ПОЛНЫЙ КУРС И СБОРНИК БЛАНКОВ ПО ЗАЩИТЕ ДАННЫХ

Полный перевод материалов вебинара AMAC (Все слайды 1–32) и полный комплект сопутствующих практических бланков (EX-01 – EX-09).
На основе лучших практик в сфере водоснабжения и водоотведения.

ЧАСТЬ 1: МАТЕРИАЛЫ ПРЕЗЕНТАЦИИ (СЛАЙДЫ 1–32)

СЛАЙД 1 · ТИТУЛЬНЫЙ

ВЕБИНАР AMAC · ОКТЯБРЬ 2026 г.

Защита данных в деятельности оператора водоснабжения

Рабочие ситуации. Простые вопросы. Более безопасные решения.

> **Важное примечание:** Примеры компании APAVITAL служат исключительно учебным и методическим материалом. Каждый конкретный оператор самостоятельно проверяет собственные процедуры, регламенты и требования местного законодательства.

СЛАЙД 2 · НАЧИНАЕМ С ПОВСЕДНЕВНОЙ ДЕЯТЕЛЬНОСТИ

Главная цель курса — научиться своевременно распознавать ситуации, связанные с обработкой персональных данных, и четко знать, какие параметры необходимо проверить.

Ключевой аналитический вопрос:

В каком документе или программном приложении вы чаще всего сталкиваетесь с конфиденциальными данными клиентов или ваших коллег по работе?

Итоги вебинара — к концу обучения участники должны уметь:

- Самостоятельно и безошибочно распознавать персональные данные в обычных повседневных рабочих примерах.
- Четко верифицировать и проверять легитимную цель обработки, уровень доступа сотрудников и конечного получателя информации.
- Оперативно и в установленные сроки докладывать руководству о любой допущенной ошибке или утечке (инциденте) данных.

Рассматриваемые в материале направления:

- Пользователи (потребители услуг) и штатные сотрудники компании.
- Используемые рабочие приложения и документы.
- Выполнение задач непосредственно в офисе (на месте) и при выезде на объекты (в полевых условиях).

СЛАЙД 3 · ВВОДНЫЙ ОПРОС · ГДЕ ВЫ ВИДИТЕ НАИБОЛЬШИЙ РИСК?

Голосование участников с возможностью выбора только одного варианта ответа. Время на заполнение — 1 минута. Результаты агрегируются и выводятся полностью анонимно (без идентификации участников вебинара).

Варианты для голосования персонала:

- **A** · Случайная (ошибочная) отправка документов или сообщений не тем адресатам / внешним получателям.
- **B** · Получение доступа к базам данных со стороны посторонних (неавторизованных) лиц.
- **C** · Ввод конфиденциальных персональных данных во внешние публичные приложения или системы искусственного интеллекта (ИИ).
- **D** · Физическая утеря бумажных документов, служебных накопителей или мобильных рабочих устройств.
- **E** · Незнание действующих внутренних процедур организации или их неправильное применение на практике.

> **Пояснение спикера:** В данном интерактивном опросе не существует единственного правильного ответа. Основная цель — определить, какие именно зоны и риски вызывают наибольшее беспокойство у сотрудников в данный момент.

СЛАЙД 4 · КОГДА ИНФОРМАЦИЯ ЯВЛЯЕТСЯ ПЕРСОНАЛЬНЫМИ ДАННЫМИ?

Любая информация считается персональными данными (ПД), если она позволяет идентифицировать конкретное физическое лицо напрямую или опосредованно (путем сопоставления и связывания с другими сопутствующими сведениями).

МОЖЕТ ЯВЛЯТЬСЯ ПЕРСОНАЛЬНЫМИ ДАННЫМИ	НЕ ИДЕНТИФИЦИРУЕТ ЧЕЛОВЕКА САМО ПО СЕБЕ
• ФИО, номер телефона и адрес электронной почты (email) пользователя. • Уникальный номер (код) клиента, если его можно сопоставить с конкретным лицом. • Баланс счета, история начислений, объемы потребления или полная история договора. • Записи телефонных разговоров и любые изображения, по которым можно узнать человека.	• Официальные регистрационные данные компании (юридического лица). • Технические параметры сети (например, диаметр водопроводной трубы). • Обезличенная общая сумма счетов по району/городу без возможности идентификации абонентов.

Главный практический вопрос для самопроверки: *Есть ли у нас техническая или логическая возможность узнать, о каком конкретно человеке идет речь на основе имеющихся сведений?*

СЛАЙД 5 · ПУТЬ ДАННЫХ ВНУТРИ ОРГАНИЗАЦИИ

Персональные данные сопровождают всю основную деятельность предприятия и постоянно встречаются в бумажных бланках, цифровых приложениях, письмах, личных делах сотрудников и архивах.

Основные этапы жизненного цикла (маршрута) данных:

1. **ПОСТУПЛЕНИЕ (ВХОД):** Заявления от граждан · Заключение договоров · Телефонные звонки в колл-центр · Запросы через личный кабинет на веб-портале.
2. **ИСПОЛЬЗОВАНИЕ (ОБРАБОТКА):** Текущее обслуживание · Выставление квитанций и счетов · Выезд бригад на аварии и технические интервенции · Расчет заработной платы.
3. **ПЕРЕДАЧА (КОММУНИКАЦИЯ):** Взаимодействие с банками · Ответы на запросы государственных органов · Обмен данными с подрядчиками · Курьерская доставка.
4. **ОБНОВЛЕНИЕ (АКТУАЛИЗАЦИЯ):** Изменение контактных телефонов/адресов · Официальное исправление допущенных технических ошибок и опечаток.
5. **ХРАНЕНИЕ И УНИЧТОЖЕНИЕ:** Нахождение в рабочих ИТ-системах · Передача в архив · Полное удаление или уничтожение документов по истечении установленных сроков.

> **Обязанность сотрудника:** Проверять легитимную цель и уровень доступа к информации; своевременно выявлять и исправлять любые неточные или устаревшие данные на всем протяжении их маршрута.

СЛАЙД 6 · В ОТНОШЕНИЯХ С ПОЛЬЗОВАТЕЛЕМ ОТТАЛКИВАЕМСЯ ОТ ЦЕЛИ

Базовый практический пример: Управление договором водоснабжения и непосредственное предоставление услуг потребителям.

- **1. Собираем строго необходимые данные:** Фамилию, имя, точный адрес объекта и контактные сведения, требуемые для легитимного оказания услуг.
- **2. Используем по прямому назначению:** Для администрирования договора, начисления платы, выставления счетов и выполнения аварийно-восстановительных работ.
- **3. Опираемся на законные основания:** Непосредственное исполнение условий договора, выполнение возложенных на оператора юридических обязательств или реализация задач в общественных интересах, прямо предусмотренных законодательством.
- **4. Храним строго в рамках правил:** Данные находятся в активной системе в течение срока, обоснованного правилами, после чего подлежат архивированию или окончательному удалению.

> **Важное правило юридического основания:** Для обработки персональных данных, которые необходимы для прямого оказания коммунальных услуг, запрашивать отдельное «согласие» лица, как правило, не требуется. Законным основанием здесь выступает сам договор или норма закона.

СЛАЙД 7 · ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ОБ УСЛУГЕ ИЛИ МАРКЕТИНГ?

Перед тем как использовать имеющуюся базу контактов (списки телефонов или email) для массовой рассылки, необходимо четко определить юридическую категорию и характер отправляемого сообщения.

- **ИНФОРМИРОВАНИЕ ОБ УСЛУГЕ (Операционные сообщения):** Выставление текущего счета · Экстренное отключение водоснабжения · Запрос показаний водомера или плановые технические работы.
- **КОММЕРЧЕСКОЕ СООБЩЕНИЕ (Маркетинг):** Рекламные кампании · Продвижение платных дополнительных услуг · Специальные коммерческие предложения, акции или приглашения на мероприятия.

> **Запомните:** Для отправки сообщений маркетингового характера требуется предварительно полученный, четко выраженный и задокументированный выбор (согласие) пользователя. Обычное отсутствие возражений или молчание со стороны клиента ни в коем случае не означают его согласие. Перед отправкой любых SMS или email-писем всегда проверяйте актуальность списков получателей.

СЛАЙД 8 · УСЛУГА ИЛИ МАРКЕТИНГ? СРАВНИМ ДВА СООБЩЕНИЯ

Конкретный пример для понимания разницы на практике:

- **Категория «Информирование об услуге» (Разрешено в рамках договора):** *«Завтра, в период с 09:00 до 13:00, подача питьевой воды по Вашему адресу будет временно приостановлена в связи с проведением планового ремонта».*
- **Категория «Коммерческая коммуникация» (Требуется отдельное согласие):** *«Откройте для себя наше новое уникальное предложение по установке и сервисному обслуживанию современных систем фильтрации воды».*

> **Вывод:** Один и тот же технический канал связи (например, SMS-шлюз или email-рассылка) может использоваться организацией для совершенно разных целей, к которым применяются принципиально разные юридические условия.

СЛАЙД 9 · ПЕРЕД ОТПРАВКОЙ: ПРОВЕРКА ПОЛУЧАТЕЛЕЙ

Каждый сотрудник перед запуском информационной рассылки обязан последовательно ответить на три вопроса:

1. **ЦЕЛЬ:** Это обязательное информирование об услуге в рамках договора или коммерческое сообщение?
2. **ПОЛУЧАТЕЛИ:** Соответствует ли сформированный список адресатов и выбранный населенный пункт содержанию сообщения?
3. **КОНТАКТНЫЕ ДАННЫЕ:** Правильно ли указаны номера телефонов, адреса и выбранный технический канал коммуникации?

> **Анализ инцидента:** Если SMS об аварии по технической ошибке было отправлено жителям другого города, это является операционным сбоем в коммуникации, но не классифицируется автоматически как критическая утечка (брешь) персональных данных.

СЛАЙД 10 · УПРАЖНЕНИЕ: РОДСТВЕННИК ЗАПРАШИВАЕТ БАЛАНС СЧЕТА КЛИЕНТА

> *«Здравствуйте, я дочь владельца счета. Подскажите, пожалуйста, какая у него точная сумма к оплате за этот месяц?»*

Вопросы для предварительного анализа ситуации (Время на обсуждение — 2 минуты):

- **A** · Какую именно категорию информации запрашивает обратившееся лицо?
- **B** · Кем является заявитель по отношению к абоненту и системе?
- **C** · Является ли данное лицо официально уполномоченным представителем?

Проанализируйте параметры перед тем, как озвучить ответ. Рекомендуемый алгоритм действий приведен на следующем слайде.

СЛАЙД 11 · РЕКОМЕНДУЕМОЕ РЕШЕНИЕ · РОДСТВЕННИК ЗАПРАШИВАЕТ БАЛАНС

ПРАВИЛЬНЫЙ АЛГОРИТМ ДЕЙСТВИЙ СОТРЕДНИКА:

- **Что мы обязаны сделать:**
  - Надежно идентифицировать личность человека, запрашивающего сведения.
  - Проверить наличие официального статуса по договору или законного права на представительство (например, доверенности).
  - Если право доступа не подтверждено документально, вежливо объяснить пошаговый порядок прохождения авторизации, **не разглашая при этом сумму задолженности и баланс счета**.
- **Чего необходимо избегать:**
  - Категорически запрещено сообщать баланс счета только на том основании, что звонящий знает ФИО владельца, адрес проживания или утверждает, что является близким родственником.

> **ЗАПОМНИТЕ:** Факт близкого или дальнего родства сам по себе не предоставляет человеку автоматического юридического права на доступ к чужим персональным и финансовым данным.

СЛАЙД 12 · ДАННЫЕ СОТРУДНИКОВ СОПРОВОЖДАЮТ ВЕСЬ ПЕРИОД ТРУДОВЫХ ОТНОШЕНИЙ

Персональные данные персонала обрабатываются на протяжении всех этапов работы в компании. При этом действует строгий принцип разграничения прав доступа: каждая должность видит исключительно ту информацию, которая необходима для выполнения обязанностей.

Этапы обработки данных в трудовых отношениях:

1. **Кандидатура (Найм):** Резюме (CV), дипломы, результаты собеседований и первичные контактные данные.
2. **Прием на работу:** Формирование личного дела, подписание трудового договора, сбор документов.
3. **Текущая деятельность:** Начисление заработной платы, учет рабочего времени (табель), премии и KPI.
4. **Здоровье и охрана труда (СМ):** Результаты обязательных медицинских осмотров, листки нетрудоспособности.
5. **Актуализация:** Своевременное изменение адреса проживания, номера телефона или банковского счета для выплат.
6. **Увольнение:** Расторжение договора, окончательный расчет, отзыв всех прав доступа к корпоративным системам.

> **Пример разграничения прав:** Непосредственному руководителю или менеджеру проекта для работы должно быть достаточно официального медицинского заключения «годен к выполнению обязанностей». Доступ к полному тексту медицинской карты, диагнозам и истории болезней сотрудника ему категорически запрещен.

СЛАЙД 13 · МОНИТОРИНГ НА РАБОЧЕМ МЕСТЕ ДОЛЖЕН БЫТЬ РАЗЪЯСНЕННЫМ И СОРАЗМЕРНЫМ

Использование таких инструментов, как корпоративная электронная почта, навигация GPS на автомобилях, камеры видеонаблюдения и электронные системы контроля доступа (СКУД), неизбежно генерирует персональные данные сотрудников.

Четыре обязательных критерия легитимного мониторинга:

1. **Что именно мы отслеживаем?** Четкий перечень: геолокация автомобиля, логи систем, видеопоток.
2. **Зачем? (Обоснование):** Наличие четко сформулированной законной цели, реальная производственная необходимость и соразмерность мер (нельзя собирать больше, чем нужно).
3. **Кто имеет доступ и сколько хранятся данные?** Доступ открыт только уполномоченным лицам (например, службе безопасности), а сроки хранения строго ограничены (например, 30 дней для видео).
4. **Было ли проведено предварительное информирование?** Сотрудники должны быть под подпись ознакомлены с целями, границами и правилами ведения мониторинга.

> **Пример с GPS:** Перед активацией трекеров на машинах мы обязаны официально уведомить команду, четко определить цели (оптимизация маршрутов выезда бригад) и ограничить круг лиц, видящих перемещения в реальном времени.

СЛАЙД 14 · ПЕРЕРЫВ

ПАУЗА · 10 МИНУТ

Тема следующей части вебинара: Как правильно и безопасно действовать, если в работе организации что-то пошло не так?

СЛАЙД 15 · МЫ ЗАЩИЩАЕМ ДАННЫЕ ЧЕРЕЗ ПРАВИЛА, КОТОРЫЕ ДОПОЛНЯЮТ ДРУГ ДРУГА

Один лишь сложный пароль или современное антивирусное приложение сами по себе не способны обеспечить полную безопасность. Защита персональных данных — это комплексная система, состоящая из трех взаимодополняющих уровней.

- **ТЕХНИЧЕСКИЙ УРОВЕНЬ (ИТ-меры):** Использование строго индивидуальных учетных записей, разграничение прав доступа на основе служебных ролей, регулярное создание резервных копий (бэкапов).
- **ОРГАНИЗАЦИОННЫЙ УРОВЕНЬ (Процедуры):** Обязательная проверка адресатов перед отправкой, оперативное информирование ИТ-отдела об ошибках, регулярный аудит прав доступа.
- **ФИЗИЧЕСКИЙ УРОВЕНЬ (Среда):** Своевременное извлечение распечатанных документов из лотков принтеров, запирание кабинетов и серверных комнат на ключ, физическая защита техники.

> **Примечание:** Все активные технические меры должны быть официально подтверждены и настроены ИТ-специалистами компании. Приведенные примеры служат для демонстрации комплексного подхода.

СЛАЙД 16 · ТЕХНИЧЕСКИЕ МЕРЫ: КТО ВХОДИТ И ЧТО МОЖЕТ ДЕЛАТЬ?

Базовые стандарты защиты информации в корпоративных ИТ-системах:

- **ИНДИВИДУАЛЬНЫЕ УЧЕТНЫЕ ЗАПИСИ:** Каждому сотруднику создается уникальный именной аккаунт. Использование общих (коллективных) профилей и передача паролей коллегам категорически запрещены.
- **ДОСТУП НА ОСНОВЕ РОЛЕЙ:** Права разграничиваются по должностям. Сотрудники коммерческого отдела и инженеры технической аварийной бригады имеют принципиально разные потребности и разные уровни доступа к базе.
- **РЕЗЕРВНОЕ КОПИРОВАНИЕ (БЭКАП):** Регулярное создание бэкапов имеет практический смысл только в том случае, если процесс восстановления данных из копии был успешно протестирован на практике.

СЛАЙД 17 · ЭФФЕКТИВНАЯ МЕРА ВКЛЮЧАЕТ В СЕБЯ И ЛЮДЕЙ, И ПРАВИЛА

МИКРО-УПРАЖНЕНИЕ ДЛЯ ЗАКРЕПЛЕНИЯ МАТЕРИАЛА:

- **Организационный контроль на практике:** Всегда проверяем адресатов перед отправкой писем; четко знаем внутренние инструкции; немедленно докладываем об инцидентах.
- **Физический контроль на практике:** Сразу забираем документы с принтера; запираем пустые кабинеты; защищаем технику от кражи и повреждений.

АНАЛИТИЧЕСКИЙ ВОПРОС:

Если сотрудник ушел на обед и оставил компьютер в офисе разблокированным — какие уровни защитных мер нарушены и как их дополнить?

> **Правильный ответ:** Надежная защита — всегда многоуровневая. В данном случае техническая мера (автоматическая блокировка экрана через 5 минут) должна быть дополнена организационной (привычка блокировать ПК клавишами `Win+L`) и физической (запирание двери кабинета).

СЛАЙД 18 · ИИ И ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЧТО МЫ ОТПРАВЛЯЕМ ЧАТ-БОТУ?

Разбор практической производственной ситуации:
Сотрудник компании полностью скопировал поступившую от клиента претензию (включая ФИО гражданина, домашний адрес, номер телефона и код абонента) во внешний публичный ИИ-чат-бот, чтобы быстро сгенерировать красивый и вежливый текст ответа.

Можно ли использовать ИИ для подготовки текстов и на каких условиях?

- Используемый инструмент ИИ должен быть официально одобрен ИТ-департаментом организации, а условия обработки данных — проверены юристами на соответствие GDPR.
- Перед отправкой запроса в чат-бот сотрудник обязан полностью удалить из текста все данные, позволяющие прямо или косвенно идентифицировать человека (провести деперсонализацию текста).
- Сгенерированный ИИ ответ подлежит обязательной проверке сотрудником на предмет фактических ошибок перед отправкой клиенту.

СЛАЙД 19 · ЕСЛИ ПОЯВЛЯЕТСЯ ИНЦИДЕНТ — ДОКЛАДЫВАЕМ НЕЗАМЕДЛИТЕЛЬНО

Любая ошибка, о которой сотрудник сообщил оперативно, может быть быстро локализована, что минимизирует возможные негативные последствия для организации.

Пять шагов при обнаружении инцидента:

1. **ОБНАРУЖЕНИЕ (ФИКСАЦИЯ):** Заметили отправку SMS не в тот город, обнаружили утерю папки с договорами или служебного устройства.
2. **ЛОКАЛИЗАЦИЯ:** Немедленно останавливаем дальнейшую отправку писем или оперативно блокируем учетные записи и удаленный доступ к потерянному устройству, если это возможно.
3. **УВЕДОМЛЕНИЕ:** Срочно докладываем о случившемся руководству по внутренней цепочке информирования и направляем данные Сотруднику по защите данных (DPO).
4. **СБОР ДОКАЗАТЕЛЬСТВ:** Надежно сохраняем логи, скриншоты, файлы и любые детали, которые могут помочь в ходе проведения внутреннего расследования.

> **Важная обязанность компании:** Работник обязан лишь оперативно доложить о факте ошибки. Руководство компании и DPO на основе полученных сведений проводят юридический анализ и принимают решение, нужно ли официально уведомлять Государственный надзорный орган и информировать пострадавших граждан.

СЛАЙД 20 · ПЕРВЫЕ МИНУТЫ ПОСЛЕ ОБНАРУЖЕНИЯ ОШИБКИ

Алгоритм немедленных действий для рядового сотрудника:

- **1 · ОГРАНИЧИВАЕМ ЭФФЕКТЫ:** Пытаемся заблокировать распространение информации доступными техническими способами, но строго без уничтожения логов и системных доказательств.
- **2 · ДОКЛАДЫВАЕМ:** Безотлагательно сообщаем о происшествии по внутренней установленной цепочке инстанций.
- **3 · ДОКУМЕНТИРУЕМ:** Фиксируем точное время, хронологию событий, описание того, что произошло, и примерный объем пострадавших персональных данных.

Сотрудник обеспечивает оперативное информирование; организация проводит комплексную оценку рисков и назначает компенсирующие меры.

СЛАЙД 21 · ОПЕРАЦИОННАЯ ОШИБКА ИЛИ УТЕЧКА ДАННЫХ?

Практическое сравнение для понимания разницы:

- **СИТУАЦИЯ 1: Отправка общего информационного SMS-уведомления в другой город.**
  Классифицируется как ошибочное информирование. Ситуация является операционным сбоем в работе, но не влечет за собой автоматического несанкционированного раскрытия персональных данных третьим лицам.
- **СИТУАЦИЯ 2: Отправка SMS-сообщения с указанием ФИО абонента и баланса его счета посторонним людям.**
  Является классическим инцидентом безопасности (несанкционированным разглашением личных данных). Ситуация подлежит обязательной фиксации, оперативному докладу DPO и комплексной оценке рисков.

> **Строгий запрет:** Сотрудникам категорически запрещено самостоятельно присваивать класс инциденту, занижать его критичность или единолично принимать решение о том, нужно ли скрывать факт ошибки от Сотрудника по защите данных (DPO).

СЛАЙД 22 · ПОСТАВЩИКИ И ГОСУДАРСТВЕННЫЕ ОРГАНЫ: ЧТО МЫ ПРОВЕРЯЕМ

Перед тем как предоставить удаленный доступ к базам или направить выгрузку сведений внешнему контрагенту, необходимо провести обязательные проверки.

- **При взаимодействии с внешними Поставщиками (Подрядчиками):**
  - Какую конкретно услугу оказывает контрагент и какие категории данных ему действительно необходимы?
  - Ограничен ли его доступ строго рамками выполнения текущих задач и лимитирован ли по времени?
  - Заключены ли между нами четкие правила, соглашение о безопасности и обязательство полного удаления данных по окончании проекта?
- **При взаимодействии с Государственными органами / Судебными исполнителями:**
  - Кто именно прислал официальный запрос и входит ли это в компетенцию данного органа?
  - Какое конкретное правовое основание, цель и категории данных указаны в тексте запроса?
  - Какие именно документы релевантны и как передать их получателю максимально безопасным способом?

Главное правило: Всегда четко определяйте юридическую роль контрагента, цель передачи, строго минимальный объем сведений и сохраняйте официальное подтверждение факта отправки.

СЛАЙД 23 · ИТ-ПОСТАВЩИК: КАКОВА ЕГО РОЛЬ И КАКОЙ УРОВЕНЬ ДОСТУПА ОН ИМЕЕТ?

Особенности контроля внешних ИТ-партнеров:

- **РЕАЛЬНАЯ ЮРИДИЧЕСКАЯ РОЛЬ:** Контрагент обрабатывает личные данные строго от имени и по поручению нашего предприятия (как обработчик/процессор) или использует их для реализации собственных целей?
- **ДОГОВОР И ГАРАНТИИ БЕЗОПАСНОСТИ:** Помните, что подписание простого соглашения о конфиденциальности (NDA) не способно заменить собой полноценное Соглашение об обработке персональных данных (DPA), обязательное к заключению в соответствии с требованиями GDPR.
- **НЕОБХОДИМЫЙ УРОВЕНЬ ДОСТУПА:** Все учетные записи, объемы видимых данных и длительность сессий должны быть строго лимитированы рамками проведения конкретных технических работ (ремонта).

> **Важный принцип безопасности:** Наличие у внешнего инженера технической возможности зайти в любую папку системы ни в коем случае не означает наличие у него официального юридического права на просмотр этой конфиденциальной информации.

СЛАЙД 24 · КОГДА ГОСУДАРСТВЕННЫЙ ОРГАН ОФИЦИАЛЬНО ЗАПРАШИВАЕТ ДАННЫЕ

При поступлении любого запроса от властей необходимо последовательно выполнить четыре ступени проверки:

1. **ПОДЛИННОСТЬ:** Проверяем, кто именно направил запрос и по какому официальному каналу связи он поступил в организацию.
2. **КОМПЕТЕНЦИЯ И ПРАВОВОЕ ОСНОВАНИЕ:** Верифицируем, наделен ли данный орган законными полномочиями и указал ли он в тексте конкретную норму закона, обязывающую нас выдать сведения.
3. **НЕОБХОДИМОСТЬ:** Проверяем, какие именно документы релевантны и строго необходимы для выполнения этого точечного запроса (избегаем избыточной выгрузки).
4. **БЕЗОПАСНАЯ ПЕРЕДАЧА:** Оцениваем технический канал отправки и проверяем корректность адреса ведомства-получателя.

> **Запомните:** Всегда сохраняйте официальные доказательства и квитанции о передаче сведений. Фактор срочности или давления со стороны проверяющих органов никогда не отменяет необходимость выполнения базовых юридических проверок.

СЛАЙД 25 · СЦЕНАРИЙ 1 · СЧЕТ ПОПАЛ НА ОШИБОЧНЫЙ АДРЕС

Описание рабочей ситуации:
В офис компании поступает звонок от гражданина, который сообщает, что на его домашний адрес или email по ошибке пришел чужой счет за воду, содержащий персональные и финансовые данные другого абонента.

Вопросы для анализа (Время на обсуждение — 2 минуты):

- Какое действие необходимо предпринять в самые первые минуты после звонка?
- Какие именно отправки и процессы обработки нам нужно приостановить?
- Какие контактные данные подлежат немедленной проверке и исправлению в CRM?
- Кого из сотрудников внутри организации мы обязаны уведомить?

Порядок правильного решения кейса приведен на следующем слайде.

СЛАЙД 26 · РЕКОМЕНДУЕМОЕ РЕШЕНИЕ · СЧЕТ ОТПРАВЛЕН НЕВЕРНО

Юридическая квалификация ситуации: Случайное (несанкционированное) разглашение персональных данных третьим лицам вследствие операционной ошибки.

ПРАВИЛЬНЫЙ АЛГОРИТМ ДЕЙСТВИЙ:

- **Что мы обязаны сделать на рабочем месте:**
  - Локализовать последствия инцидента и незамедлительно доложить о случившемся DPO по внутреннему каналу.
  - Зафиксировать и задокументировать, какие конкретно категории данных и по какому числу абонентов ушли на неверный адрес.
  - Провести верификацию базы, связаться с правильным клиентом и внести исправления в CRM-систему только после подтверждения корректных данных.
- **Чего необходимо избегать:**
  - Категорически запрещено скрывать факт допущенной ошибки от руководства. Простая повторная отправка квитанции на правильный адрес без фиксации самого инцидента не решает проблему.

СЛАЙД 27 · СЦЕНАРИЙ 2 · ФОТОГРАФИИ С ОБЪЕКТА НА ЛИЧНОМ СМАРТФОНЕ

Описание рабочей ситуации:
Выездная аварийно-техническая бригада успешно завершила ремонтные работы на объекте и провела обязательную фотофиксацию. Однако снимки остались в памяти личного смартфона одного из сотрудников. При анализе кадров выяснилось, что в объектив, помимо отремонтированной трубы, попали ворота частного дома, четкая табличка с адресом и посторонний человек, находившийся в этот момент во дворе.

Вопросы для анализа (Время на обсуждение — 2 минуты):

- Какие из сделанных кадров действительно необходимы организации для отчетности?
- Через какие официальные каналы и куда их необходимо перенести для хранения?
- Что сотрудник обязан сделать с копиями файлов, оставшимися на его личном телефоне?

Рекомендуемое решение кейса приведено на следующем слайде.

СЛАЙД 28 · РЕКОМЕНДУЕМОЕ РЕШЕНИЕ · ФОТОГРАФИИ В ПОЛЕВЫХ УСЛОВИЯХ

Юридическая квалификация ситуации: Риск неконтролируемого хранения и обработки персональных данных (изображений физических лиц и адресов) на личных устройствах персонала.

ПРАВИЛЬНЫЙ АЛГОРИТМ ДЕЙСТВИЙ:

- **What we must do:**
  - Провести жесткий отбор снимков, оставив только те кадры, которые непосредственно документируют факт выполнения технических работ (без лиц людей).
  - Перенести отобранные файлы через официальные защищенные каналы связи в утвержденные корпоративные базы данных компании.
  - Полностью удалить все оставшиеся файлы и их копии с личного мобильного устройства в соответствии с внутренними процедурами ИБ.
- **Чего необходимо избегать:**
  - Категорически запрещено пересылать рабочие фотографии объектов, содержащие адреса или лица людей, через личные мессенджеры, социальные сети или хранить их в публичных облачных сервисах.

СЛАЙД 29 · СЦЕНАРИЙ 3 · ПОСТАВЩИК ТРЕБУЕТ ПРЕДОСТАВИТЬ ДОСТУП КО ВСЕЙ БАЗЕ КЛИЕНТОВ

Описание рабочей ситуации:
В ИТ-отдел обращаются инженеры внешней компании-подрядчика, выполняющей техническое обслуживание программного обеспечения, со следующим требованием: *«Для оперативного выявления и устранения возникшей системной ошибки нам необходимо создать учетную запись администратора с постоянным полным доступом ко всей базе данных клиентов оператора».*

Вопросы для анализа (Время на обсуждение — 2 минуты):

- Какие параметры и условия контракта необходимо прояснить перед ответом?
- Какой конкретно уровень прав доступа мы имеем право предоставить инженерам партнера?
- Каким образом этот доступ должен быть ограничен и как его правильно закрыть?

СЛАЙД 30 · РЕКОМЕНДУЕМОЕ РЕШЕНИЕ · УРОВЕНЬ ДОСТУПА ДЛЯ ПОДРЯДЧИКА

Юридическая квалификация ситуации: Запрос на предоставление расширенных прав доступа к персональным данным со стороны внешнего обработчика (процессора). Риск избыточной выгрузки информации.

ПРАВИЛЬНЫЙ АЛГОРИТМ ДЕЙСТВИЙ:

- **Что мы обязаны сделать в организации:**
  - Четко прояснить техническую цель вмешательства, текущую роль контрагента и строго минимальный объем данных, без которых ремонт невозможен.
  - Предоставить строго индивидуальный временный аккаунт с минимально достаточными правами доступа, зафиксировав условия в специальном акте.
  - Обеспечить непрерывный мониторинг и логирование действий инженера во время сессии и полностью отозвать (удалить) учетную запись сразу по окончании работ.
- **Чего необходимо избегать:**
  - Категорически запрещено предоставлять полный, неограниченный или постоянный доступ ко всей базе клиентов только на основе устных заверений подрядчика о производственной необходимости.

СЛАЙД 31 · ПЯТЬ ПРАВИЛ, КОТОРЫЕ МЫ ОБЯЗАНЫ ПРИМЕНЯТЬ ЕЖЕДНЕВНО

Практический краткий синтез всех рассмотренных рабочих ситуаций и ключевой итог курса.

ОБЯЗАТЕЛЬНЫЕ ДЕЙСТВИЯ СОТРУДНИКА (ЧЕК-ЛИСТ НА КАЖДЫЙ ДЕНЬ):

- **ПРОВЕРЯЙ** личность заявителя и его официальное право на получение доступа к информации.
- **ОГРАНИЧИВАЙ** объемы обрабатываемых данных только тем минимумом, который строго необходим для работы.
- **ЗАЩИЩАЙ** конфиденциальные сведения, используя только утвержденные ИТ-системы и каналы связи.
- **ДОКЛАДЫВАЙ** незамедлительно о любых обнаруженных ошибках, утерях документов или инцидентах.
- **СПРАШИВАЙ** совета у Сотрудника по защите данных (DPO) при возникновении малейших сомнений.

> **Главный вывод вебинара:** Надежная защита персональных данных всегда начинается до того, как произойдет инцидент безопасности, а не после. Никогда не предполагайте, что фактор спешки, устное распоряжение или удобство в работе могут служить оправданием для нарушения правил.

СЛАЙД 32 · СЕМЬ ВОПРОСОВ, КОТОРЫЕ НУЖНО ПОМНИТЬ И ПРИМЕНЯТЬ НА РАБОЧЕМ МЕСТЕ

Выберите как минимум один пункт проверки, который вы начнете активно применять в своей деятельности прямо с сегодняшнего дня:

1. С какой конкретно законной целью мы используем эти персональные данные?
2. Какие именно категории данных нам действительно необходимы для выполнения этой задачи?
3. Кто именно из сотрудников имеет легитимную производственную потребность в доступе к этой информации?
4. Кому именно за пределами организации мы передаем эти сведения и на каком основании?
5. В течение какого точного срока мы имеем право хранить эти данные у себя?
6. Какими конкретно техническими и организационными мерами мы защищаем эту информацию от утечки?
7. Как именно мы проверяем корректность, точность и актуальность данных перед их непосредственным использованием или отправкой внешним адресатам?

ЧАСТЬ 2: КОМПЛЕКТ ПРАКТИЧЕСКИХ ПРИЛОЖЕНИЙ И БЛАНКОВ (EX-01 – EX-09)

ПРИЛОЖЕНИЕ 1 (КОД: AMAC-GDPR-EX-01) · МАТРИЦА ИНФОРМИРОВАНИЯ КЛИЕНТОВ

Цель бланка: Предоставление субъектам данных (клиентам) исчерпывающих сведений об обработке их ПД в понятной и прозрачной форме.

Категория данных	Цели обработки	Правовое основание	Сроки хранения	Получатели данных
Идентификация и контакты (ФИО, адрес, телефон, email)	Заключение договора, управление отношениями, оперативная связь.	Исполнение договора, выполнение законных обязанностей оператора.	В течение срока действия договора + архивный срок по закону.	Банки, платежные системы, госорганы, подрядчики рассылок.
Договорные параметры (Документы на объект, доверенности)	Подключение к сетям, выдача техусловий, рассмотрение официальных жалоб.	Исполнение контракта, реализация законных интересов предприятия.	Согласно установленным срокам хранения технической документации.	Уполномоченные внутренние службы, проектные институты, госорганы.
Финансовые сведения (Счета, баланс, долги, реквизиты)	Начисление платы, ведение учета, взыскание долгов в судебном порядке.	Законные обязанности в сфере финансово-бухгалтерского учета.	В соответствии с нормами налогового и бухгалтерского законодательства.	Банки, налоговые органы, судебные исполнители, суды.
Медиа-данные (Аудиозаписи звонков, фото с объектов)	Контроль качества обслуживания, фиксация выполнения ремонтов.	Защита прав оператора, соразмерная необходимость.	В течение минимального срока, обоснованного конкретной целью.	Служба внутреннего контроля, органы следствия (при запросе).

ПРИЛОЖЕНИЕ 2 (КОД: AMAC-GDPR-EX-02) · БАЗОВОЕ ЗАЯВЛЕНИЕ О РЕАЛИЗАЦИИ ПРАВ

ЗАЯВЛЕНИЕ СУБЪЕКТА ДАННЫХ НА РЕАЛИЗАЦИЮ ПРАВ (ОСНОВНАЯ ФОРМА)

ФИО заявителя:

_____

Контактные данные (телефон, email, почтовый адрес):

_____

Статус по отношению к организации: [ ] клиент [ ] сотрудник [ ] кандидат [ ] представитель

Выбираемые права (отметьте галочкой):

- [ ] **Право на доступ:** Прошу выдать подтверждение обработки моих данных и предоставить их копию.
- [ ] **Право на исправление:** Прошу изменить следующие неточные или устаревшие сведения: _____
- [ ] **Право на удаление («забвение»):** Требую полностью стереть мои данные из систем при наличии оснований.
- [ ] **Право на ограничение:** Прошу временно приостановить активное использование моих данных в системах.
- [ ] **Право на переносимость:** Прошу выгрузить мои данные в структурированном цифровом формате.
- [ ] **Право на возражение:** Возражаю против обработки моих данных в следующих целях: _____

Желаемый канал получения официального ответа: [ ] email [ ] почта [ ] лично в руки

Дата: _____ Подпись: _____

ПРИЛОЖЕНИЕ 3 (КОД: AMAC-GDPR-EX-03) · РАСШИРЕННАЯ ФОРМА ЗАЯВЛЕНИЯ СУБЪЕКТА

Используется службой DPO для детальной фиксации требований после прохождения этапа верификации личности.

Заявитель (ФИО):

_____

Ссылка на первичное обращение (Дата и входящий номер):

_____

Детализация запрашиваемых изменений:

Тип требования	Конкретное содержание запроса физического лица
[ ] Исправление	Заменить ошибочные данные на новые корректные: _____
[ ] Удаление файлов	Удалить из архивных баз и логов следующие сведения: _____
[ ] Ограничение	Заблокировать использование данных в связи со следующей причиной: _____
[ ] Переносимость	Направить выгрузку моих данных внешнему оператору (Наименование контрагента): _____

Дата: _____ Подпись: _____

ПРИЛОЖЕНИЕ 4 (КОД: АМАС-GDPR-EX-04) · ШАБЛОН АНАЛИЗА ВОЗДЕЙСТВИЯ (DPIA) ДЛЯ МАРКЕТИНГА

Краткий отчет об оценке рисков при запуске рекламных рассылок:

- **Цель:** Отправка информационно-коммерческих SMS/email-сообщений о новых услугах.
- **Правовое основание:** Исключительно предварительное, явное и фиксируемое согласие клиента.

Выявленный риск	Возможные последствия	Уровень риска	Обязательная мера контроля
Отправка рекламы без согласия	Жалобы граждан, крупные штрафы от надзорного органа, потеря репутации.	Высокий	Строгое разделение баз на операционные (аварии) и коммерческие (маркетинг).
Ошибочный ввод галочки оператором	Направление спама лицам, не дававшим согласия.	Средне-высокий	Регулярный выборочный аудит соответствия бумажных анкет записям в CRM.
Игнорирование отзыва согласия	Продолжение отправки рекламы после официального отказа клиента.	Высокий	Внедрение автоматической ссылки «Отписаться» с мгновенным исключением из списков.

ПРИЛОЖЕНИЕ 5 (КОД: AMAC-GDPR-EX-05) · РЕГЛАМЕНТ РАБОТЫ С НЕАКТИВНЫМИ КЛИЕНТАМИ

После официального расторжения договора или смены собственника объекта личные данные не должны оставаться доступными в общих рабочих базах в прежнем виде.

Пошаговый алгоритм изоляции данных бывших абонентов:

1. **Фиксация статуса:** Система автоматически присваивает договору маркер «Неактивен».
2. **Псевдонимизация:** Прямые идентификаторы (ФИО, телефон) в операционной CRM заменяются на обезличенные технические коды.
3. **Архивация и перенос:** Исторические данные о платежах извлекаются из текущей рабочей базы производства и переносятся в изолированное хранилище.
4. **Ограничение прав:** Доступ к архиву закрывается для обычных менеджеров и контролеров; данные могут быть открыты только сотрудникам со спец-правами (например, юристам для судов).

ПРИЛОЖЕНИЕ 6 (КОД: AMAC-GDPR-EX-06) · ИНСТРУКЦИЯ ПО ЗАЩИТЕ КАДРОВЫХ ДАННЫХ

Обязательные требования к обработке данных сотрудников и кандидатов:

- **Сбор анкет:** Категорически запрещено собирать у кандидатов избыточные документы (копии свидетельств, паспортов родственников) на этапе первичного собеседования.
- **Безопасное хранение:** Все бумажные личные дела хранятся строго в запираемых металлических шкафах отдела кадров. Запрещено создание неучтенных локальных копий на компьютерах.
- **Уничтожение:** Резюме кандидатов, не прошедших конкурсный отбор, подлежат уничтожению сразу после подведения итогов конкурса. Бумажные документы уничтожаются через офисный шредер, электронные файлы удаляются без возможности восстановления.

ПРИЛОЖЕНИЕ 7 (КОД: AMAC-GDPR-EX-07) · РЕГЛАМЕНТ СОРАЗМЕРНОГО ИТ-МОНИТОРИНГА

Правила контроля использования служебного оборудования и инфраструктуры предприятия.

Область контроля	Допустимые границы (Правильный подход)	Строгие запреты (Чего избегать)
Видеонаблюдение (CCTV)	Установка камер на входах, в коридорах, кассовых зонах и серверных для безопасности.	Размещение камер в рабочих кабинетах офиса, зонах отдыха и санитарных комнатах.
Служебные авто (GPS)	Контроль перемещения для оптимизации выездов аварийных бригад и расчета топлива.	Отслеживание перемещений сотрудников вне установленного рабочего времени.
Личные гаджеты (BYOD)	Доступ к рабочей почте без локального сохранения файлов на личный телефон.	Скачивание, копирование и хранение баз данных клиентов компании на личных ПК/ смартфонах.
Корпоративная почта	Анализ логов безопасности, блокировка спама и фишинга на уровне сервера.	Регулярное чтение содержания писем сотрудников руководителями «из любопытства».

> **Обязательное условие:** Введение или изменение любых мер технического мониторинга требует предварительного официального уведомления персонала под подпись и проведения консультаций с профсоюзом (представителями работников).

ПРИЛОЖЕНИЕ 8 (КОД: AMAC-GDPR-EX-08) · ЧЕК-ЛИСТ БЕЗОПАСНОСТИ РАБОЧЕГО МЕСТА

Ежедневные гигиенические правила ИБ для каждого сотрудника организации:

Раздел А. Логическая защита

- Никогда не передавать свои пароли коллегам.
- Всегда блокировать экран компьютера (`Win+L`) при любом выходе из кабинета.
- Запрещено устанавливать личные или пиратские программы.
- Не открывать подозрительные ссылки и вложения в email.

Раздел Б. Физическая защита

- Дверь в серверную комнату должна быть всегда закрыта на замок.
- Правило «Чистого стола»: не оставлять документы с ПД на столе или у принтера.
- Разворачивать мониторы так, чтобы посетители не видели конфиденциальный экран.

ПРИЛОЖЕНИЕ 9 (КОД: AMAC-GDPR-EX-09) · ПОЛОЖЕНИЕ О РАБОТЕ С ИТ-ПОДРЯДЧИКАМИ

Когда внешняя обслуживающая организация получает доступ к ИТ-системам оператора, отношения сторон должны быть жестко регламентированы.

Обязательные этапы и требования к бизнес-процессу:

- **Проверка роли:** Определяется, является ли подрядчик обработчиком данных (процессором) от имени оператора. Простое соглашение о конфиденциальности (NDA) не заменяет обязательный договор DPA.
- **Минимизация выгрузок:** Партнеру передается только та часть базы, без которой невозможно оказать услугу (передача полных баз «на всякий случай» запрещена).
- **Сроки уведомления DPO:** Ответственный менеджер проекта **обязан в течение 5 календарных дней** с момента подписания договора передать сведения Сотруднику по защите данных (DPO) для внесения контрагента в обязательный корпоративный Реестр лиц, уполномоченных на обработку данных.

Дисклеймер: Настоящий документ носит информационный характер. Для получения официальных юридических заключений и настройки систем консультируйтесь с профильными специалистами и вашим DPO. AI-модели могут допускать неточности.