

- Необходимо проводить оценку вреда
- Оператор, осуществляющий сбор ПДн 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 ПДн, документ, определяющий его политику в отношении обработки ПДн, и сведения о реализуемых требованиях к защите ПДн, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

Оформить комиссии акт оценки вреда

На каждой странице сайта вставить гиперссылку на Политику обработки ПДн

Ключевые изменения

- Взаимодействие с ГОССОПКА по компьютерным инцидентам, повлекшим неправомерную передачу (предоставление, распространение, доступ) ПДн.
- Обмен данные о компьютерных инцидентах между РОСКОМНАДЗОРом и ФСБ
- Информирование о инцидентах РОСКОМНАДЗОР в течение 24 часов с момента обнаружения и в течение 72 часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии)
- Создание реестра инцидентов РОСКОМНАДЗОРом

Внедрить процессы управления компьютерными инцидентами и инструменты выявления компьютерных инцидентов

Назначить ответственных лиц за реагирование на компьютерные инциденты

Ключевые изменения

- Подтверждение уничтожения персональных данных в случаях, предусмотренных настоящей статьей, осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных.
- Сократилось число случае когда можно не подавать уведомление об обработке персональных данных
- Изменилась форма уведомления об обработке персональных данных
- Направление информационного письма об изменения уведомления надо делать в срок до 15 числа следующего за изменениями месяца

Внести изменения в порядок уничтожения ПДн и утвердить новую форму акта

Ключевые изменения

- РОСКОМНАДЗОР теперь орган осуществляющий самостоятельно функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных

266-ФЗ. НПА принятые во исполнение

✅Постановление Правительства Российской Федерации от 29.12.2022 № 2526 «Об утверждении перечня случаев, при которых к операторам, осуществляющим трансграничную передачу персональных данных в целях выполнения возложенных международным договором Российской Федерации, законодательством Российской Федерации на государственные органы, муниципальные органы функций, полномочий и обязанностей, не применяются требования частей 3 — 6, 8 — 11 статьи 12 Федерального закона „О персональных данных“».

✅Постановление Правительства Российской Федерации от 10.01.2023 № 6 «Об утверждении Правил принятия решения о запрещении или об ограничении трансграничной передачи персональных данных уполномоченным органом по защите прав субъектов персональных данных и информирования операторов о принятом решении».

✅Постановление Правительства Российской Федерации от 16.01.2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан».

266-ФЗ. НПА принятые во исполнение

✓Приказ Роскомнадзора от 05.08.2022 № 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных».

✓Приказ Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона „О персональных данных“».

✓Приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

✓ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 180 "Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных"

✓Приказ Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

266-ФЗ. НПА принятые во исполнение

✓Приказ ФСБ России от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».

Приказ РКН 178 от 27.10.22

OVODOV CyberSecurity

- ✓ Утверждает требования к оценке вреда, который может быть причинен субъектам персональных данных
- ✓ Срок действия Приказа - с 01.03.2023 по 01.03.2029 г.
- ✓ Оценку вреда проводит - ответственный за организацию обработки ПДн или комиссия
- ✓ Определяют степень вреда, который может быть причинен субъекту ПДн, в случае нарушения Закона о персональных данных.
- ✓ 3 степени вреда - высокая, средняя, низкая

Приказ РКН 178 от 27.10.22

OVODOV CyberSecurity

Высокая степень вреда

- Биометрия, за исключением случаев установленными ФЗ;
- Специальные категории, за исключением случаев установленными ФЗ;
- Обработка ПДн несовершеннолетних по договору;
- Обезличивание ПДн в целях скорринга, прогнозирования спроса и иных исследований, не предусмотренных разрешенными способами обработки ПДн в статистических и исследовательских целях;
- Поручение обработки ПДн граждан России иностранном лицу;
- Сбор ПДн с использованием баз расположенных за границей РФ.

Приказ РКН 178 от 27.10.22

OVODOV CyberSecurity

Средняя степень вреда

- Распространение ПДн на сайте оператора и предоставление ПДн третьим лицам;
- Обработка ПДн в дополнительных целях, отличных от первоначальной цели сбора;
- Продвижение товаров, работ, услуг компании в Интернете;
- Получение согласия на сайте без дальнейшей идентификации и аутентификации субъекта;
- Получение согласие об осуществлении обработки ПДн с поручением обработки определенному или неопределенному кругу лиц в целях несовместимых между собой;

Приказ РКН 178 от 27.10.22

Низкая степень вреда

- Ведение общедоступных источников ПДн, сформированных согласно статьи 8 152-ФЗ;
- Назначение ответственным за организацию обработки ПДн не сотрудника организации.

Приказ РКН 178 от 27.10.22

OVODOV CyberSecurity

Акт оценки вреда

1. Наименование /ФИО и адрес оператора;
2. Дата издания акта;
3. Дата проведения оценки вреда;
4. ФИО, должность и подпись лиц проводивших оценку
5. Степень вреда которая была определена

Степень вреда указывается максимальная из возможных.

Приказ РКН 179 от 28.10.22

OVODOV CyberSecurity

- ✓ Утверждает требования к подтверждению уничтожения ПДн
- ✓ Срок действия Приказа - с 01.03.2023 по 01.03.2029 г.
- ✓ Оформляется акт уничтожения
- ✓ Акт об уничтожении ПДн и выгрузка из журнала должны хранится 3 года.

Приказ РКН 179 от 28.10.22

OVODOV CyberSecurity

Акт об уничтожению должен содержать:

1. Наименование и адрес оператора;
2. Наименования и адреса лиц, осуществляющих обработку ПДн по поручению Оператора;
3. ФИО или иную информацию, относящуюся к определенным физ лицам, чьи ПДн были уничтожены;
4. ФИО, должность, подпись лиц уничтоживших ПДн;
5. Перечень категорий уничтоженных ПДн;
6. Наименование уничтоженных материальных носителей, содержащих ПДн, с указанием количества листов;
7. Наименование ИСПДн;
8. Способ уничтожения ПДн;
9. Причина унитожения ПДн;
10. Дата уничтожения ПДн

Приказ РКН 179 от 28.10.22

Не автоматизированная обработка ПДн - бумажный акт

Обработка ПДн в ИСПДн - акт об уничтожении и выгрузка из журнала регистрации событий ИСПДн.

Акт может быть подписан ЭП, лиц ответственных за уничтожение и указанных в акте.

Приказ РКН 179 от 28.10.22

OVODOV CyberSecurity

Выгрузка из журнала должна содержать:

1. ФИО или иную информацию, относящуюся к субъектам ПДн;
2. Перечень категорий уничтоженных ПДн;
3. Наименование ИСПДн;
4. Причину уничтожения ПДн;
5. Дата уничтожения ПДн.

Если в выгрузку невозможно внести какие-то из указанных данных - они вносятся в акт об уничтожении.

Приказ РКН от 14.11.2022 № 187

OVODOV CyberSecurity

«Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»

- Если РКН выявляет факт неправомерного распространения скомпроментированной БД, указывающей на принадлежность конкретному оператору, то направляет ему представление. У Оператора есть 24 часа на подачу уведомления об инциденте или ответ с актом о расследование подтверждающем отсутствие утечки или уведомление с данными ранее поданного уведомления

Приказ РКН от 14.11.2022 № 187

Приказ Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»

- Определяет состав уведомления об инциденте и результатах расследования инцидента.
- Форма подачи уведомления - бумажно, в электронном виде через портал с ЭП.
- В случае неполных сведений будет дозапрос сведений, в случае их не предоставления в течение 3х рабочих дней направляется требование.
- Ответ на требование - 1 рабочий день

Постановление Правительства РФ от 29.12.2022 № 2526

«Об утверждении перечня случаев, при которых к операторам, осуществляющим трансграничную передачу ПДн в целях выполнения возложенных международным договором РФ, законодательством РФ на государственные органы, муниципальные органы функций, полномочий и обязанностей, не применяются требования частей 3 - 6, 8 - 11 статьи 12 Федерального закона "О персональных данных»

Не надо подавать уведомление:

Безопасность, перевозки, дипломатические и консульские сношения, сотрудничества в ЕЭС, уголовные дела, международные суды, оказание госуслуг, почта Почтой РФ, обмен фин информацией с компетентными органами

Постановление Правительства РФ от 29.12.2022 № 2526

OVODOV CyberSecurity

«Об утверждении перечня случаев, при которых к операторам, осуществляющим трансграничную передачу ПДн в целях выполнения возложенных международным договором РФ, законодательством РФ на государственные органы, муниципальные органы функций, полномочий и обязанностей, не применяются требования частей 3 - 6, 8 - 11 статьи 12 Федерального закона "О персональных данных»

Надо подавать уведомление, но вправе до решения РОСКОМНАДЗОРА осуществлять передачу в страны не обеспечивающие адекватную защиту:

физкультура, спорт, культура, наука, образование, обеспечение платежей с использованием платежных систем и платежной инфраструктуры

Вступает в силу - 01.03.2023

Приказ ФСБ от 13.02.2023 № 77

Приказ ФСБ от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн»

Вступает в силу – 01.03.2023г.

Приказ ФСБ от 13.02.2023 № 77

OVODOV CyberSecurity

Взаимодействие ГОССОПКА осуществляется через НКЦКИ
Срок на подачу – 24 часа в момента инцидента, срок на предоставление результатов расследования инцидента – 72 часа.

- Субъекты КИИ, иные субъекты ГОССОПКА у которых организовано взаимодействие с НКЦКИ - подают уведомление в соответствие с форматами определенными НКЦКИ с использованием каналов информационного взаимодействия.

За помощью могут обратить соответственно через канал взаимодействия.

- Остальные Операторы ПДн подают только уведомление через портал РОСКОМНАДЗОРа и через него же получают идентификатор инцидента.

Присвоение индикатора инцидента есть подтверждение принятия уведомления об инциденте. Индикатор направляется в течение 24 часов с момента получения НКЦКИ.
За помощь могут обратится через сайт - https://cert.gov.ru/index.html
НКЦКИ может запрашивать уточнения. Срок ответа – 24 часа.

ПДн И ЕБС

ФЗ от 29.12.2022 N 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации"

Часть вступает в силу сразу.

Часть с 1.06.23

Часть с 01.01.24

Часть с 01.01.27

ФЗ от 29.12.2022 № 584-ФЗ

ФЗ от 29.12.2022 № 584-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"

Запрет на использование ИС и ПО, использующегося для обмена электронными сообщениями между пользователями, содержащими ПДн

- при предоставлении гос услуг;
- выполнения гос или мун задания;
- при реализации организациями с гос или мун участием, ПАО, кредитными и некредитными финансовыми организациями (согласно 86-ФЗ), субъектами национальной платежной системы товаров, работ, услуг, имущественных прав

ФЗ от 29.12.2022 № 584-ФЗ

Запрет при реализации кредитными и некредитными финансовыми организациями, субъектами НПС

товаров, работ, услуг, имущественных прав

с использованием принадлежащим иностранным компаниям и гражданам ИС и ПО, используемым для обмена электронными сообщениями между пользователями ИС и ПО, для передачи платежных документов и(или) предоставления информации, содержащей ПДн (без размещения общедоступной информации в сети ИНтернет), данных о переводах денежных средств необходимых для осуществления платежей и(или) сведений о счетах (вкладах) граждан РФ в банках.

ФЗ от 29.12.2022 № 584-ФЗ

Запрещается подключать к ИС и ПО, указанных выше иных ИС, обеспечивающих возможность перевода денежных средств граждан РФ в рамках применяемых форм безналичных расчетов.

РОСКОМНАДЗОР размещает на своем сайт перечень запрещенных ИС и ПО.

Действует с 1 марта 2023г.

ПДн И ЕБС

ФЗ от 29.12.2022 N 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации"

Часть вступает в силу сразу.

Часть с 1.06.23

Часть с 01.01.24

Часть с 01.01.27

ГОСТы по инцидентам

OVODOV CyberSecurity

- ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения»
- ГОСТ Р 59710-2022 Защита информации. Управление компьютерными инцидентами. Общие положения
- ГОСТ Р 59711-2022 Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами
- ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения

Как мы можем помочь вам

OVODOV CyberSecurity

1. Привести обработку персональных данных в соответствие с требованиями законодательства как организационно так и технически
2. Обучить ответственных за организацию обработки и обеспечение безопасности персональных данных
3. Взять ваши процессы организации обработки и обеспечения безопасности персональных данных на аутсорсинг
4. Выявлять и реагировать на компьютерные атаки
5. Расследовать компьютерные инциденты

Финансово гарантируем успешное прохождение проверок

ГАРАНТИИ

OVODOV CyberSecurity

1. Опыт успешного прохождения проверок РОСКОМНАДЗОРа, ФСБ, ФСТЭК, Прокуратуры и других регуляторов в сфере персональных данных
2. Финансовые гарантии компенсации штрафов и устранения предписаний за наш счет
3. Мы будет с вами рядом в момент проверки или инцидента и будем максимально решать все вопросы за вас

OVODOV
CyberSecurity

СПАСИБО
ЗА ВНИМАНИЕ!

АЛЕКСАНДР ОВОДОВ

Основатель компании Ovodov CyberSecurity

ТЕЛЕФОН: 8–800–301–67–43

EMAIL: INFO@OVODOV.SU

INSTAGRAM: https://www.instagram.com/ovodov_cs/

Чат в Telegram: https://t.me/+nHXASZh9PbY0MmE6

Чат в Telegram

Наш канал на YouTube

Наш Телеграм