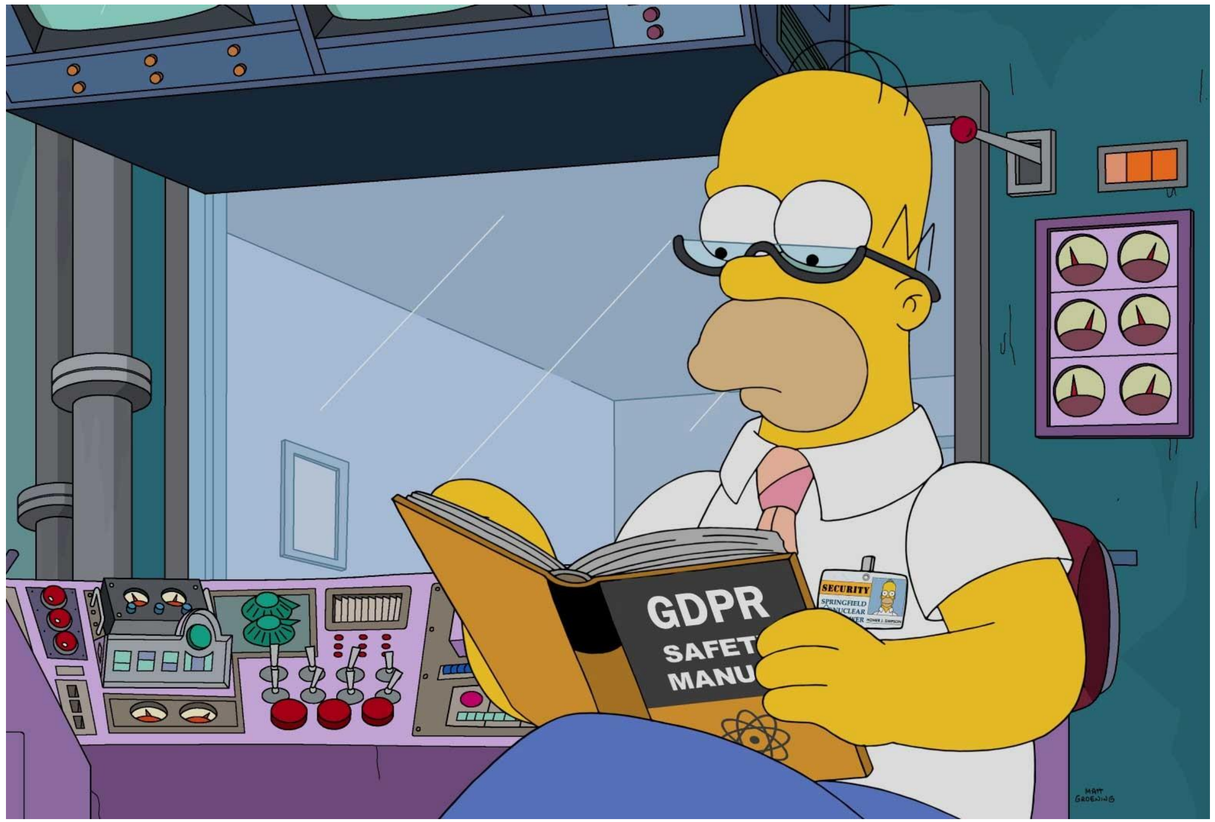
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

25 октября 2018 г.
г. Казань

#CODEIB

КАК СООТВЕТСТВОВАТЬ GDPR, ОКАЗЫВАЯ СЕРВИС ИЗ РОССИИ



КАМИЛА ИОСИПОВА, МИХАИЛ ЦЫКАРЕВ
КОМПАНИЯ ICL-SERVICES

EMAIL: Kamila.Balzamova@icl-services.com
Mikhail.Tsykarev@icl-services.com

СОДЕРЖАНИЕ

Еще раз про GDPR

#CODEIB

Цель закона

- 25 мая вступил в силу GDPR – новый европейский закон о защите персональных данных граждан ЕС
- Цель закона - предоставить гражданам ЕС инструменты для полного контроля над своими персональными данными
- GDPR имеет экстерриториальное действие и применяется ко всем компаниям, обрабатывающим персональные данные граждан ЕС, независимо от местонахождения такой компании

Основные термины

Персональные данные (ПДн) — все что может участвовать в идентификации человека (имя, фото, адрес, друзья, cookies, IP – адрес). Очень широкое понятие.

Контролер (**Data Controller)**: лицо или организация, которая определяет цели и средства обработки персональных данных.

Обработка ПДн (Processing): Любая операция или набор операций, выполняемых с ПДн или с набором ПДн как с использованием средств автоматизации, так и без использования оных, включая: сбор, запись, структурирование, хранение, адаптацию или изменение, использование, распространение, ограничение, уничтожение

Обработчик ПДн (Data Processor): это лицо или организация, которая обрабатывает персональные данные от имени **Data Controller**.

Соглашение об обработке данных (Data Processing Agreement, DPA): это общее определение любого соглашения между Russia GDC и Дата Контроллером(Data Controller) или другим Обработчиком ПДн (Data Processor), которое регулирует обработку и защиту ПДн

Утечка ПДн (Personal Data breach) – означает нарушение безопасности, приводящее к случайному или противозаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к ПДн, переданных, хранящихся или обработанных иным образом

Обработка ПДн

6 принципов обработки данных по GDPR

1. ЗАКОННОСТЬ, СПРАВЕДЛИВОСТЬ И ПРОЗРАЧНОСТЬ
2. ОГРАНИЧЕНИЕ ЦЕЛИ
3. МИНИМИЗАЦИЯ ДАННЫХ
4. ТОЧНОСТЬ
5. ОГРАНИЧЕНИЕ ХРАНЕНИЯ
6. ЦЕЛОСТНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ

Обеспечение ИБ – один из принципов обработки ПДн по GDPR

#CODEIB

GDPR Compliance Project

#CODEIB

DATA MAPPING

1 ОПРЕДЕЛЕНИЕ ВСЕХ СТОРОННИХ ПОСТАВЩИКОВ, СИСТЕМ И СЕРВИСОВ ТРЕТЬИХ СТОРОН, ОБРАБАТЫВАЮЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

2 ВЫПОЛНЕНИЕ DATA MAPPING ВСЕХ ВЫЯВЛЕННЫХ СИСТЕМ И СЕРВИСОВ ТРЕТЬИХ СТОРОН, ОБРАБАТЫВАЮЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

3 ПОДГОТОВКА И УТВЕРЖДЕНИЕ ПЛАНА ДЕЙСТВИЙ ПО КАЖДОЙ ИЗ СИСТЕМ

РАЗРАБОТКА ПОЛИТИК И ПРОЦЕССОВ

1 АНАЛИЗ ПРОЦЕССОВ, СВЯЗАННЫХ С ПЕРЕДАЧЕЙ ДАННЫХ

2 УВЕДОМЛЕНИЯ ОБ УТЕЧКАХ

3 РЕАЛИЗАЦИЯ «ПРАВА НА ЗАБВЕНИЕ» (RTBF)

4 РЕАЛИЗАЦИЯ ЗАПРОСОВ НА ОБРАБОТКУ ДАННЫХ (SAR)

5 ОПИСАНИЕ ЖИЗНЕННОГО ЦИКЛА ДАННЫХ

СООТВЕТСТВИЕ СИСТЕМ

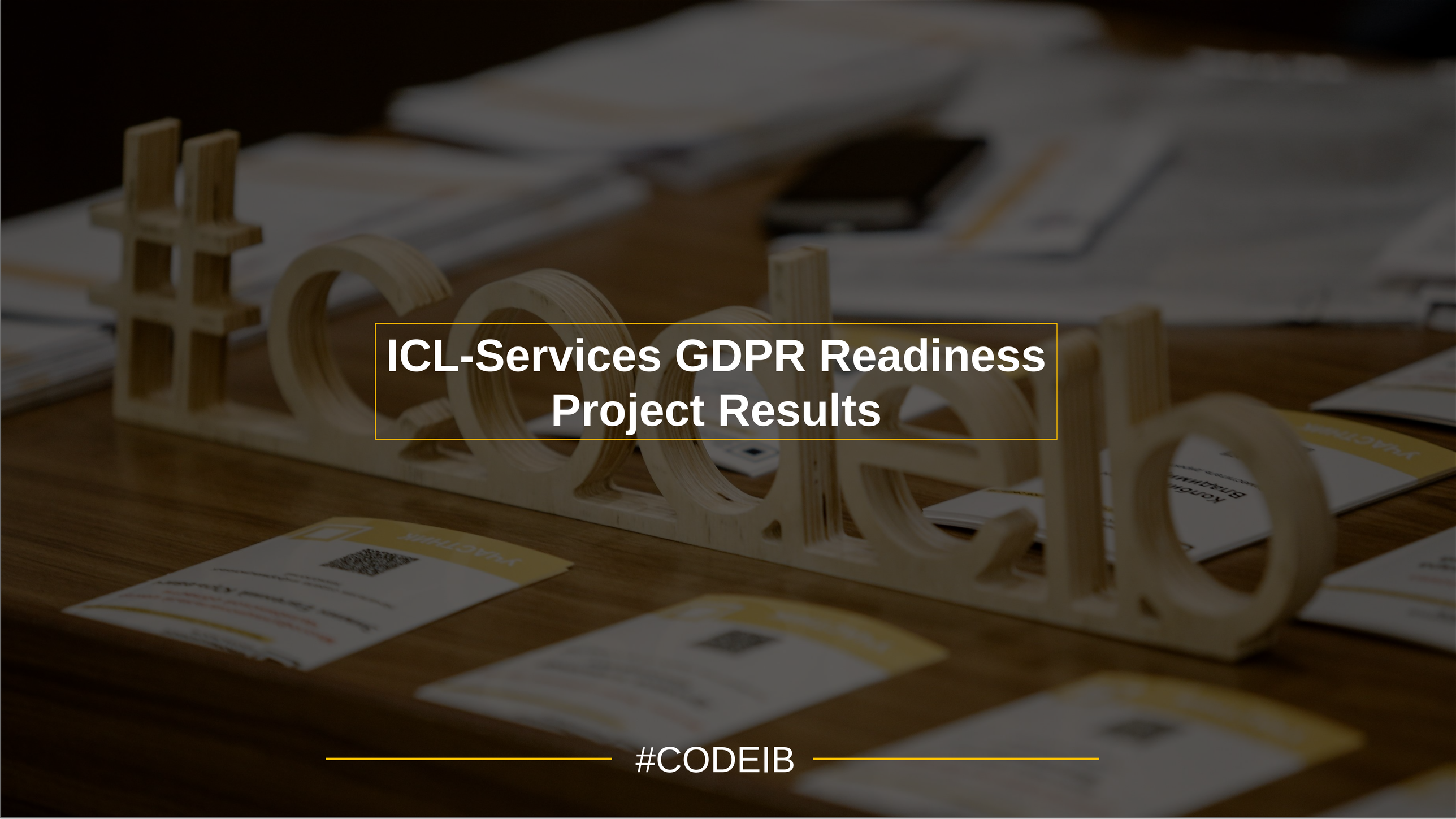
1 АУДИТ СИСТЕМ, ИСПОЛЬЗУЕМЫХ СОВМЕСТНО С ПАРТНЕРАМИ, ОБРАБАТЫВАЮЩИХ ПДН ЗАКАЗЧИКОВ

2 АУДИТ ВНУТРЕННИХ СИСТЕМ, ОБРАБАТЫВАЮЩИХ ПДН ЗАКАЗЧИКОВ

3 АУДИТ САЙТОВ ОБРАБАТЫВАЮЩИХ ПДН ЗАКАЗЧИКОВ

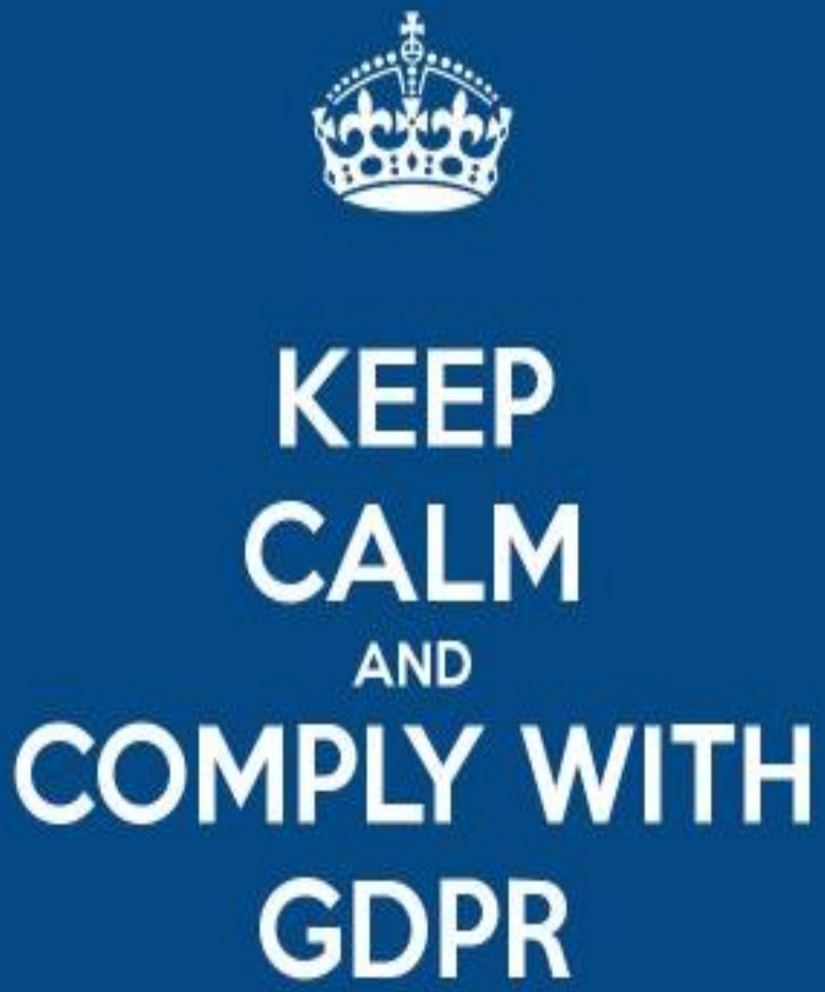
4 РАЗРАБОТКА ПЛАНОВ И МЕТОДОВ РЕАГИРОВАНИЯ

5 ПРИВЕДЕНИЕ СИСТЕМ В СООТВЕТСТВИЕ С GDPR



ICL-Services GDPR Readiness Project Results

#CODEIB



GDPR Readiness Project Results

- В рамках стратегического проекта «GDPR compliance»:
  - разработан ряд документов, в том числе General Personal Data Protection Policy
  - разработаны новые положения в контракты
  - создан новый класс инцидента ИБ – Personal Data Breach
  - Разработана ролевая инструкция Data Protection Consultant Role Profile
- Провели тренинг по GDPR в e-learning системе
- Включили пункты про GDPR в план адаптации новых сотрудников

Data Protection Consultant

- Разработана ролевая инструкция
Data Protection Consultant Role Profile
- Обязанности Data Protection Consultant:
  - Разработка документов, процессов
  - Осведомленность сотрудников компании по вопросам GDPR
  - Координация исполнения запросов и инцидентов на тему GDPR
  - Взаимодействие с DPO Data Controller/ заказчика
  - Инвентаризация ПДн
  - Пересмотр DTA

Обработка запросов (Data Controller Requests)

- **Data Controller Request Guideline** регламентирует деятельность Компании при получении запросов от Data Controller, выполнении таких запросов, подготовку и отправку ответа. У нас 14 рабочих дней на то чтобы оформить ответ
- Для подготовки запроса и ответа на данный запрос разработаны шаблоны форм **Data Controller Request Form** и **Response to Data Controller Request Form** соответственно

Реагирование на инциденты

- GDPR обязывает Data Controller уведомлять об утечках ПДн (Personal Data breach) в течении 72 часов
- У нас всего 24 часа чтобы сформировать отчет и сообщить Data Controller что произошла утечка ПДн
- Мы ввели новый класс инцидента ИБ - «Personal Data Breach».

И внесли изменения в существующий процесс «Управлять инцидентами ИБ» и в процедуру «Классифицировать инцидент ИБ»

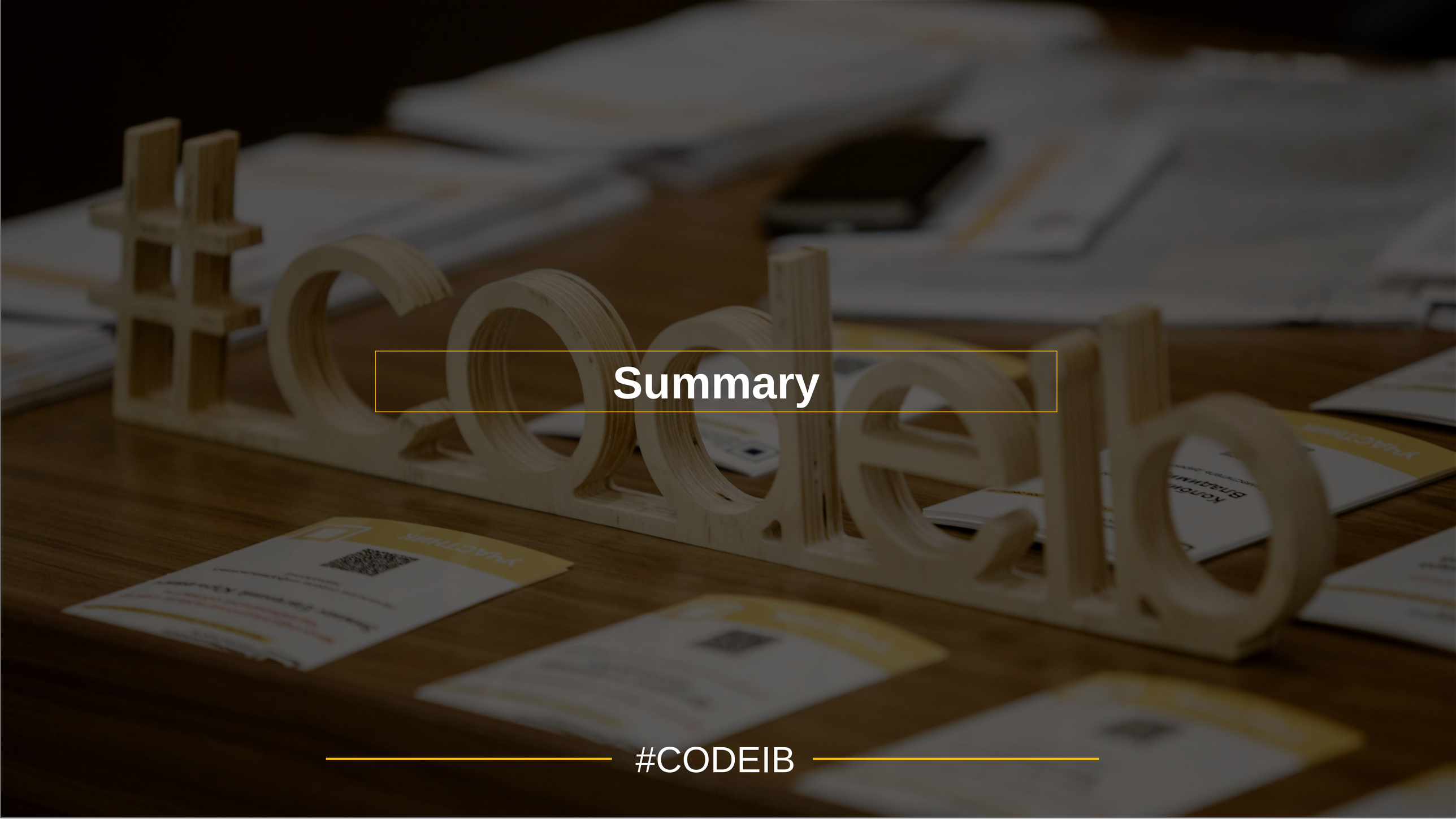
- Порядок реагирования на подобные инциденты описан в процедуре «Реагировать на Personal Data Breach»

Аудит и отчетность

- Группа Внутреннего аудита отвечает за проверку соответствия подразделений компании политике GDPR Policy

- Мы предоставляем право нашим заказчикам проводить GDPR аудиты

Любой сотрудник, который нарушает GDPR Policy компании будет подвергнут дисциплинарному взысканию, а также может быть подвергнут гражданским или уголовным обязательствам, если его поведение нарушает законы или правила Российской Федерации.



Summary

#CODEIB

Summary

ОПРЕДЕЛИТЕ ПЕРЕЧЕНЬ
КОНТРАГЕНТОВ

ОПРЕДЕЛИТЕ СВОИ РОЛИ
В ОТНОШЕНИИ КОНТРАГЕНТОВ

ОПРЕДЕЛИТЕ ПЕРЕЧЕНЬ
СИСТЕМ, ОБРАБАТЫВАЮЩИХ ПДн

РАЗРАБОТАЙТЕ И ВНЕДРИТЕ
ПРОЦЕССЫ

ПОДГОТОВЬТЕ НЕОБХОДИМЫЕ
ДОКУМЕНТЫ,
ВЫДЕЛИТЕ РОЛЬ DPC(DPO)

ОБУЧИТЕ СОТРУДНИКОВ

СПАСИБО ЗА ВНИМАНИЕ!