



GREAT CREW

ГИД ПО НОВОМУ РЕГЛАМЕНТУ ПО ЗАЩИТЕ ДАННЫХ

10 пунктов, которые нужно знать для GDPR-friendly кампаний

Регламент GDPR — Общий регламент по защите данных — постановление Европейского союза для усиления защиты персональных данных всех лиц Европейского союза.

Для кого: для всех компаний, которые осуществляют сбор или хранение данных лиц Европейского союза (даже если физически не находятся в Европе)

[Полный текст регламента.](#)

Постановление вступает в силу 25 мая 2018 года, напрямую влияет на все действия компаний связанных с сбором данных. За невыполнение нового регламента штраф может достигнуть 20 000 000 евро или 4% финансового оборота компании за предыдущий год.

В законе расширено понятие персональных данных, установлено «право на забвение», введена роль офицера безопасности.

Мы решили разобраться в новом законе, и у нас получился гид, следуя которому, вы приведете свою компанию к новому регламенту.

Глоссарий:

Персональные данные (ПД): любая определяющая информация, относящаяся к физическому лицу: имя, фамилия, возраст, пол, e-mail, номер телефона, псевдоним, адрес IP, семейное положение, банковские данные, геолокация, данные навигации.

! Рабочий e-mail также попадает в эту категорию.

! Cookies с 25 мая 2018 года будут считаться персональными данными.

Сбор персональных данных: действие получения персональных данных, вне зависимости от метода сбора, цели и источника.

! Покупка e-mail баз также является сбором персональных данных.

Обработка персональных данных: любые операции с данными: сбор, хранение, организация, архивация, передача другим лицам, адаптация, модификация, уничтожение и др.

! Просто хранение персональных данных тоже является их обработкой.

Sensitive data: персональные данные раскрывающие расовую и этническую принадлежность, политические предпочтения, религиозные убеждения, генетические данные, сексуальную ориентацию.

! Сбор и обработка таких данных строго запрещена, за исключением легального разрешения.

Ответственный за обработку: сторона, которая определяет цели «зачем» и методы «как» в сборе и обработке данных.

Подрядчик: сторона, которая обрабатывает данные для ответственного за обработку и следуя его инструкциям. Может одновременно им и являться.

DPO (офицер безопасности): Референтное лицо, назначенное компанией, которое отвечает за соблюдение постановления. Может быть внутренним сотрудником и внешним подрядчиком.

Сбор данных во время маркетинговых кампаний

Пункт 1:

Как составить обязательную Политику Конфиденциальности

Постановление GDPR в целом выступает за активную коммуникацию прав пользователю. Вам нужно опубликовать или обновить Политику конфиденциальности на онлайн и офлайн интерфейсах.

В обновленной политике должны быть следующие пункты:

- Кто является ответственным за обработку данных;
- Кто является DPO;
- Зачем собираются данные;
- Кому данные отправляются (даже если данные отправляются вне Европейского союза);
- Период обработки и хранения данных;
- Перечисление пользовательских прав (право доступа, исправления, уничтожения, лимитирования и др.);
- Контакт, куда можно обратиться за активацией этих прав;
- Обращение за помощью в нужные инстанции.

Политика Конфиденциальности должна быть предоставлена пользователю в момент сбора данных отдельно от бланка заполнения. Она должна быть объяснена доступным и понятным языком. Можно создавать несколько политик конфиденциальности для разных маркетинговых кампаний, можно создать одну, и ссылаться на нее.

Пункт 2:

Как собирать соглашения при проведении маркетинговой кампании?

Соглашение — большой и важный пункт в новом постановлении. Это именно тот момент, ради которого мы запускаем маркетинг активности и пользователь нажимает «Да, я хочу получать информацию от вашей компании».

Так вот, согласно новому постановлению, соглашение должно быть абсолютно понятным пользователю. Оно также должно быть представлено отдельно от любых других требований.

Внимание: GDPR запрещает соглашение с уже поставленными галочками. Отсутствие активности пользователя или молчание НЕ может быть принято за соглашение.

Пункт 3:

Как составить корректную форму запроса данных?

Идеальный бланк:

- Запрашивает только необходимые данные для цели именно этой кампании.
- Запрашивает отдельные согласие на все планируемые действия (отправка рассылки, использование данных для профайлинга, коммуникация с пользователем)
- Запрашивает согласие на правила конкурса или маркетинговой операции
- Запрашивает принятие политики конфиденциальности

После сбора данных, вы должны:

- удостовериться в их правильности, и удалить некорректные данные
- обеспечить их безопасное и конфиденциальное хранение
- хранить их только определенный период времени.

При контроле вы будете обязаны показать, что эти принципы соблюдаются.

Распространение маркетинговых операций

Пункт 4:

Как быть со списком имейлов, которые уже есть в вашей базе?

Помните, что пользователь может в любой момент забрать свое соглашение.

Вы также в любой момент должны показать пользователю доказательство, что согласие было дано.

На каждого пользователя у вас должна быть полная информация:

- Дата и время согласия
- Способ сбора данных
- Какая информация была коммуницирована пользователю
- Какие виды согласия пользователь принял, какие — нет
- Бланк сбора данных
- Способ коммуникации (e-mail, социальная сеть, другое)

Многие платформы, например Mailchimp, уже предлагают [GDPR-friendly формы](#). Используйте их.

Пункт 5: Как квалифицировать базу?

GDPR распространяется не только на новые данные, которые вы собираете, но и на те, которые вы уже имеете.

Как провести полную квалификацию вашей базы:

1. Сделайте полный список всех ваших opt-in, со всех кампаний.
2. Проверьте, вся ли информация у вас есть на каждый opt-in. Разделите на «подтверждены» и «не подтверждены».
3. Подтверждены: автоматизируйте процесс. По истечению определенного срока высылайте автоматическое письмо с просьбой обновить согласие. Если обновления не последовало: контакт удаляется.
4. Не подтверждены: отправьте письмо (вы наверняка уже получаете такие письма) с просьбой подтвердить согласие. Если согласия не получено до 25 мая, вы должны удалить контакт из рассылки.

Пункт 6: Как квалифицировать рассылку?

1. Если вы покупаете базы данных у третьих лиц, вы должны удостовериться что подрядчик соблюдает постановление, и пользователи дали свое согласие.
2. Если ваша база собирается через онлайн и офлайн интерфейсы, точно также, пользователи должны дать свое согласие.
3. В вашем письме обязательно должна быть ссылка на отписку от рассылки.
4. Вы должны прокоммуницировать контактное лицо для активации прав.
5. И, наконец, все правила и принципы применяются также к рабочим e-mail-ам.

Пост-кампания

Пункт 7:

Как долго хранить данные?

Вы должны определить период хранения данных для осуществления целей маркетинговых кампаний.

Например: данные банковской карты должны храниться только для проведения оплаты, и затем должны быть удалены.

Контакты клиента или потенциального клиента, который не проявляет никакой активности, и не отвечает должны быть удалены по истечению 3-ех лет.

Cookies — хранятся максимум 13 месяцев.

Пункт 8:

Что делать с подрядчиками?

Впервые, новое постановление призывает к ответственности подрядчиков и третьих лиц.

- Подрядчик не может нанять другого подрядчика без письменного согласия клиента (ответственного за обработку)
- Любая обработка данных подрядчиком должны быть оформлена контрактом
- Подрядчик должен предоставить гарантии, что данные собираются и хранятся конфиденциально и безопасно — согласно постановлению GDPR — уже с 25 мая.
- Подрядчик должен обозначить DPO и вести регистр.

Даже если ваш подрядчик находится не в Европе, он подвергается новому постановлению, так как обрабатывает данные лиц Европейского союза.

Пункт 9:

Как организовать cookies?

Как мы уже говорили, согласно GDPR, cookies являются персональными данными.

- Подразумеваемого согласия больше не достаточно. Обязательно запросить его через действие.
- Забрать свое согласие должно быть также легко, как его дать.
- Предупреждение на сайте должно содержать информацию о том, что cookies — это персональные данные.
- Нужно предоставить опцию отмены

Пункт 10:

Как соблюдать права пользователя?

GDPR ввело новые права пользователя:

- Право доступа. Позволяет клиенту узнать, какую информацию о нем хранит компания.
- Право портативности. Клиент имеет право при запросе получить эту информацию в корректном, читабельном виде, чтобы далее ее использовать по собственному усмотрению. При этом вы можете продолжать их хранить до истечения «срока годности» данных.
- Право на забвение. Позволяет клиенту запросить полное уничтожение всех персональных данных, связанных с ним.
- Право на оппозицию. Позволяет клиенту больше не получать никаких писем ни от вашей компании, ни от ваших партнеров.

Как правильно управлять правами:

1. Завести регламент, адаптировать ваш сайт, добавив информацию о правах.
2. Выбрать сотрудника, который будет ответственен за получение запросов от клиентов. Создать ему отдельный e-mail и бланк запроса на сайте.
3. Коммуницировать этот контакт везде, онлайн и офлайн.
4. Обрабатывать запросы от клиентов как можно быстрее.

Новый закон давно занимает маркетологов европейских компании, а мы уверены в том, что он окажет только позитивное влияние. Тренд на прозрачность информации, новые права пользователя, новый процесс соглашения, все это — новая эра маркетинга.

GDPR поставил точку эре массовых рассылок, бесконечному спаму, ненужным новостям и надоевшей рекламе.

Качество победит количество, и маркетинговые коммуникации станут еще более точными и нацеленными на персональное и доверительное общение с клиентом.

Ваши маркетинговые кампании должны предлагать только то, что действительно интересно клиенту, а ваши рассылки клиент должен ждать и открывать с нетерпением.

Как именно этого добиться? Контентом, который адаптирован под нужды и интересы клиента, клиент-ориентированными маркетинговыми кампаниями и последними знаниями в поведенческой экономике и нейромаркетинге.

Обязательно пишите нам, если у вас есть вопросы или комментарии.