



Обработка персональных данных

Комплексное правовое регулирование обработки персональных данных в цифровой среде, устанавливающее принципы, основания и гарантии защиты прав субъектов данных.

Сфера применения

Правовое регулирование обработки персональных данных

Применение Кодекса

Настоящий Кодекс применяется к любым отношениям по обработке персональных данных, в том числе в составе цифровых записей и цифровых ресурсов. Предусматривает особенности обработки информации персонального характера, не являющейся цифровыми персональными данными.

Исключения

Кодекс не применяется к отношениям по обработке персональных данных физическим лицом исключительно в связи с его личными или семейными делами.

Приоритет норм

Нормативные правовые акты, регулирующие обработку персональных данных, противоречащие настоящему Кодексу или не опубликованные в установленном порядке, не подлежат применению.

Семь принципов обработки персональных данных

Законность и прозрачность

Обработка на законных основаниях, справедливым и открытым образом в отношении субъекта персональных данных.

Ограничение цели

Обработка ограничивается достижением конкретных, заранее определенных и законных целей. Изменение цели без согласия субъекта не допускается.

Минимизация данных

Содержание и объем обрабатываемых данных должны соответствовать заявленным целям и не быть избыточными.

Точность

Обеспечение точности, достаточности и актуальности персональных данных. Владелец обязан удалять или уточнять неполные или неточные данные.



Ограничение хранения

Хранение в форме, позволяющей определить субъекта, не дольше, чем требуют цели обработки. Данные подлежат уничтожению или обезличиванию по достижении целей.

Целостность и конфиденциальность

Обработка способом, обеспечивающим безопасность данных с обязательным принятием организационных и технических мер защиты.

Подотчетность

Владелец записей несет ответственность за соблюдение всех принципов и должен быть способен подтвердить их соблюдение.

Основания обработки персональных данных

Обработка персональных данных допускается при наличии хотя бы одного из следующих оснований:

01

Договорные отношения

Обработка необходима для заключения или исполнения договора, в котором субъект является стороной, представителем или выгодоприобретателем.

02

Законные обязанности

Обработка необходима для выполнения владельцем записей обязанностей, установленных законом или нормативными правовыми актами.

03

Жизненно важные интересы

Обработка необходима для защиты жизненно важных интересов субъекта персональных данных либо иного физического лица.

04

Публичные задачи

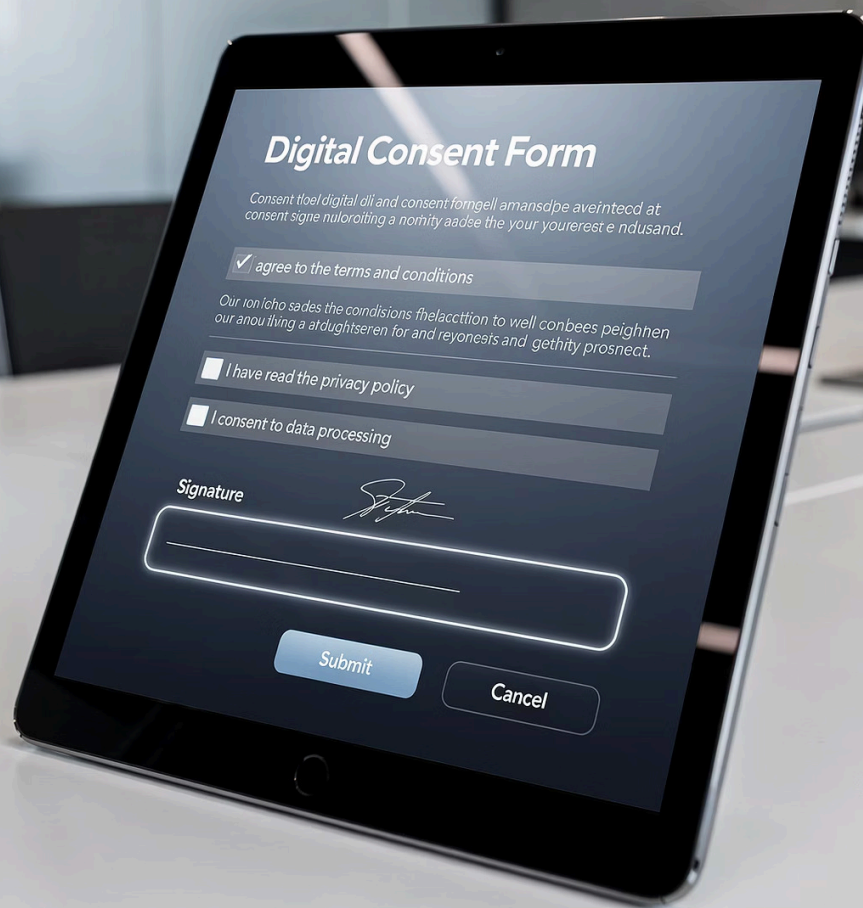
Обработка необходима для реализации владельцем записей публичных или иных общественно полезных задач.

05

Законные интересы

Обработка необходима для реализации законных интересов владельца записей или третьего лица при условии, что не нарушаются права субъекта данных.

Согласие на обработку персональных данных



Требования к согласию

Согласие должно быть:

- Добровольным
- Конкретным
- Информированным
- Сознательным

Может быть дано в любой форме, позволяющей подтвердить факт его получения.

Ничтожность согласия

Согласие ничтожно, если запрос:

1. Не выделен из других запросов к субъекту
2. Не понятен и не доступен субъекту, изложен сложным языком
3. Направлен при наличии других оснований обработки

 **Важно:** Согласие может быть отозвано субъектом персональных данных. Процедура отзыва не должна быть более обременительной, чем процедура предоставления согласия.

Обработка специальных категорий персональных данных

Запрещенные категории

- Расовое или этническое происхождение
- Политические взгляды
- Религиозные или философские воззрения
- Членство в профсоюзе
- Генетическая информация
- Биометрические данные для цифровой идентификации
- Данные о здоровье, половой жизни или сексуальной ориентации

Исключения из запрета

Обработка допускается при наличии мер защиты в случаях:

- Договорные отношения
- Прямое указание в законе
- Защита жизненно важных интересов
- Общедоступные данные
- Медицинские цели
- Общественное здравоохранение
- Деятельность общественных объединений
- Осуществление правосудия
- Национальная безопасность
- Научные исследования при обезличивании

Особенности обработки персональных данных детей

Условия обработки

Обработка персональных данных детей допускается только при условии:

- Обработка осуществляется в интересах ребенка
- Применяются установленные гарантии защиты основных прав и свобод детей

Согласие законного представителя

При отсутствии законных оснований обработка допускается только при получении согласия законного представителя ребенка.

Дети с 14 лет вправе самостоятельно давать согласие в рамках своей дееспособности.

Требования к запросу

Запрос согласия и информация об обработке должны быть изложены **ясным и доступным языком**, понятным для ребенка.

- ❏ **Владельцы записей** обязаны принимать меры, необходимые для предотвращения незаконной обработки персональных данных детей.



Оценка воздействия на защиту персональных данных



Обязательная оценка

Владелец записей обязан провести оценку воздействия перед обработкой персональных данных.



Содержание оценки

Описание операций и целей, оценка необходимости и пропорциональности, система управления рисками.



Пересмотр

Обязательный пересмотр при существенном изменении операций или перечней данных.

Оценка воздействия обязательна в следующих случаях:

Автоматическое принятие решений

При систематической и комплексной оценке личных аспектов для автоматического принятия решений, порождающих правовые последствия.

Специальные категории данных

При обработке специальных категорий персональных данных в отношении более чем тысячи субъектов.

Наружный мониторинг

При систематическом автоматическом наружном мониторинге общественных мест техническими средствами.

Права субъектов персональных данных



Удаление персональных записей

Владелец записей обязан немедленно удалить персональные записи, если данные больше не нужны для целей обработки, прекратило действие основание обработки или субъект отозвал согласие.



Возражение против обработки

Субъект вправе направить возражение против обработки определенными способами или в определенных целях. Владелец обязан рассмотреть возражение в течение семи рабочих дней.



Ограничение обработки

Владелец обязан ограничить обработку при получении возражения, требования регулятора или при возникновении оснований для исправления или удаления данных.



Участие обработчика в обработке персональных данных

Основные требования

Обработчик осуществляет обработку персональных записей в соответствии с правовым актом или договором с владельцем на тех же основаниях обработки.

Владелец записей обязан обеспечить соблюдение обработчиком требований Кодекса.

Важно: Обработчик не вправе привлекать другого обработчика без предварительного письменного разрешения владельца записей.

Содержание договора

- Период обработки
- Характер и цель обработки
- Тип персональных данных и категории субъектов
- Обязанность обрабатывать данные только по распоряжениям владельца
- Обязанность обеспечить ограничение доступа
- Процедуры взаимодействия
- Порядок учета операций

❏ Отраслевой регулятор разрабатывает и публикует типовые формы договора обработчика с владельцем записей.

Совместные владельцы записей

Определение

Владельцы, которым совместно принадлежат цифровые права на одни и те же персональные записи и которые совместно определяют цели и средства обработки.

Цифровые экосистемы

Владелец цифровой экосистемы обязан обеспечить соблюдение требований Кодекса и несет ответственность за их несоблюдение.



Порядок взаимодействия

Совместные владельцы должны открытым образом определить и опубликовать порядок совместного осуществления прав и исполнения обязанностей.

Цифровые сообщества

Обработка в цифровых сообществах осуществляется в соответствии с правилами сообщества, определяющими ответственное лицо.

Субъект персональных данных может осуществлять свои права в отношении любого из владельцев записей по своему выбору независимо от договоренностей между совместными владельцами.

Защита персональных данных



Конструктивная защита

Реализация защиты данных при проектировании цифровых технологических систем.



Учет операций

Ведение учета операций с персональными записями в соответствии с рекомендациями регулятора.



Ответственное лицо

Определение лица, ответственного за обработку персональных данных (для организаций с более чем 10 работниками).



Обучение персонала

Организация обучения правилам и рекомендациям в сфере обработки персональных данных.

- ☐ Кабинет Министров устанавливает требования по защите персональных данных при их обработке в цифровых технологических системах в соответствии с установленными уровнями защищенности.



Трансграничная передача персональных данных

1

Перечень государств, обеспечивающих адекватную защиту ПД

Отраслевой регулятор утверждает и публикует перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

2

Передача в адекватные государства

Трансграничная передача на территории государств из перечня осуществляется в соответствии с Кодексом и не может быть запрещена или ограничена.

3

Проверка владельцем записей

Владелец записей обязан до начала трансграничной передачи убедиться, что иностранное государство включено в перечень.

4

Передача в другие государства

Передача в государства, не обеспечивающие адекватной защиты, возможна при наличии согласия субъекта, международных договоров, законодательных оснований или договорных гарантий.

Отраслевой регулятор в сфере персональных данных

Независимость и квалификация

Регулирование и надзор осуществляются уполномоченным государственным органом, который должен быть независим от лиц, в отношении которых он осуществляет свои полномочия.

Руководитель должен обладать квалификацией, опытом и знаниями, в том числе в сфере защиты персональных данных.

Основные функции

- Обеспечение применения и надзор за применением Кодекса
- Повышение осведомленности субъектов и владельцев данных
- Консультирование государственных органов
- Аккредитация лиц на проведение проверок
- Рассмотрение жалоб и проведение проверок
- Применение профилактических и принудительных мер
- Публикация руководств и рекомендаций

Реестр владельцев записей

Инциденты с персональными данными

Регистрация всех инцидентов, связанных с нарушением безопасности персональных данных.

Проверки и решения

Данные о проверках соблюдения владельцами записей и обработчиками положений Кодекса и вынесении обязательных для исполнения решений.

Привлечение к ответственности

Информация о привлечении к ответственности за нарушения в сфере персональных данных.

- ❏ Порядок ведения реестра определяется отраслевым регулятором самостоятельно. Доступ к реестру осуществляется посредством сайта отраслевого регулятора.

Полномочия отраслевого регулятора

Запрос информации

Право запрашивать у физических лиц и организаций информацию, в том числе относящуюся к государственным секретам или иной охраняемой законом тайне, необходимую для реализации своих полномочий.

Мониторинг государственных органов

Право осуществлять мониторинг обработки персональных данных государственными органами и их подведомственными организациями (за исключением разведывательной деятельности).

Доступ к помещениям и документам

Право осуществлять доступ во все помещения, к документам, оборудованию, сотрудникам и контрагентам владельца персональных записей для установления фактов.

Требования к владельцам записей

Право требовать уточнения, блокирования или удаления недостоверных либо полученных незаконным путем персональных данных, а также приостановления обработки при нарушениях.



Судебная защита и взаимодействие

Судебные полномочия

Отраслевой регулятор вправе:

- Обращаться в суд с исковыми заявлениями в защиту нарушенных прав субъектов персональных данных
- Защищать права неопределенного круга лиц
- Представлять интересы субъектов персональных данных в суде
- Направлять материалы о нарушениях в соответствии с подведомственностью

Взаимодействие и развитие

Регулятор обязан:

- Взаимодействовать с другими государственными органами
- Заключать меморандумы о совместных действиях
- Вносить предложения о совершенствовании регулирования
- Сотрудничать с аналогичными органами в иностранных государствах
- Утверждать перечень государств с адекватной защитой

Обязанности отраслевого регулятора

01

Организация соблюдения прав

Организовывать соблюдение прав субъектов персональных данных в соответствии с положениями Кодекса.

02

Проведение проверок

Проверять соблюдение владельцами записей и обработчиками положений Кодекса и выносить обязательные для исполнения решения.

03

Межведомственное взаимодействие

Взаимодействовать с другими государственными органами в целях исключения дублирования контрольно-надзорных мероприятий.

04

Рассмотрение жалоб

Рассматривать жалобы и обращения физических и юридических лиц по вопросам обработки персональных данных.

05

Разъяснения и рекомендации

Давать разъяснения по вопросам применения законодательства и разрабатывать рекомендации с публикацией на своем сайте.

❏ Отраслевой регулятор публикует годовой отчет о деятельности и результаты своих расследований на своем сайте.

Особенности обработки информации персонального характера на бумажных носителях



Применение принципов

Информация персонального характера, не являющаяся цифровыми данными и обрабатываемая без использования цифровых устройств, должна обрабатываться с соблюдением принципов обработки, установленных Кодексом, и только при наличии предусмотренных оснований обработки.

Изготовление копий

Если для реализации требований субъекта персональных данных требуется изготовление копий информации на бумажном носителе, субъект обязан оплатить стоимость изготовления таких копий.

Обязанности собственника носителей

Собственник материальных носителей, содержащих информацию персонального характера, не обязан соблюдать требования Кодекса по защите персональных данных, однако обязан ограничить доступ к таким носителям и вести учет носителей и лиц, имеющих доступ к ним.