

Защита данных по GDPR

Штрафы и утечки

Алексей Мунтян
Генеральный директор Privacy Advocates

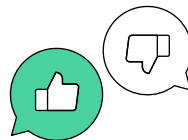


Проверка связи





Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти



Поставьте в чат:

-  если меня видно и слышно
-  если нет

Алексей Мунтян

О спикере:

- основатель и CEO компании Privacy Advocates
- соучредитель [Сообщества профессионалов](#) в области приватности
- внешний data protection officer в нескольких транснациональных холдингах
- сопредседатель кластера Privacy & Legal Innovation в РАЭК
- участник центров компетенций «Информационная безопасность» и «Нормативное регулирование» при АНО «Цифровая экономика»
- участник комитета по безопасности данных партнёров и пользователей при Консультативном совете Яндекса по развитию экосистемы



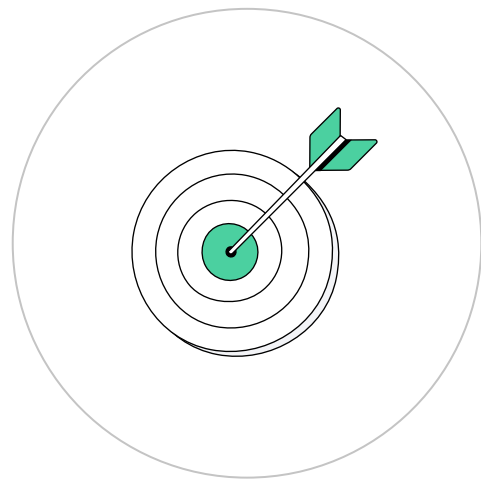
Правила участия

- 1 Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
- 2 Продолжительность вебинара — 80 минут
- 3 Вы можете писать свои вопросы в чате
- 4 Запись вебинара будет доступна



Цели занятия

- Обсудим, какие штрафы накладывают за нарушение GDPR
- Узнаем требования GDPR к защите персональных данных (ПД)
- Поймём, как реализовать концепт *privacy by design & by default*
- Изучим процесс оценки воздействия на защиту данных — DPIA (data protection impact assessment)



План занятия

- 1 Штрафы за нарушение GDPR
- 2 Требования GDPR к защите персональных данных
- 3 Privacy by design & by default
- 4 DPIA: как с ней работать



Штрафы за нарушение GDPR



1

Штрафы по GDPR

В GDPR (ст. 83) есть две категории штрафов за невыполнение требований*:

- До 10 млн € или 2% годового оборота. Например, за нарушение правила privacy by design
- До 20 млн € или 4% годового оборота. Например, за нарушение правил защиты данных

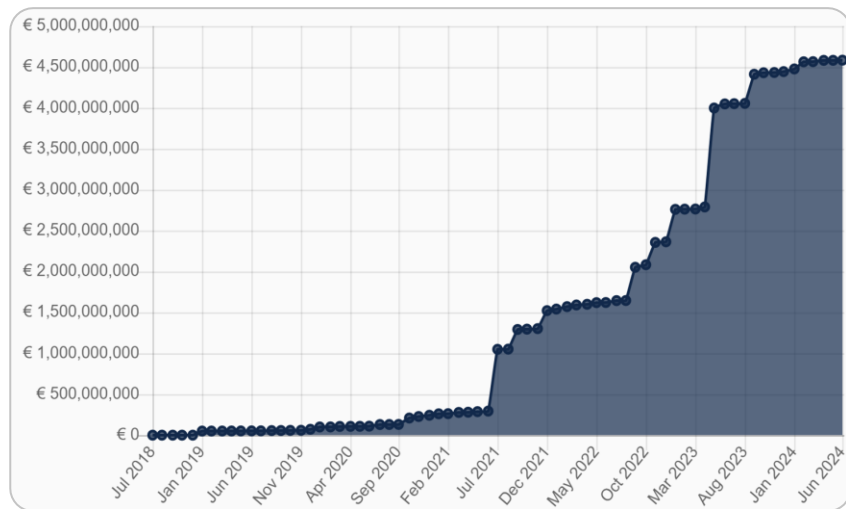
Государства — участники ЕС устанавливают нормы относительно иных санкций, применимых за нарушения GDPR, в том числе за нарушения, которые не подпадают под административные штрафы, а также принимают все меры для того, чтобы обеспечить их применение (ст. 84 GDPR)



Источник

* По состоянию на 31 октября 2023 г.

Объём и количество наложенных штрафов



Статистика по общей сумме штрафов. Топ-10 стран

	Страна	Сумма штрафов
1	Ирландия	2 855 363 400 € (при 27 штрафах)
2	Люксембург	746 314 000 € (32 штрафа)
3	Франция	371 699 300 € (49 штрафов)
4	Италия	229 657 327 € (373 штрафа)
5	Испания	81 208 010 € (865 штрафов)
6	Великобритания	75 541 500 € (при 15 штрафах)
7	Германия	55 496 833 € (всего 192 штрафа)
8	Греция	34 247 140 € (всего 68 штрафов)
9	Швеция	27 762 230 € (всего 39 штрафов)
10	Нидерланды	24 930 500 € (при 25 штрафах)

Общая сумма— 3 млрд €

По состоянию на 27 июня 2024 г.

Источник

Статистика по количеству штрафов. Топ-10 стран

	Страна	Количество штрафов
1	Испания	865 (на общую сумму 81 208 010 €)
2	Италия	373 (на общую сумму 229 657 327 €)
3	Германия	192 (на общую сумму 55 496 833 €)
4	Румыния	182 (на общую сумму 1 144 950 €)
5	Польша	76 (на общую сумму 4 002 979 €)
6	Греция	68 (на общую сумму 34 247 140 €)
7	Венгрия	68 (на общую сумму 2 518 861 €)
8	Норвегия	51 (на общую сумму 12 117 950 €)
9	Франция	49 (на общую сумму 371 699 300 €)
10	Кипр	44 (на общую сумму 1 432 500 €)

По состоянию на 27 июня 2024 г.

Источник

Статистика штрафов по типам нарушений. Общая сумма штрафов

Нарушение	Сумма штрафов
Несоблюдение общих принципов обработки данных	2 082 560 039 € (всего 592 штрафа)
Недостаточная правовая база для обработки данных	1 652 000 812 € (всего 643 штрафа)
Недостаточные технические и организационные меры для обеспечения информационной безопасности	475 577 615 € (всего 385 штрафов)
Недостаточное выполнение информационных обязательств	247 850 060 € (всего 192 штрафа)
Недостаточное соблюдение прав субъектов персональных данных	98 553 370 € (при 210 штрафах)
Неизвестно	23 200 700 € (всего 11 штрафов)
Недостаточное сотрудничество с надзорным органом	6 433 329 € (всего 119 штрафов)
Недостаточное выполнение обязательств по уведомлению о нарушении данных	3 031 392 € (при 44 штрафах)
Недостаточное соглашение об обработке данных	1 117 110 € (всего 12 штрафов)
Недостаточное участие сотрудника по защите данных	961 300 € (всего 21 штраф)

По состоянию на 27 июня 2024 г.
Источник

Статистика штрафов по типам нарушений. Количество штрафов

Нарушение	Количество штрафов
Недостаточная правовая база для обработки данных	643 (на общую сумму 1 652 000 812 €)
Несоблюдение общих принципов обработки данных	592 (на общую сумму 2 082 560 039 €)
Недостаточные технические и организационные меры для обеспечения информационной безопасности	385 (на общую сумму 475 577 615 €)
Недостаточное соблюдение прав субъектов персональных данных	210 (на общую сумму 98 553 370 €)
Недостаточное выполнение информационных обязательств	192 (на общую сумму 247 850 060 €)
Недостаточное сотрудничество с надзорным органом	119 (на общую сумму 6 433 329 €)
Недостаточное выполнение обязательств по уведомлению о нарушении данных	44 (на общую сумму 3 031 392 €)
Недостаточное участие сотрудника по защите данных	21 (на общую сумму 961 300 €)
Недостаточное соглашение об обработке данных	12 (на общую сумму 1 117 110 €)
Неизвестно	11 (на общую сумму 23 200 700 €)

По состоянию на 27 июня 2024 г.
[Источник](#)

Выводы

- Штрафы за неисполнение GDPR высокие и могут быть оборотными
- Неисполнение и неполное исполнение требований к обеспечению безопасности персональных данных — самые частые нарушения, за которые накладывают штрафы
- Штрафы по GDPR могут наложить за несоответствие более чем 40 требованиям, что делает обработку данных по нему высокорискованной





Ваши вопросы

Требования GDPR к защите персональных данных



2

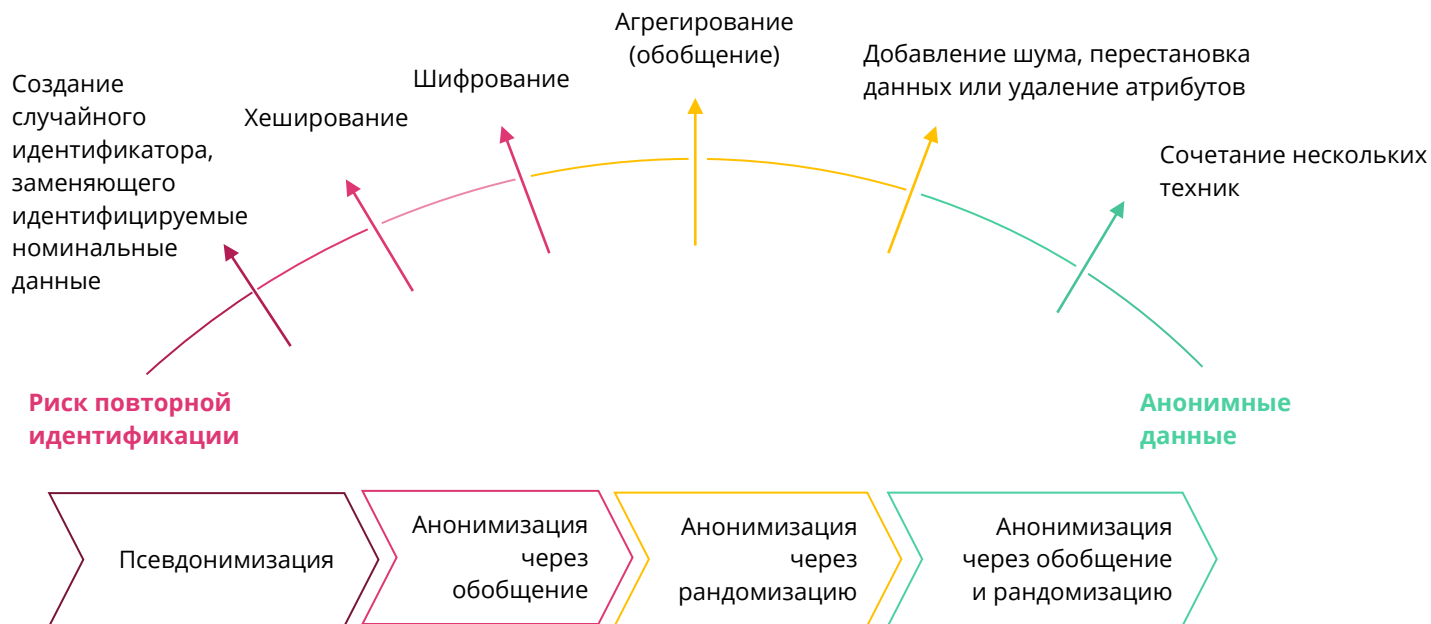
Основные требования к безопасности

1

Псевдонимизация
и шифрование данных*

* Псевдонимизация (pseudonymisation) — обработка персональных данных таким образом, что их больше невозможно отнести к конкретному субъекту данных без использования дополнительной информации, при условии, что такая дополнительная информация хранится отдельно и в отношении неё приняты технические и организационные меры, предотвращающие её отнесение идентифицированному или идентифицируемому физическому лицу. П. 5 ст. 4 GDPR

От псевдонимизации к анонимизации

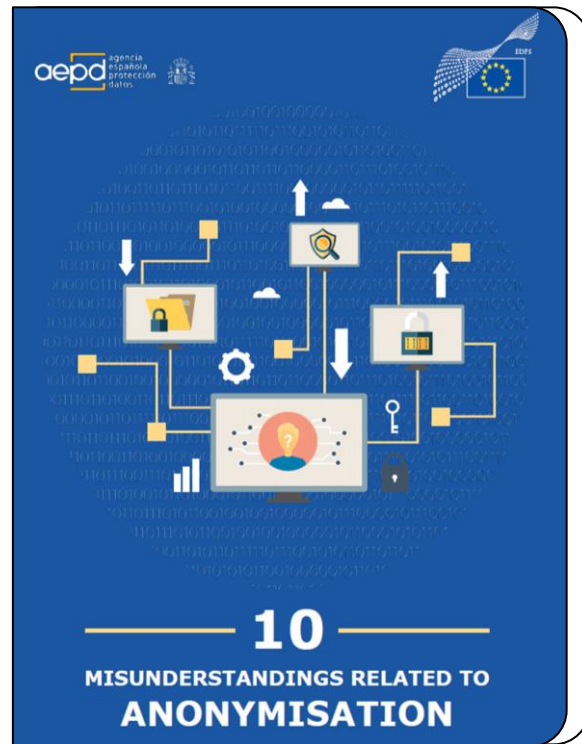


! Псевдонимизированные данные всё равно являются персональными данными

10 заблуждений об анонимизации

EDPS и AEPD опубликовали обзор заблуждений об анонимизации

- 1 Псевдонимизация — то же самое, что и анонимизация
- 2 Шифрование — это анонимизация
- 3 Анонимизация данных всегда возможна
- 4 Анонимизация — это навсегда
- 5 Анонимизация всегда сводит вероятность повторной идентификации набора данных к нулю

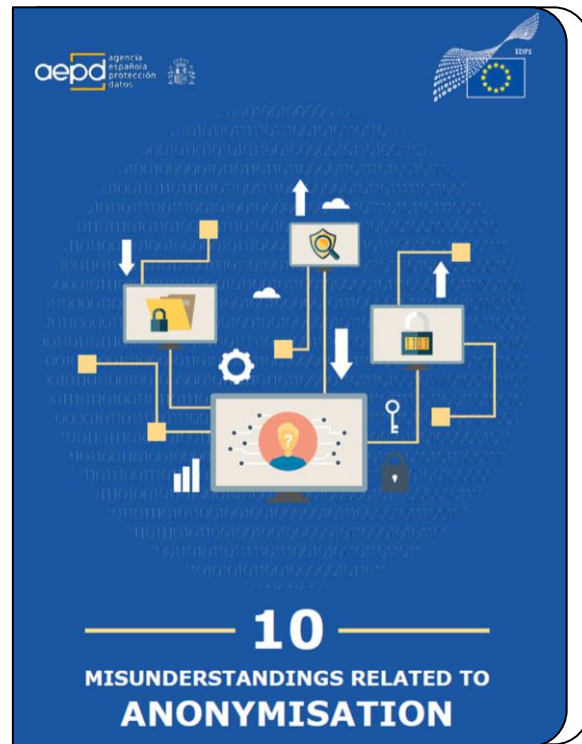


Источник

10 заблуждений об анонимизации

EDPS и AEPD опубликовали обзор заблуждений об анонимизации

- 6 Анонимизация — бинарное понятие, которое невозможно измерить
- 7 Анонимизация может быть полностью автоматизирована
- 8 Анонимизация делает данные бесполезными
- 9 Следование процессу анонимизации, который успешно использовали другие, приведёт ту или иную организацию к эквивалентным результатам
- 10 Нет никакого риска и интереса в том, чтобы узнать, к кому относятся эти данные



Источник

Основные требования к безопасности

1

Псевдонимизация
и шифрование данных

Основные требования к безопасности

1

Псевдонимизация
и шифрование данных

2

Обеспечение
конфиденциальности,
целостности, доступности
и устойчивости

Основные требования к безопасности

1

Псевдонимизация
и шифрование данных

2

Обеспечение
конфиденциальности,
целостности, доступности
и устойчивости

3

Обеспечение
восстановления
доступности данных

Основные требования к безопасности

1

Псевдонимизация
и шифрование данных

2

Обеспечение
конфиденциальности,
целостности, доступности
и устойчивости

3

Обеспечение
восстановления
доступности данных

4

Регулярное тестирование
и оценка эффективности
принимаемых мер

Основные требования к безопасности

1

Псевдонимизация
и шифрование данных

2

Обеспечение
конфиденциальности,
целостности, доступности
и устойчивости

3

Обеспечение
восстановления
доступности данных

4

Регулярное тестирование
и оценка эффективности
принимаемых мер

5

Реагирование
на инциденты безопасности
персональных данных

Основные требования к безопасности

1

Псевдонимизация
и шифрование данных

2

Обеспечение
конфиденциальности,
целостности, доступности
и устойчивости

3

Обеспечение
восстановления
доступности данных

4

Регулярное тестирование
и оценка эффективности
принимаемых мер

5

Реагирование
на инциденты безопасности
персональных данных

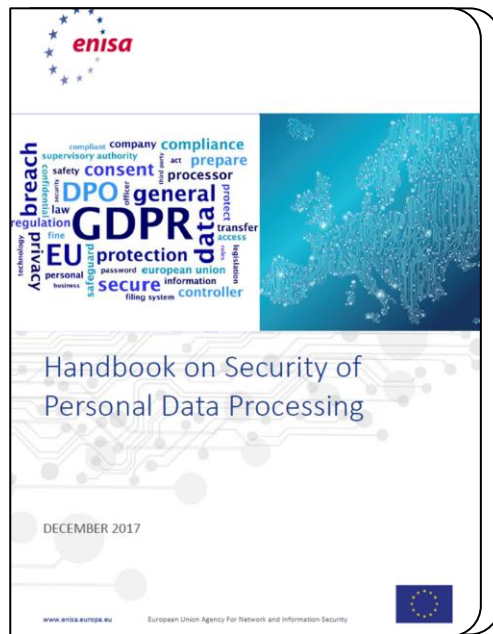
6

Обязательное обеспечение
безопасности данных
при любой их обработке

Руководство ENISA*



Источник



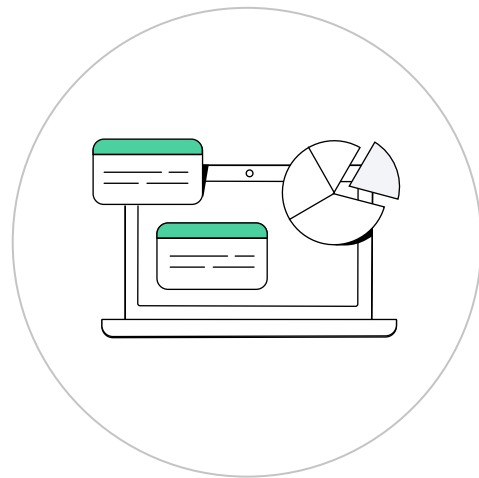
Источник

*ENISA (European Union Agency for Cybersecurity) — агентство Европейского союза по кибербезопасности

Data breach (инцидент с ПД)

Если инцидент в безопасности персональных данных влечёт риск для субъектов данных, необходимо:

- уведомить надзорный орган страны — участницы Евросоюза в течение 72 часов: предоставить информацию об инциденте, результатах расследования и минимизации последствий инцидента
- уведомить и субъектов персональных данных, если есть высокий риск для них и его нельзя уменьшить

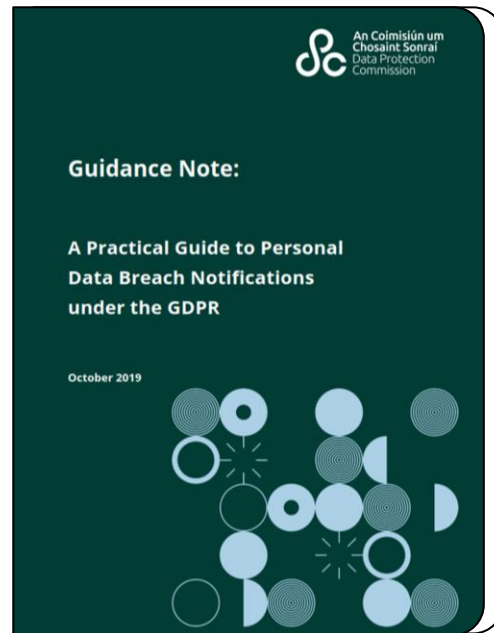


Руководство ирландского DPC по data breach

Ирландский надзорный орган **DPC (Data Protection Commission)** проанализировал полученные уведомления об утечках ПД (data breach notifications) из различных государственных и частных сфер, таких как банковское дело и финансы, страхование, телекоммуникации, здравоохранение, правоохранительные органы.

В октябре 2019 г. он опубликовал руководство, посвящённое **разбору типичных ошибок/проблем при уведомлениях об утечке данных:**

- несвоевременное уведомление
- сложность в оценке рейтингов риска
- неспособность сообщить об утечке субъектам данных, где это применимо
- повторные уведомления об утечках
- предоставление неполной и неточной информации



Источник

Сертификация

Требования к обеспечению безопасности ПД будут считаться выполненными, если соблюдено одно из условий:

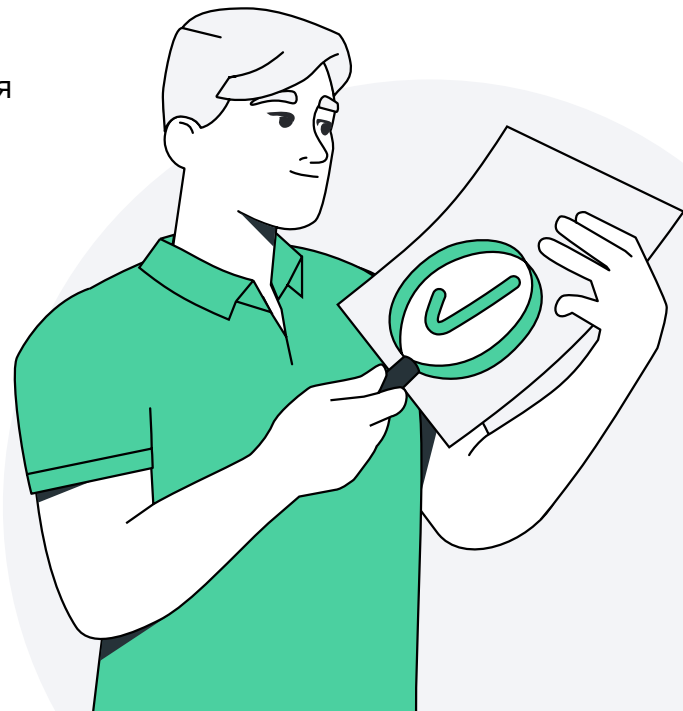
- ① Пройдена сертификация по GDPR
- ② Пройдена сертификация по одному из международных стандартов ИБ:
 - ISO 27701
 - ISO 27001
 - PCI DSS
 - SOC 2



Источник

Выводы

- Требования к обеспечению безопасности не устанавливают максимально точного перечня мер защиты, а только задают вектор. Меры защиты определяет сам контролёр
- Требования к обеспечению безопасности персональных данных в рамках GDPR можно не исполнять, если пройдена сертификация по одному из международных стандартов информационной безопасности
- К data breach по GDPR относятся не только утечки персональных данных, но и любые инциденты информационной безопасности, которые могут привести к риску для прав и свобод физических лиц





Ваши вопросы

Privacy by design & by default



3

Privacy by design & by default (PbDD)

Под приватностью в самом общем смысле понимают неприкосновенность частной и личной жизни.

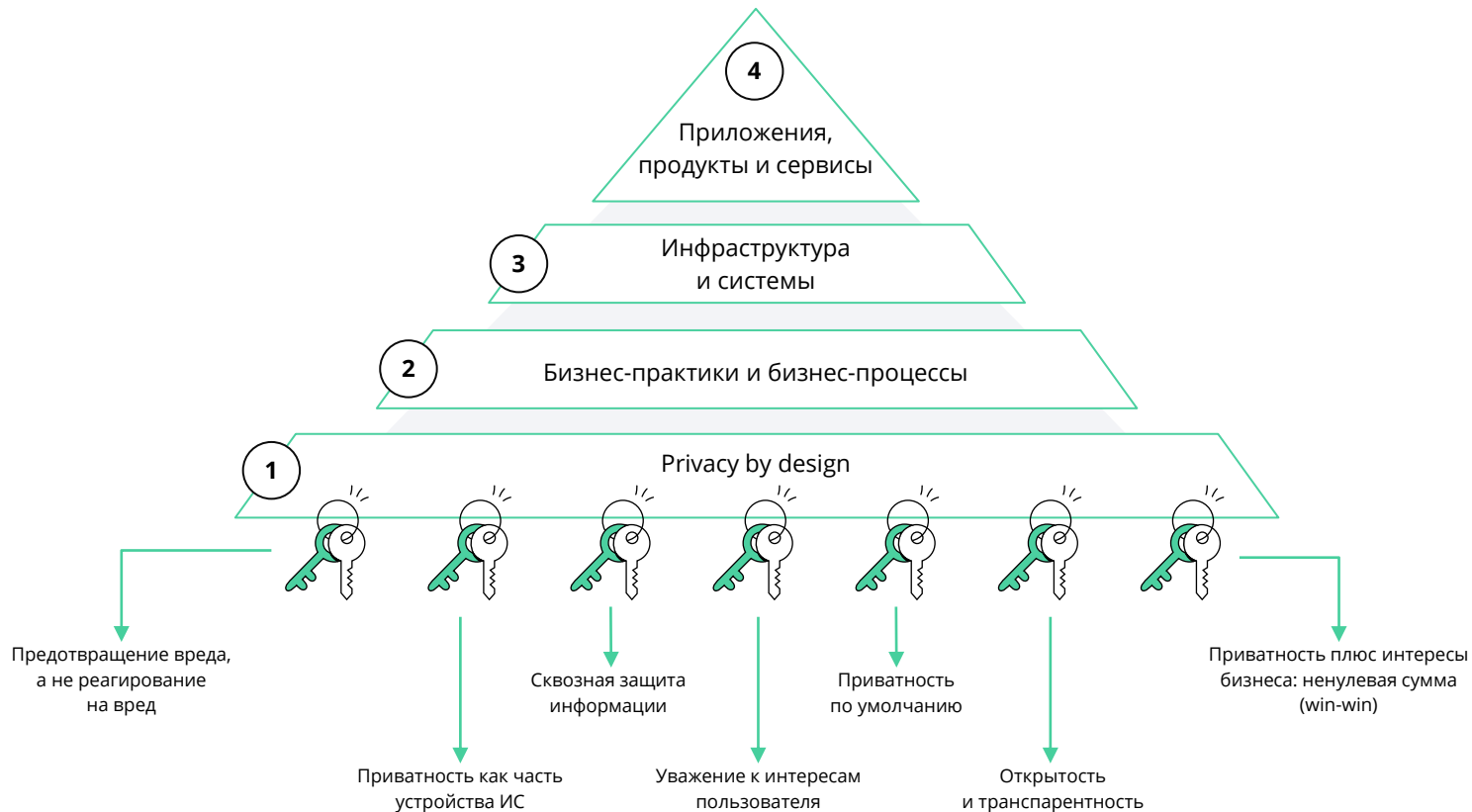
Виды приватности:

- телесная
- пространственная
- коммуникационная
- информационная

Термин «приватность» — калька с английского *privacy*, которое появилось в конце 19-го века как отражение желания уединиться и защитить личное пространство в ответ на развитие технологий, в частности фотографии

- Необходимость обеспечивать приватность потребовала мультидисциплинарного подхода к защите ПД при их обработке в информационных системах
- Его воплощением стала концепция **PbDD** — *privacy by design* (проектируемая приватность) и *privacy by default* (приватность по умолчанию)

Семь принципов PbDD от Энн Кавукян



Проектируемая приватность

Концепт призван решить проблему недальновидности контролёров, которые должны заранее продумывать механизмы защиты ПД на этапе планирования процедур их обработки в бизнес-активностях и ИТ-системах.

Концепт должен быть внедрён в процессы жизненного цикла разработки системы (SDLC), управления изменениями, а также в процессы проектного управления



Проектируемая приватность

- Контролёры перед запуском новых (модификацией существующих) бизнес-активностей и ИТ-систем должны проанализировать возможные риски для субъектов ПД с точки зрения возможности реализации их прав на доступ к своим данным, актуализации обрабатываемых данных, прекращения обработки данных и т. д.
- Дополнительно оценивается возможный вред субъектам ПД (privacy impact assessment), который может быть им нанесён в случае нарушения конфиденциальности ПД и безопасности их обработки



Стратегии проектируемой приватности

- 1 **Стратегии, ориентированные на данные**, имеют технический характер и фокусируются на обработке ПД с учётом требований приватности: **минимизации, сокрытия, разделения, объединения**
- 2 **Стратегии, ориентированные на процессы**, имеют организационный характер и фокусируются на определении процессов, обеспечивающих ответственное управление ПД: **информирование, контроль, принуждение, демонстрация**
- Стратегии проявляются в том числе как элементы пользовательского интерфейса (**паттерны приватности, privacy patterns**) и являются способом превращения privacy by design в практические советы для разработки ПО



Приватность по умолчанию

Суть концепта — **минимизировать активности по обработке ПД.**

Чем меньше объём обрабатываемых данных, способов и сроков их обработки, круг вовлечённых в обработку третьих лиц, тем безопаснее обработка для субъектов данных и самого контролёра



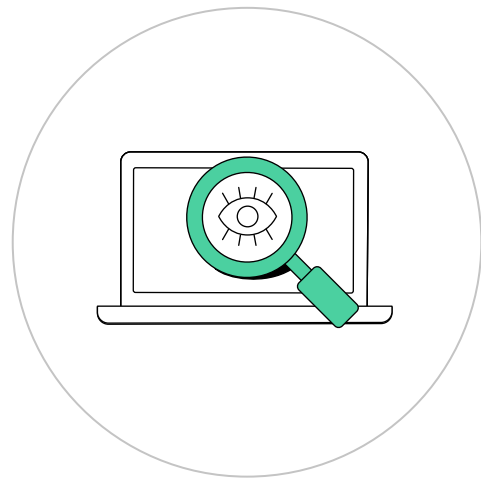
Приватность по умолчанию

- Минимизация обработки ПД позволяет вывести часть бизнес-процессов из-под регулирования законодательства о ПД и тем самым сэкономить силы и средства на контролёров
- Концепт privacy by default требует от контролёров соблюдения принципа подотчётности (accountability principle), то есть они должны знать, в каких процессах и ИТ-системах обрабатываются данные, в каком объёме, с какой целью и как долго



Стратегии приватности по умолчанию

- 1 **Оптимизация** направлена на анализ обработки данных с точки зрения приватности. То есть принимаются меры, которые минимизируют объём собираемых данных, способы и длительность их обработки, а также степень их доступности
- 2 **Конфигурирование** — возможность настроить параметры обработки данных с помощью функций, доступных пользователю в приложениях, устройствах или системах. То есть разумная часть этих параметров передаётся под контроль пользователя
- 3 **Ограничение** гарантирует, что при обработке данных максимально соблюдается приватность, поэтому настройки параметров должны быть установлены по умолчанию на значения, минимизирующие обработку персональных данных



Паттерны privacy by design для разработки ПО

Защита от отслеживания

Этот шаблон позволяет избежать отслеживания посетителей веб-сайтов с помощью файлов cookie. Для этого он удаляет файлы cookie через регулярные промежутки времени или полностью отключает их

Детализация местоположения

Поддержка минимизации сбора и распространения данных. Это важно, когда служба собирает данные о местоположении пользователя (в том числе от него самого) или передаёт данные о местоположении пользователя третьей стороне

Категории

- Контроль
- Абстрактный
- Отдельный
- Скрывать
- Минимизировать
- Поставить в известность
- Обеспечивать соблюдение

Минимальная информационная асимметрия

Предотвращайте лишение пользователей прав из-за незнания политик, потенциальных рисков и их участия в обработке

Информированные безопасные пароли

Убедитесь, что пользователи поддерживают здоровые привычки аутентификации посредством осведомлённости и понимания

Теги

- Печенье
- Анонимное общение
- Запутывание
- Прокси
- Анонимность
- РЗр
- Облако
- Маршрутизация

Выводы

- Лучший способ снизить риски, связанные с приватностью, — не создавать их. Чем меньше данных оператор собирает и обрабатывает, тем меньше риск нарушения прав и свобод субъектов данных, а также нанесения ущерба самому контролёру
- От человека не должно требоваться никаких действий для защиты его прав и свобод при обработке ПД. Субъект данных не должен нести бремя защиты своих ПД при использовании каких-либо услуг или продуктов. Право на неприкосновенность частной жизни будет защищаться автоматически в качестве настройки по умолчанию





Ваши вопросы

DPIA

Как с ней работать



4

DPIA

Если обработка данных несёт высокий риск для прав и свобод людей, требуется проводить процедуру DPIA*.

- Основная цель — понять последствия, которые могут наступить для субъекта и контролёра/процессора, если что-то пойдёт не так
- GDPR ставит задачи, обязательно решаемые в ходе DPIA. Структуру, форму и методологию контролёр/процессор определяет самостоятельно
- Вопрос необходимости проводить DPIA рекомендуется внедрить в процессы privacy by design



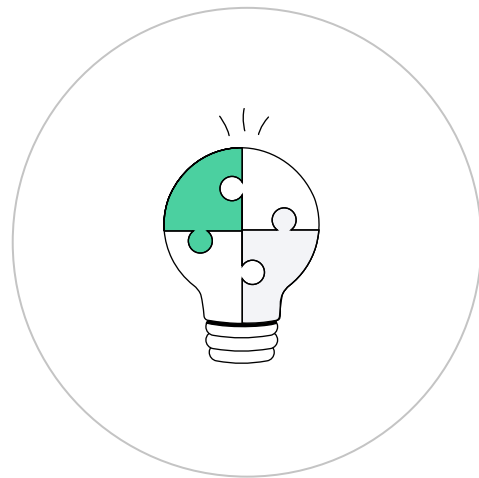
Источник

* Data protection impact assessment (DPIA) — оценка воздействия на защиту данных

DPIA

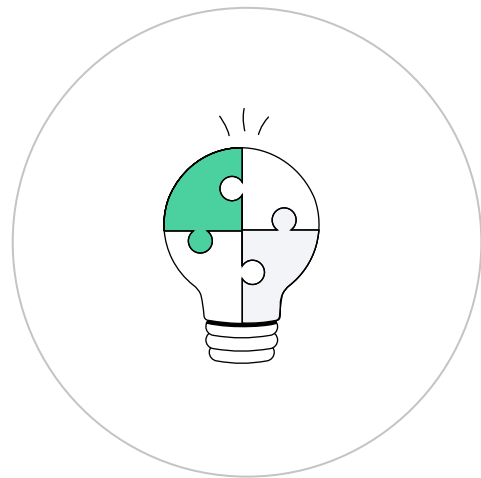
DPIA требуется в следующих случаях:

- профилирование и принятие автоматизированных решений
- крупномасштабная обработка чувствительных данных
- масштабный систематический мониторинг общедоступных мест



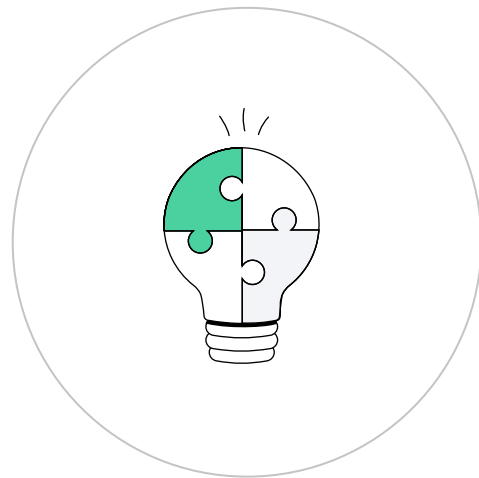
Что должно быть в DPIA

- 1 Информация об обработке персональных данных и инфраструктуре
- 2 Оценка исполнения принципов GDPR
- 3 Оценка законности работы с третьими лицами
- 4 Оценка исполнения прав по GDPR
- 5 Оценка рисков безопасности персональных данных

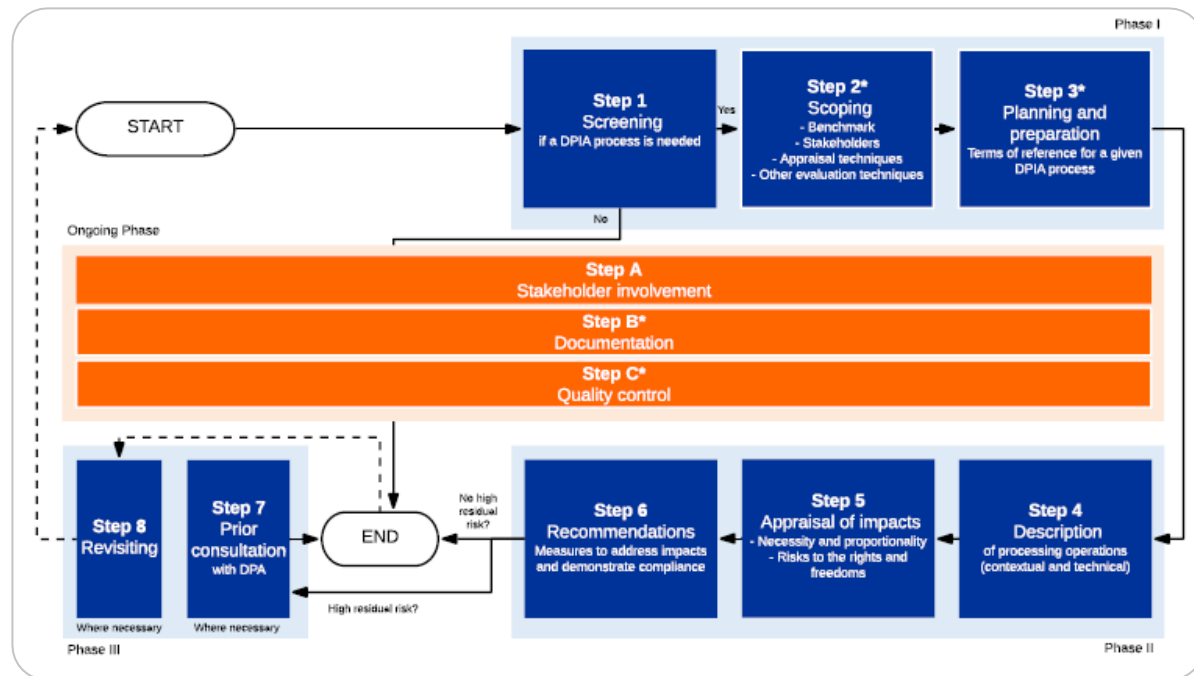


Что должно быть в DPIA

- 1 Информация об обработке персональных данных и инфраструктуре
 - 2 Оценка исполнения принципов GDPR
 - 3 Оценка законности работы с третьими лицами
 - 4 Оценка исполнения прав по GDPR
 - 5 Оценка рисков безопасности персональных данных
- DPIA можно проводить для отдельной процедуры обработки данных или для всей компании сразу



Руководство по проведению и образец DPIA от Брюссельского свободного университета



Выводы

- Процедуры data protection impact assessment нужно проводить, если при обработке данных создаётся высокий риск для прав и свобод физических лиц
- DPIA носит декларативный характер и призвана показать, что организация сделала всё, чтобы минимизировать риски для прав и свобод физических лиц





Ваши вопросы

Итоги занятия

Сегодня мы:

- Разобрали штрафы GDPR за невыполнение мер по безопасности данных
- Ознакомились с основными требованиями GDPR к обеспечению безопасности данных
- Обсудили актуальные подходы к обеспечению приватности
- Разобрали реализацию концепта privacy by design & by default
- Изучили, что такое DPIA и как её проводить



Дополнительные материалы

- [Методы](#) псевдонимизации
- [Data protection engineering](#)
- [Методика оценки](#) риска от утечки
- [Разъяснения EDPB](#) по реагированию на инциденты
- [Методика и тул CNIL](#) по проведению PIA



Защита данных по GDPR

Штрафы и утечки

Алексей Мунтян
Генеральный директор Privacy Advocates

