Технические аспекты GDPR
Как не задолжать внезапно €20 Million

Дмитрий Соловьев

Program Manager, Plesk

plesk

Кто читал статьи на хабре?

GDPR как оружие массового поражения

Управление продуктом, Информационная безопасность, Законодательство в IT, IT-стандарты, Блог компании Plesk

Под угрозой все. Вообще все

Бытует мнение, что сочинение законов, которые нарушают практически все – это изобретение нашей Родины. Но, как и со слонами, всё не так однозначно: при изучении General Data Protection Regulation (GDPR) я понял, что в этом мы безнадёжно отстали от Европы. Шутка ли – завиноватить одним махом весь мир! Думаете, вашей компании не предстоит прогибаться под GDPR? Я развею это опасное заблуждение.

В этой статье я не буду описывать все закорючки GDPR, знакомство с которыми первым делом порождает вопрос «А нельзя ли просто забанить всех европейцев?» (и это не шутка, так и спрашивают), но сосредоточусь на запугивании тех, кто до сих пор не исследовал вопрос влияния GDPR на свою работу, априори полагая, что находятся вне зоны поражения.

GDPR на носу – прекращаем панику и начинаем спасаться

Управление продуктом, Информационная безопасность, Законодательство в IT, IT-стандарты, Блог компании Plesk

Судя по нарастающей в сети панике, очень многие либо только узнали о GDPR, либо оттянули удовольствие до предела.

Уже 25 мая угроза штрафа в 20 млн Евро или 4% от мирового оборота (что из этого больше) станет реальностью – впадать в панику или не впадать? Поскольку я уже ливанул ведро бензина в огонь, чувствую себя обязаным показать дорогу к пожарному выходу, не дожидаясь анонсированного в предыдущей статье события. Зарание прошу прощения за шероховатости – экспромт, очень fast и очень dirty, зато полезность зашкаливает (надеюсь).

plesk

Если вы здесь - вы уже боитесь

И это хорошо

plesk

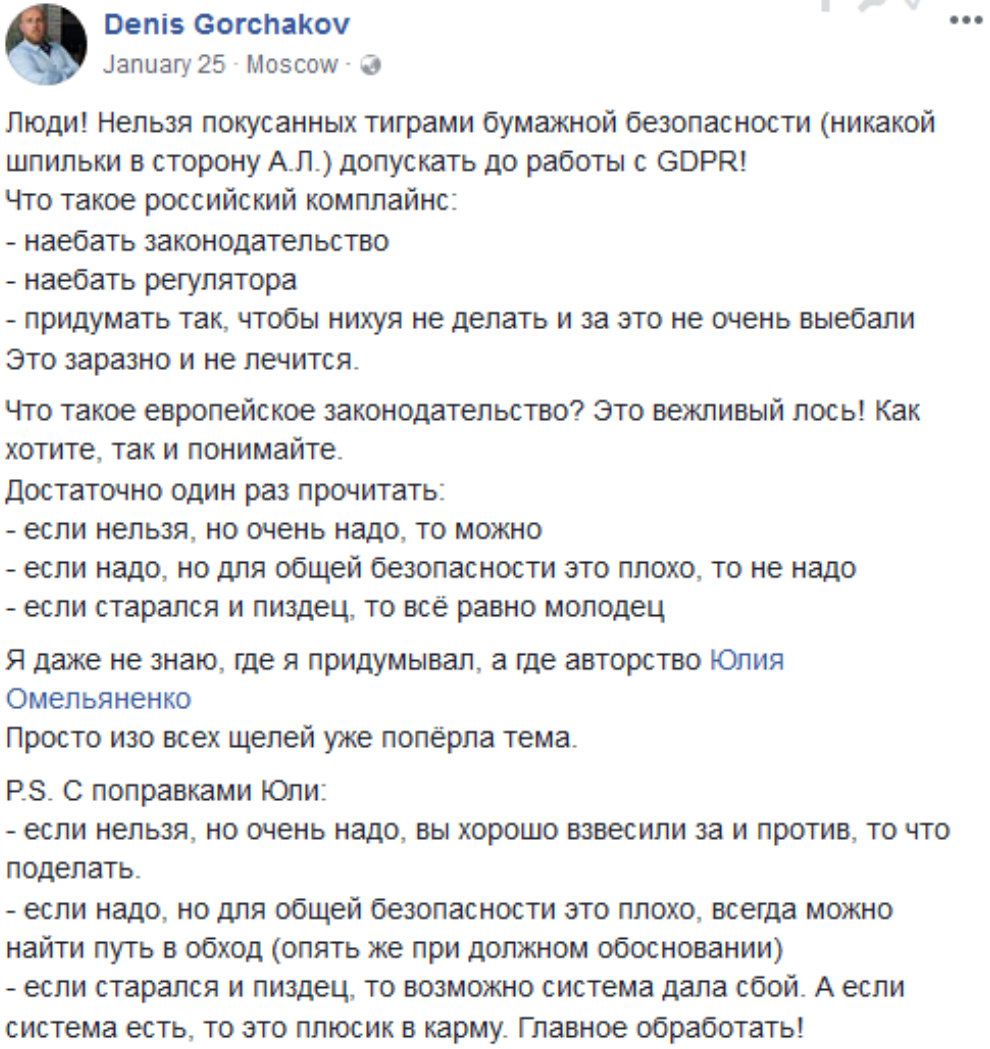
Буду делиться своей паранойей

А что?..

Отсутствие правоприменительной практики позволяет.

plesk

GDPR – не бумажная проблема



Denis Gorchakov
January 25 · Moscow ·

Люди! Нельзя покусанных тиграми бумажной безопасности (никакой шпильки в сторону А.Л.) допускать до работы с GDPR!
Что такое российский комплайнс:
- наебать законодательство
- наебать регулятора
- придумать так, чтобы нихуя не делать и за это не очень выебали
Это заразно и не лечится.

Что такое европейское законодательство? Это вежливый лось! Как хотите, так и понимайте.
Достаточно один раз прочитать:
- если нельзя, но очень надо, то можно
- если надо, но для общей безопасности это плохо, то не надо
- если старался и пиздец, то всё равно молодец

Я даже не знаю, где я придумывал, а где авторство Юлия Омельяненко
Просто изо всех щелей уже попёрла тема.

P.S. С поправками Юли:
- если нельзя, но очень надо, вы хорошо взвесили за и против, то что поделать.
- если надо, но для общей безопасности это плохо, всегда можно найти путь в обход (опять же при должном обосновании)
- если старался и пиздец, то возможно система дала сбой. А если система есть, то это плюсик в карму. Главное обработать!

Нельзя купить какой-нибудь сертификат и успокоиться.

Точнее, можно – но только до первого вопроса по теме.

plesk

Точнее – не только бумажная

- Пачки бумаг нужны – но вместе с реальными изменениями, а не вместо них.
- Бумажная часть сейчас out of scope.
- Ну буквально пару слов:
  - Политики конфиденциальности для клиентов.
  - Соглашения о защите данных с партнёрами.
  - Контракты с работниками.
  - И т.д. и т.п.
- Да, вам придётся заплатить юристу.

plesk

Соответствие GDPR - комплексная задача

plesk

Есть только два простых решения (1 из 2)

Избавиться от европейцев.

Увы, этот сервис – шутка.

Но решение – не шутка. Если вы можете себе это позволить.

plesk

Есть только два простых решения (2 из 2)

- Избавится от всего, что может быть сочтено персональными данными по GDPR.
- Для этого придётся:
  - Понять, что считается персональными данными в GDPR.
  - Провести ревизию своих продуктов и сервисов для идентификации таких данных.
  - Определить возможность их удаления или анонимизации.
  - Реализовать это.
- Хм… Есть только одно простое решение.

plesk

В остальных случаях

- Назначаем ответственного.
- Определяем риски для бизнеса.
- Диагностируем основные проблемы.
- Решаем их в порядке приоритета.
- Параллельно оформляем бумаги.

(Последний раз вспоминаю про бюрократию)

plesk

Выбираем ответственного за GDPR

- Modus operandi.
- Знания продуктов и сервисов.
- Способность донести требования до исполнителей.

plesk

Почему PM оказался ответственным за GDPR?

Согласованная работа нескольких команд:

Выполнение требований GDPR требует взаимодействия нескольких команд, организация чего является типичной задачей для PM.

Технические знания:

Необходимы знания имеющейся функциональности и использованных сервисов.

Изменения в продукте:

Для выполнения требований GDPR нужны доработки в продукте – это зона ответственности PM.

plesk

Определяем риски для бизнеса

- Оштрафуют евровласти?
    - Или не оштрафуют, но сломают все планы.
- Наедут "чёрные юристы"?
- Убегут клиенты?
- Убегут партнёры?

plesk

Диагностируем основные проблемы

В зависимости от идентифицированных рисков.

Например (для онлайн-проекта):

- Грубые нарушения основных принципов GDPR.
- Нарушения, которые легко обнаружить, особенно автоматизированным сканированием.

PS: Отсутствие "бумажной" подготовки тоже может быть основной проблемой (например, отсутствие Data Protection Agreement).

plesk

В конце концов

- Решаем проблемы в порядке приоритета.
- Параллельно оформляем бумаги.
- Когда готовы – тогда готовы. Сертификата не требуется.

plesk

Ключевые положения GDPR

plesk

Что считается персональными данными в GDPR

В GDPR персональными данными объявляется не только информация, прямо идентифицирующая или позволяющая идентифицировать физическое лицо, но и та информация, которая, в совокупности с другой имеющейся или доступной информацией, с разумной вероятностью может быть использована для идентификации физического лица.

plesk

Границы GDPR

- GDPR применяется к обработке персональных данных, осуществляемой организациями, действующими в ЕС.
- Это также относится к организациям за пределами ЕС, которые предлагают товары или услуги частным лицам в ЕС / гражданам ЕС (независимо от того, требуется ли оплата).
- Это также относится к организациям за пределами ЕС, которые отслеживают поведение, происходящее в границах ЕС.

plesk

Исключение

GDPR не распространяется на обработку персональных данных физическим лицом в ходе чисто личной или бытовой деятельности и, следовательно, без связи с профессиональной или коммерческой деятельностью.

Однако GDPR применяется к контроллерам или процессорам, которые предоставляют средства для обработки персональных данных для такой личной или бытовой деятельности.

plesk

“Контроллер” и “процессор”

GDPR применяется как к “контроллерам”, так и к “процессорам” – контроллер указывает, как и почему обрабатываются персональные данные, и процессор действует от имени контроллера.

plesk

Минимизация данных

- Независимо от законного основания.
- Не только по количеству, но и по времени хранения.
- И по количеству имеющих доступ сотрудников тоже.

plesk

Законное основание

- Для каждого кусочка персональных данных и каждой конкретной цели обработки.
- Должно быть определено изначально.
- Это не бумажный вопрос - от этого зависит функциональность.

plesk

Законные основания

plesk

6 возможных законных оснований

1. Согласие (consent)
2. Контракт
3. Требование закона
4. Жизненные интересы физических лиц
5. Общественные интересы
6. Законные интересы контроллера (т.е. ваши)

plesk

Согласие (consent)

- Намного сложнее, чем мы привыкли.
- Не во всех случаях разрешено.
- Имеет свои минусы.

plesk

Согласие должно быть (1/3)

- Выделенным: запросы на согласие должны быть отделены от других условий. Согласие не должно быть предварительным условием регистрации на услугу, если это не требуется для этой услуги.
- Активным: предварительно отмеченные флажки ввода недействительны – используйте не отмеченные флажковые поля или аналогичные активные методы выбора (например, выбор двух равнозначных вариантов).

plesk

Согласие должно быть (2/3)

- Гранулярно: раздельные запросы для отдельного согласования для разных типов обработки, где это необходимо.
- Персонифицировано: назовите свою организацию и любые третьи стороны, которые будут полагаться на согласие. Даже четко определенные категории сторонних организаций не будут приемлемыми в рамках GDPR.
- Документировано: ведите учет, чтобы продемонстрировать, на что согласился человек, включая то, что им сказали, и когда и как они согласились.

plesk

Согласие должно быть (3/3)

- Легко отозвать: сообщите людям, что они имеют право отозвать свое согласие в любое время, и как это сделать. Должно быть так же легко отозвать, как и дать согласие. Это означает, что вам понадобятся простые и эффективные механизмы отзыва.
- Без дисбаланса в отношениях: согласие не будет дано свободно, если есть дисбаланс в отношениях между физическим лицом и контролером – это сделает согласие особенно трудным для государственных органов и для работодателей, которые должны искать альтернативную законную основу.

plesk

Согласие, полученное до GDPR

- Согласие, полученное до вступления в силу GDPR, может продолжать использоваться только если оно было получено совместимым с GDPR образом:
    - Активно (opt-in).
    - Отдельно от других условий.
    - На ограниченный набор данных с указанием целей обработки.
    - Без дисбаланса в отношениях.
- А нет – нет. И персональные данные удалить.

plesk

Контракт

- Покрывает только данные, необходимые для исполнения контракта.
- Это законное основание ограничено временем действия контракта.

plesk

Требование закона

- Главное - не спутать закон с чем-то другим.
- Что будет при конфликте законов?..

plesk

Законные интересы контроллера (т.е. ваши)

Вы можете обрабатывать личные данные без согласия владельца персональных данных, если у вас есть подлинная и законная причина (включая коммерческую выгоду), если только это не перевешивает вред правам и интересам личности.

plesk

Воплощаем основные принципы GDPR

plesk

Шаги к соответствию

- Идентифицируем персональные данные в наших продуктах и сервисах.
- Избавляемся от лишнего.
- Идентифицируем свою роль и проверяем контрагентов.
- Подводим законные основания под оставшиеся данные и цели обработки.
- В процессе – маскируемся, т.е. устраняем легко обнаруживаемые нарушения.

plesk

Устранение легко обнаруживаемых нарушений

Что легко обнаружить (в том числе автоматически), например, в онлайн-проектах:

- Отслеживание поведения без согласия.
- Неправильную форму согласия.
- Согласие по умолчанию.
- Запрос лишних персональных данных (например, слишком много обязательных полей с персональными данными в формах).

plesk

Полезные ссылки

- GDPR как оружие массового поражения
- GDPR на носу – прекращаем панику и начинаем спасаться
- Почему не нужно всегда получать согласие на обработку персональных данных в рамках GDPR
- General Data Protection Regulation (GDPR)
  - Document (PDF)
- Overview of the GDPR by UK ICO
- ICO's GDPR Consent Guidance (draft)

plesk