IAB RUSSIA
РАБОЧАЯ ГРУППА ПО GDPR КОМИТЕТА ПО BIG DATA
GDPR WHITE PAPER 2018

Сопредседатели комитета:
Александр Логачев, Директор по разработке рекламных и аудиторных технологий Rambler&Co.
Любовь Пшеничникова, Заместитель управляющего директора Weborama в Восточной Европе и Центральной Азии.
Руководитель проекта: Оксана Долженко, Руководитель направления по коммуникациям Weborama.

Активное участие принимали:
Юлия Селиверстова, Publicis Media
Алексей Шиховец, CleverData
Елена Ефремцева, Rambler&Co
Наталья Недоцук, Rambler&Co
Леся Савченко, Media Sniper
Станислав Кремнев, Sizmek

СОДЕРЖАНИЕ

ЗАКАЗЧИКИ ИССЛЕДОВАНИЯ

IAB Russia GDPR White Paper 2018 был подготовлен по инициативе Комитета по BIG DATA IAB Russia.

Мы выражаем благодарность компаниям-членам IAB Russia, которые оказали активную поддержку в подготовке документа.

Благодарим за участие в подготовке документа экспертов Рабочеи группы по GDPR Комитета по BID DATA IAB Russia, а также представителеи компании, не входящих в состав Комитета, и, в частности, Александра Логачева (Rambler&Co), Любовь Пшеничникову (Weborama), Оксану Долженко (Weborama), Юлию Селиверстову (Publicis Media), Алексея Шиховец (CleverData), Елену Ефремцеву (Rambler&Co), Наталью Недоцук (Rambler&Co), Лесю Савченко (Media Sniper), Станислава Кремнева (Sizmek).

GDPR: ОСНОВНЫЕ ВОПРОСЫ И РЕАЛЬНЫЕ ДЕЙСТВИЯ

ОБЩЕЕ

25 мая 2018 г. в Евросоюзе вступил в силу новый регламент по защите данных – GDPR (General Data Protection Regulation) или Регламент ЕС 2016/679 от 27 апреля 2016 г. Данный регламент, имеющий прямое действие во всех 28 странах ЕС, заменит рамочную Директиву о защите персональных данных 95/46/ЕС от 24 октября 1995 года.

Документ является экстерриториальным и касается защиты персональных данных (ПД) как граждан стран Европейского союза, так и граждан других стран, чьи данные обрабатываются на территории ЕС, а также в определенных случаях – за ее пределами. Российская Федерация не входит в ЕС, и законодательство ЕС (в частности действие GDPR) не распространяется на территорию РФ. Однако дочерние структуры российских организаций, работающие в ЕС, попадают под действие GDPR напрямую, тогда как в отношении организаций, расположенных за пределами территории ЕС и обрабатывающих данные европейцев, влияние нового законодательства косвенное – через деловых партнеров в ЕС, которые будут вынуждены учитывать риски сотрудничества с организациями, расположенными за пределами Евросоюза, с учетом возможных штрафов GDPR.

Штрафы за несоблюдение Регламента существенные:

- За «незначительные» нарушения – до 10 миллионов евро или 2% от мирового годового оборота (большая из сумм);
- За «серьезные» нарушения (в частности несоблюдение принципов защиты данных) – до 20 миллионов евро или 4% от мирового годового оборота (большая из сумм).

Важно отметить, что Регламент оказывает влияние не только здесь и сейчас, но в целом ознаменовал начало перехода к более транспарентному и жесткому отношению к работе с ПД во всем мире. К примеру, в Калифорнии был принят California's consumer Privacy Act (CCPA), а в правоприменительной практике РФ к ПД могут относить как привычные идентификаторы, так и аналитические – идентификатор устройства, ip-адрес, файлы cookie.

Таким образом, уже сейчас GDPR может затрагивать организации, работающие в РФ, что было признано Роскомнадзором, а в будущем изменение российского законодательства по ПД может быть реализовано по сценарию GDPR.

Как следствие, российским и международным компаниям, которые работают в РФ и которые обрабатывают данные, необходимо понимать общую логику Регламента, его требования, условия и критерии применимости, шаги для соответствия, а также иметь возможность оценить, что делают крупнейшие игроки рынка и какую позицию занимают. В документе мы стараемся ответить на все эти пункты.

1. ОСНОВНЫЕ ВОПРОСЫ, КАСАЮЩИЕСЯ РЕГЛАМЕНТА

Позиция Роскомнадзора[1]

В ноябре 2017 года на VIII Международной конференции «Защита персональных данных» руководитель Роскомнадзора Александр Жаров отметил, что требования Регламента Европейского союза по защите персональных данных не будут распространяться на российских операторов, осуществляющих деятельность на территории России, поскольку Российская Федерация не является участницей международных договоров с ЕС. На российских операторов распространяется действие только российских законов в этой сфере в соответствии с общепринятыми международными принципами обработки персональных данных.

Однако на дне открытых дверей 31.07.2018 г. представители Роскомнадзора озвучили обновленную позицию в отношении применения требований GDPR к российским компаниям, в частности Роскомнадзором были рекомендованы:

- критерии определения применимости GDPR;
- проведение аудита обработки персональных данных, в том числе на предмет соответствия требований GDPR;
- обеспечение оператором прав субъектов – право на забвение и право на перенос данных.

Соответственно, можно сделать вывод, что на настоящий момент Роскомнадзор допускает применение требований GDPR к российским компаниям в определенных случаях.

Что такое персональные данные[2]

м«Персональные данные» (personal data) – означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо является лицом, которое может быть идентифицировано прямо или косвенно, в частности, на основе идентификационной информации, такой как имя, идентификационный номер, данные о местоположении, идентификатор в интернете (онлайн-идентификатор) или посредством одного или нескольких показателей, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности данного физического лица.

Физические лица могут быть связаны с онлайн-идентификаторами, предоставляемыми их устройствами, приложениями, инструментами и протоколами, такими как адреса интернет-протокола, идентификаторы файлов cookie или другие идентификаторы, такие как теги радиочастотной идентификации. Это может оставить следы, которые, в частности, в сочетании с уникальными идентификаторами и другой информацией, полученной серверами, могут использоваться для создания профилей физических лиц и их идентификации.

1 Указанная позиция отражена в презентации Роскомнадзора - https://rkn.gov.ru/docs/GDPR_Pankov.pdf

2 Статья 4

Таким образом, в категорию персональных данных точно попадают:

- ФИО;
- Телефонный номер;
- E-mail;
- MAC-адрес;
- social ID;
- IP-адрес;
- Данные о местоположении;
- Device ID;
- Cookie;

Кто попадает под действия GDPR[3]

Обработка ПД Попадает под действие Регламента в следующих случаях:

1. если контроллер или процессор ПД учрежден в ЕС, вне зависимости от того проходит ли сам процесс обработки на территории ЕС;
2. субъект ПД находится в ЕС, а контроллер или процессор учреждены не в ЕС, если деятельность по обработке связана со следующим:

- предложение продуктов и услуг, вне зависимости от необходимости оплаты (возмездная и безвозмездная основы), субъектам в ЕС.

К примеру, использование доступного в ЕС веб-сайта на языке страны – члена ЕС или валюты страны – члена ЕС для предоставления товаров или сервисов.

- мониторинг поведения субъектов на территории ЕС

Профилирование субъекта персональных данных, к примеру, для принятия решения в отношении субъекта или для анализа, прогноза личных предпочтений субъекта, поведения и взглядов.

3 Статья 3

3. контроллер учрежден не в ЕС, но в том месте, где применяется законодательство государств-членов в силу международного публичного права.

Косвенные условия для применения GDPR:

- услуги/товары адаптированы на местные языки жителей ЕС;
- услуги/товары могут быть оплачены в местных валютах ЕС;
- услуги/товары предоставляются на национальных доменах верхнего уровня стран ЕС.

Для оценки вероятности попадания под действия регламента стоит ответить на вопросы ниже:

1. У вас есть аффилированное юридическое лицо (или иная форма присутствия) на территории ЕС?
2. Реализуете ли вы товары или предоставляете услуги на территории ЕС (например, осуществляете доставку товаров из РФ в ЕС)?
3. Принимаете ли вы оплату ваших товаров или услуг в евро или других валютах стран ЕС?
4. Доступна ли версия вашего корпоративного сайта на одном из европейских языков (немецком, французском, чешском и т. д.) и осуществляете ли вы сбор персональных данных на сайте (ведется ли регистрация пользователей, используются ли формы для предоставления обратной связи, проводится ли сбор и обработка анкетных данных, сведений о местонахождении, а также персональной информации о пользователях сети интернет посредством cookies и т. п.).?
5. Доступна ли версия вашего корпоративного сайта на одном из европейских языков (немецком, французском, чешском и т. д.) и осуществляете ли вы сбор статистических данных о посещаемости вашего сайта?

Если вы ответили положительно на один из вопросов выше, есть вероятность, что GDPR вас касается и вам требуется соблюдать нормы регламента. Тем не менее каждый случай индивидуален. Относится ли новый регламент к компании и рискует ли она оказаться под санкциями за его несоблюдение, необходимо оценивать отдельно в каждом конкретном случае.

Определение контроллера и процессора[4]

Регламент разделяет организации, работающие с данными, на две категории: контроллер (он же оператор) и процессор (он же обработчик).

«Контроллер» означает физическое или юридическое лицо, государственную власть, агентство или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных; где цели и средства такой обработки определяются законодательством Союза или государства-члена, контролер или конкретные критерии для его выдвижения могут быть предусмотрены законодательством Союза или государства-члена.

«Процессор» означает физическое или юридическое лицо, государственный орган, агентство или другой орган, который обрабатывает личные данные от имени контроллера.

Таким образом, контроллер определяет цели и средства обработки персональных данных, тогда как процессор технически осуществляет сбор и обработку данных в интересах контроллера и согласно обозначенным контроллером целям. При этом бизнес может выступать и контроллером и процессором в разных случаях. К примеру, технологический вендор, обрабатывая данные клиентов, выступает в качестве процессора, тогда как при работе с собственной базой данных – в качестве контроллера.

4. Статья 4

Какие основания для законной работы с данными[5]

Регламент определяет 6 законных оснований[6] для работы с данными.

Обработка должна быть законной только в том случае, если и в той мере, в которой применяется хотя бы одно из следующего:

- субъект данных дал согласие **(consent)** на обработку своих персональных данных для одной или нескольких конкретных целей;
- обработка необходима для выполнения контракта, стороной которого является субъект данных, или для принятия мер по запросу субъекта данных до заключения договора;
- обработка необходима для соблюдения юридического обязательства, которому подвержен контроль;
- обработка необходима для защиты жизненно важных интересов субъекта данных или другого физического лица;
- обработка необходима для выполнения задачи, выполняемой в общественных интересах или при осуществлении официальных полномочий, возложенных на контроллера;
- обработка необходима для целей законных интересов **(legitimate interest)**, осуществляемых контроллером или третьей стороной, за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта данных, которые требуют защиты персональных данных, в частности, когда данные субъект – ребенок.

Для работы с данными в рамках диджитал экосистемы главным образом подходят два основания: согласие (consent) и законный интерес (legitimate interest).

5. Статья 6

6. 6 принципов обработки персональных данных:
Lawfulness, fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality

Согласие: основные параметры[7]

«Согласие» субъекта данных означает любое свободно заданное, конкретное, информированное и однозначное указание желаний субъекта данных, с помощью которого он или она, посредством заявления или чётким, утвердительным действием, даёт согласие на обработку персональных данных, относящихся к нему или к ней.

Согласие должно быть дано четким утвердительным актом, устанавливающим свободно предоставленное, конкретное, информированное и однозначное указание согласия субъекта данных на обработку персональных данных, касающихся его или ее, например, письменным заявлением, в том числе с помощью электронных средств, или устное заявление. Таким образом молчание пользователя либо ранее поставленная отметка при посещении сайта, либо бездействие не рассматриваются в качестве согласия.

Согласие должно охватывать все виды обработки, осуществляемые в тех же целях или целях, когда обработка имеет несколько целей, необходимо дать согласие на все из них. Если согласие субъекта данных должно быть предоставлено по запросу с помощью электронных средств, запрос должен быть четким, кратким и необоснованно нарушать использование услуги, для которой он предоставлен.[8]

Если обработка основана на согласии, контроллер должен иметь возможность продемонстрировать, что субъект данных согласился на обработку его личных данных:

- Если согласие субъекта данных дается в контексте письменного заявления, которое также касается других вопросов, просьба о согласии должна быть представлена способом, который четко отличается от других вопросов, в понятной и легкодоступной форме, используя ясный и простой язык. Любая часть такой декларации, которая представляет собой нарушение настоящих Правил, не является обязательной;
- Субъект данных имеет право отозвать свое согласие в любое время. Отзыв согласия не влияет на законность обработки на основании согласия до его отзыва. Перед дачей согласия об этом сообщается субъекту данных. При этом отозвать согласие должно быть также легко, как и дать согласие;
- При оценке того, предоставляется ли согласие свободно, следует, в частности, учитывать связаны ли выполнение контракта/предоставление услуги с предоставлением согласия на обработку персональных данных, которые не нужны для выполнения этого контракта/оказания услуги.

Таким образом, ключевые моменты по согласию:

- Свободное, конкретное, информированное, непротиворечивое;
- Форма согласия и отзыва: заявление или утвердительное действие;
- Простой и понятный язык;
- Отдельное от каких-либо других вопросов;
- Отдельное согласие для каждой цели обработки;
- Родительское согласие на обработку данных детей до 16 лет для получения онлайн услуг;
- Отозвать также просто, как и получить;
- Контроллер должен доказать получение согласия.

Legitimate interest: условия для выбора как законного основания

Законные интересы контроллера, в том числе контроллера, которому могут быть раскрыты личные данные, или третьей стороны, могут обеспечивать правовую основу для обработки **при условии, что интересы или основные права**

7 Статья 4 и 7
8 Комментарий 32

и свободы субъекта данных не нарушаются, принимая во внимание разумные ожидания субъектов данных, основанные на их связи с контроллером.

Такой законный интерес может существовать, например, в тех случаях, когда существует соответствующая связь между субъектом данных и контроллером в тех ситуациях, когда объект данных является клиентом контроллера или состоит на службе у контроллера.

Во всяком случае, **наличие законного интереса потребует тщательной оценки,** включая вопрос о том, может ли субъект данных разумно ожидать (в то время и в контексте сбора персональных данных), что имеет место обработка данных. Интересы и основные права субъекта данных могут «перевешивать» интерес контроллера данных в случаях, когда обрабатываются персональные данные, когда субъекты данных не ожидают дальнейшей обработки.

Учитывая, что законодатель должен законодательно предусмотреть правовую основу для государственных органов для обработки персональных данных, эта правовая основа не должна применяться к обработке государственными органами при выполнении своих задач. Обработка персональных данных, строго необходимая для предотвращения мошенничества, также представляет собой законный интерес соответствующего контроллера данных.

Обработка персональных данных **для целей прямого маркетинга может рассматриваться как выполненная для законных интересов.** (Комментарий 47)

Таким образом, при выборе legitimate interest в качестве законного основания необходимо провести оценку возможности выбора бизнесом данного основания, в частности описав гарантии соблюдения основных прав и свобод субъектов данных и объяснив, в чем заключается законный интерес бизнеса для обработки персональных данных.

Общая последовательность действий для соответствия Регламенту

- Установите, есть ли вероятность, что Регламент вас касается. В качестве проверки ответьте на вопросы для проверки (выше);
- Если есть вероятность, что ваша компания Попадает под действие Регламента, то необходимо выполнить ряд действий;

1. Провести аудит дата-активов: какие данные собираются, как данные собираются, как/где/сколько данные хранятся, кто является интересантом работы с данными, есть ли система оповещения пользователей о целях сбора и обработки данных, а также об утечках данных. По результатам аудита необходимо определить два ключевых пункта для организации:

- Какое законное основание компания может выбрать для работы с данными. Как правило, для работы с данными в диджитал-экосистеме подходят согласие (consent) или законный интерес (legitimate interest). Согласие предполагает необходимость сбора и хранения согласий пользователей для работы с их персональными данными, тогда как законный интерес позволяет, при условии ненарушения интересов или основных прав и свобод субъекта данных и обосновании законного интереса бизнеса для работы с данными, не собирать согласия для работы с персональными данными пользователей.
- Кем является компания: контроллером (controller) или процессором (processor) контроллер определяет цели и средства обработки персональных данных, тогда как процессор технически осуществляет сбор и обработку данных в интересах контроллера и согласно обозначенным контроллером целям.

Ответы на два пункта выше являются важными и предполагают несколько отличные действия от компаний. К примеру, при выборе согласия в качестве законного основания для работы с данными будет необходимо собирать и хранить согласия, при выборе законного интереса собирать и хранить согласия не нужно.

2. Провести оценку рисков нарушения конфиденциальности (Data Protection Impact Assessment – DPIA) для критичных процессов обработки персональных данных;
3. Назначить DPO (data protection officer), то есть ответственного за защиту данных;
4. Привести порядок работы организации с данными в соответствии с принципами «privacy by design» (проектируемая конфиденциальность) и «privacy by default» (конфиденциальность по умолчанию);
5. Вести реестр всех действий по работе с данными, то есть документировать деятельность по обработке данных;
6. Выработать механизм исполнения предусмотренных Регламентом прав пользователей;
7. Обеспечивать безопасность данных и извещать регулятора и граждан о проблемах с данными (уведомление об «утечках» данных);

В частности, контроллер/процессор должен уведомить регулятора в течение 72 часов с момента обнаружения фактов нарушений в обработке и защите персональных данных, а также информировать в разумные сроки субъекта ПДн об обнаружении нарушений;

8. Иметь возможность доказать соблюдение принципов работы с данными по Регламенту;
9. Провести аудит партнеров и клиентов с точки зрения использования данных, скорректировать договор на оказания услуг;
10. Опубликовать обновленную политику конфиденциальности (Privacy Policy) компании, а также информировать партнеров и клиентов о принятых/принимаемых мерах по соблюдению Регламента.

Что делать с данными, собранными до 25 мая: оставить или ликвидировать

В первую очередь необходимо определить, собраны ли данные с получением согласия пользователя (если компания выбрала именно это законное основание для работы с данными) или без согласия, а также установить, если сбор происходил с согласия пользователя, сохранены ли согласия пользователей. Если данные, собранные до 25 мая, собраны с получением согласия пользователя согласно GDPR, то контроллер может продолжить работать с данными. Если данные, собранные до 25 мая, собраны без получения согласия пользователя согласно GDPR, контроллеру необходимо принять решение оставить или удалить эти данные, а также уведомить о своем решении всех связанных с ним процессоров.

Важно отметить, что сбор согласий на сайте – зона ответственности владельца сайта, то есть бизнеса/бренда, выступающего контроллером и определяющего цели и пути сбора данных.

Для того, чтобы происходил сбор только тех пользователей, которые дали согласие согласно требованием GDPR, необходимо на уровне сайта бренда настроить вызов всех тегов аналитики и сбора аудитории в момент после получения согласия пользователя, тогда как при отсутствии согласия теги аналитики и сбора аудитории как контроллера, так и процессора/процессоров не вызывать. Форму для сбора согласий пользователей рекомендуется показывать перед загрузкой содержания страницы, чтобы пользовать сначала дал/не дал согласие на обработку данных, а уже после переходил к содержанию сайта.

Основные отличия требований GDPR и Закона РФ «О персональных данных» (далее – Закон о ПД):

1. Что относится к персональным данным

GDPR расширяет круг информации, относящейся к персональным данным, а именно - прямо относит к информации, определяющей физическое лицо, **онлайн идентификатор (online identifier)**, под которым понимаются ip-адрес,

cookie или иные идентификаторы, такие как метки радиочастотной идентификации.

Закон о ПД не предусматривает такого понятия как онлайн идентификатор и не упоминает/не относит прямо к персональным данным ip-адрес, cookie и иные подобные идентификаторы.

2. Новый субъект правоотношений

GDPR определяет **обработчика/процессора (processor)** в качестве самостоятельного субъекта правоотношений, связанных с обработкой персональных данных. Обработчиком является физическое или юридическое лицо, государственный орган, агентство или иной орган, который обрабатывает персональные данные от имени оператора/контроллера. GDPR устанавливает отдельные требования к процессору.

Закон о ПД не определяет указанного субъекта, но предусматривает в ч. 3 ст. 6 условия обработки персональных данных по поручению оператора, а также обязанности лица, осуществляющего обработку персональных данных по поручению оператора.

3. Уведомление контролирующего органа

Закон о ПД устанавливает обязанность оператора (оператор по обработке персональных данных) направить уведомление об обработке персональных данных в Роскомнадзор. GDPR отказался от требования об уведомлении уполномоченного органа.

4. Новая обязанность оператора по GDPR

GDPR устанавливает обязанность оператора обеспечить соблюдение 6 принципов[9], относящихся к обработке персональных данных и закрепленных в ст. 5(1), но также устанавливает новую обязанность оператора – **быть способным продемонстрировать выполнение им данного требования.**

Закон о ПД не устанавливает указанной обязанности оператора.

5. Требования к согласию на обработку персональных данных

GDPR устанавливает **более жесткие требования к согласию** субъекта персональных данных. В частности:

- при предоставлении согласия в рамках письменного заявления, относящегося к другим вопросам, запрос согласия должен быть в форме, позволяющей четко его отличить от других вопросов, в понятной и легкодоступной форме, с использованием ясного и простого языка;
- молчание пользователя либо ранее поставленная отметка при посещении сайта, либо бездействие не рассматриваются в качестве согласия;
- отозвать согласие должно быть настолько же просто, насколько предоставить его.

6. Права субъекта персональных данных

Помимо прочих, GDPR закрепляет следующие **права субъекта персональных данных, не предусмотренные Законом о ПД**, и обязанность оператора по их обеспечению:

- право на перенос данных (right to data portability), в соответствии с которым оператор обязан обеспечить осуществление права субъекта на передачу этих данных другому контроллеру (в случаях если обработка осуществляется с помощью автоматизированных средств), в том числе на получение субъектом своих персональных данных в структурированном, общепринятом и распознаваемом автоматизированными системами формате для последующей передачи другому контролеру (ст. 20).
- право на забвение (right to erasure or ‘right to be forgotten’), согласно которому оператор обязан обеспечить реализацию права субъекта на удаление его

9. 6 принципов обработки персональных данных: Lawfulness, fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality

персональных данных в случаях, предусмотренных ст. 17, в том числе, если:

1. персональные данные больше не необходимы для целей, для которых они были собраны или иным образом обработаны;
2. субъект данных отозвал свое согласие, на основании которого осуществлялась обработка/ возражает против обработки.

7. Privacy by design and default

Новые дополнительные требования, закрепленные GDPR – Privacy by design и Privacy by default, представляют собой комплекс обязательных требований, возложенных на оператора и включающих различные технические и организационные меры. Эти меры оператор обязан обеспечить в рамках общего режима защиты прав субъектов данных.

2. КТО ЧТО ДЕЛАЕТ В РОССИИ В ОТНОШЕНИИ РЕГЛАМЕНТА

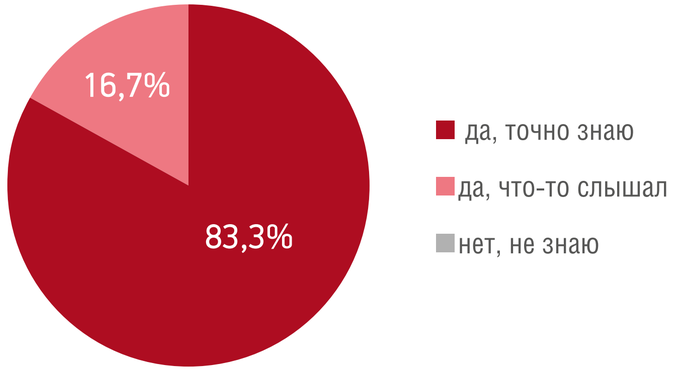
В связи с тем, что, с одной стороны Регламент европейский, а с другой – экстерриториальный, границы его применения могут быть не до конца ясны игрокам российского рынка. Для того, чтобы у игроков был ориентир, во второй части документа сделан обзор принятых мер для соответствия Регламенту российскими и международными компаниями, работающими на российском рекламном рынке. Ниже представлены позиции и действия 4 групп компаний: рекламодателей, паблишеров, рекламных агентств и технологических вендоров.

Рекламодатели

Ниже представлены результаты опроса рекламодателей, проведенного при поддержке IAB Russia в период с июня по сентябрь 2018 года.

Ответы показывают уровень осведомленности брендов о Регламенте и меры, которые были приняты для соответствия GDPR.

1. Знаете ли Вы о том, что 25 мая этого года вступил в силу Регламент Европейского Союза по защите персональных данных GDPR (General Data Protection Regulation)?



Абсолютное большинство, 83,3% опрошенных, рекламодателей знают о существовании Регламента Европейского Союза

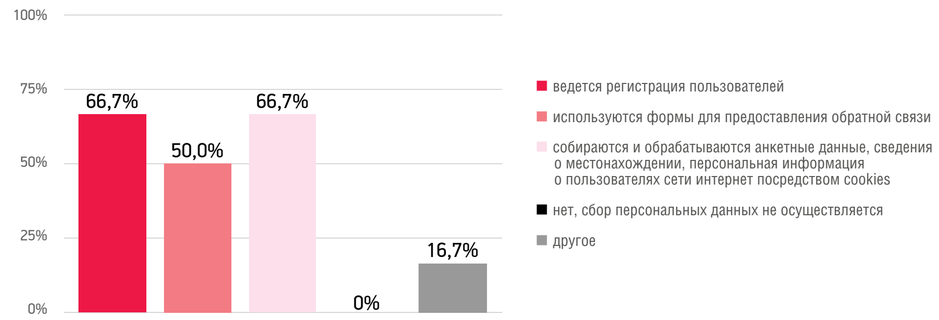
2. Затрагивает ли Вашу компанию или бренд введение Регламента GDPR?

Дополнительные вопросы для определения возможности быть затронутым Регламентом:

- Есть ли у Вашей компании / бренда аффилированное юридическое лицо (или иная форма присутствия) на территории Европейского союза (ЕС)? - НЕТ для 83,3% респондентов, ДА - 16,7%
- Реализуете ли Вы товары или предоставляете услуги на территории ЕС (например, осуществляете доставку товаров из РФ в ЕС)? - НЕТ для 100% респондентов
- Принимаете ли Вы оплату товаров или услуг в евро или других валютах стран ЕС? - НЕТ для 100% респондентов
- Принимаете ли Вы оплату товаров или услуг в евро или других валютах стран ЕС? - НЕТ для 100% респондентов
- Осуществляете ли Вы сбор статистических данных о посещаемости Вашего сайта? - ДА для 100% респондентов
- Осуществляет ли Ваша компания сбор персональных данных посетителей на корпоративном сайте - ДА для 100% респондентов

3. Осуществляет ли Ваша компания сбор персональных данных посетителей на корпоративном сайте?

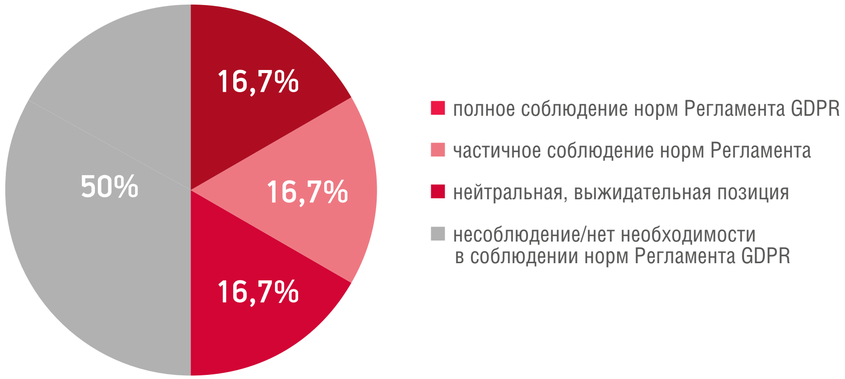
Согласно ответам, все компании собирают данные посетителей своего сайта. Наиболее распространенные способ сбора ПД: посредством cookies и с помощью формы регистрации на сайте - 66,70%.



Помимо перечисленных ответов, данные также могут собираться в Личном кабинете на сайте рекламодателя.

4. Какую позицию занимает Ваша компания / бренд по отношению к Регламенту GDPR?

50% опрошенных рекламодателей считают, что могут не соблюдать Регламент, так как нет необходимости в соблюдении его норм. Остальные ответы: полное соблюдение, частичное и нейтральная позиция разделились в равных долях.

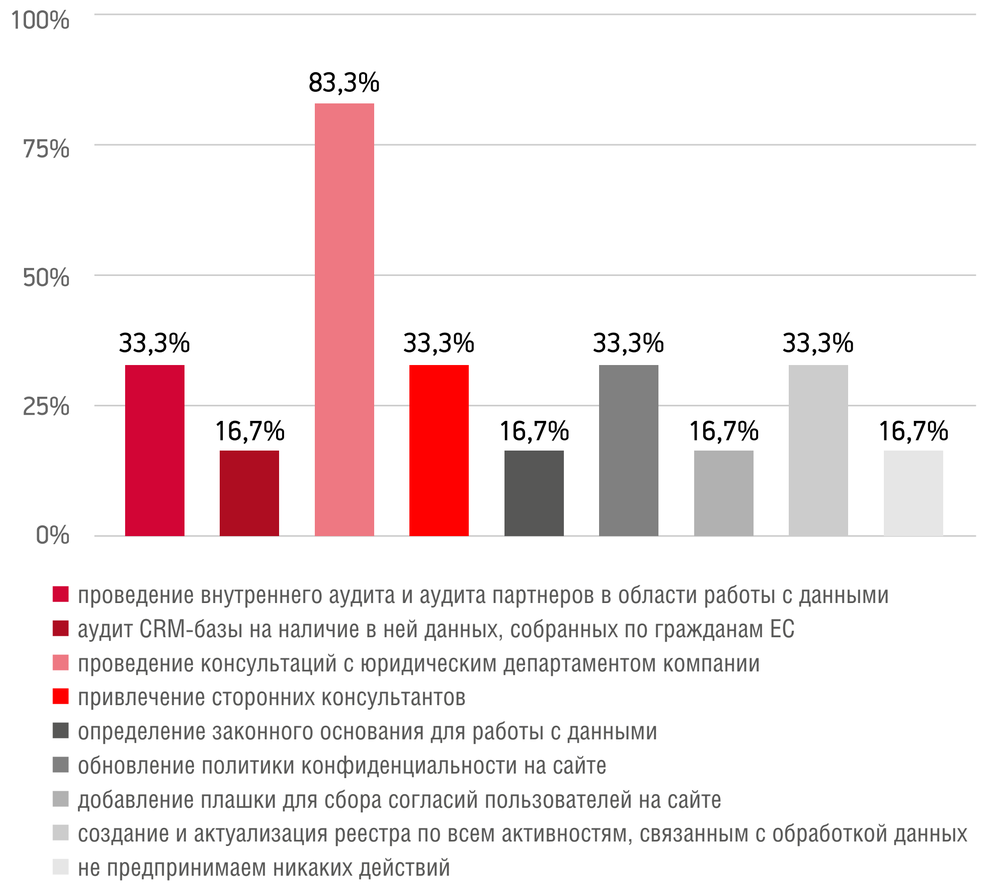


4. Почему у Вашей компании/бренда именно такая позиция?

Типовые ответы:

- Выжидательная позиция - напрямую на бизнес пока нет влияния.
- Полное соблюдение норм Регламента GDPR - так как наша компания уважает право пользователей выбирать, с кем и в каком объеме делиться своими персональными данными
- Частичное соблюдение норм Регламента GDPR - сейчас мы работаем над анализом рисков и обновлением процедуры сбора пользовательских данных таким образом, чтобы исключить работу с данными, собранными на территории Евросоюза. Также мы сообщаем глобальному офису текущий статус соответствия GDPR.
- Несоблюдение норм Регламента GDPR - не применяется по отношению к деятельности нашей компании. Поскольку наши российские юридические лица не ведут деятельность на территории, которую затрагивают юридические акты Евросоюза, мы считаем, что эти акты не имеют влияния на наши бренды. Мы ведём свою деятельность в соответствии с законодательством Российской Федерации
- Компания является Российской организацией и оказывает услуги только гражданам РФ, а также есть предупреждение на сайте, что компания руководствуется нормами российского законодательства.

5. Какие действия уже предприняты в Вашей компании для соответствия Регламенту GDPR?



83,3% опрошенных респондентов отметили, что провели консультации с юридическим департаментом компании по вопросам соответствия Регламенту. Также бренды в равной степени отметили, что обращаются за помощью к сторонним консультантам, обновляют политику конфиденциальности на сайте и выделяют ресурсы на проведение внутреннего аудита и аудита партнеров в области работы с данными, – 33,3% от всех опрошенных. Наименее популярные ответы – аудит CRM – базы на наличие в ней данных, собранных по гражданам ЕС, определение законного основания для работы с данными. Про назначение DPO (Data Protection Officer) не упомянули ни один из респондентов.

6. Какие изменения в рабочие процессы пришлось внести Вашей компании в связи с новыми правилами GDPR?

В осном рекламодатели не предпринимают никаких мер по соответствию регламенту, только 10% из всех опрошенных ответили, что была создана рабочая группа GDPR и начата корректировка процедур сбора пользовательских данных с сайтов (при условии соблюдения Регламента).

7. Столкнулись ли Вы с какими-то ограничениями на использование данных в рекламе, аналитике, передаче данных Ваших партнеров после вступления в силу Регламента GDPR?

В большинстве случаев никаких ограничений, но ряд брендов ответили, что медийные партнеры инициировали обсуждение соблюдения GDPR и ограничили работу с ретаргетингом. А также столкнулись с проблемой, что некоторые паблишеры отказываются работать в России.

ПАБЛИШЕР - RAMBLER

Попадает ли под действие Регламента: нет, поскольку онлайн-ресурсы Rambler Group

- не предлагают сервисы, адресованные субъектам персональных данных на территории ЕС (сервисы не принимают платежи в валюте стран ЕС и не обозначают стоимость товаров/ услуг в такой валюте, не предоставляют на языках/ под адресам в сети интернет в доменной зоне стран ЕС, не имеют представительства или представителей на территории ЕС);
- не мониторят поведение пользователей стран ЕС, в том числе не таргетирует пользователей, находящихся на территории ЕС, не создает профили таких пользователей;
- не принадлежат/ не предоставляют сервис от имени организаций, зарегистрированных и/или осуществляющих деятельность на территории ЕС.

АГЕНТСТВО - PUBLICIS GROUPE

Попадает ли под действие Регламента: в общих случаях - нет, в отдельных случаях – да.

1. В общих случаях – нет, так как:

- товары/услуги, предлагаемые нашими клиентами-рекламодателями и являющиеся предметом рекламирования, предназначены для реализации на территории Российской Федерации;
- предметом поручения агентству обработка/мониторинг персональных данных физических лиц с территории Евросоюза не является.

2. В отдельных случаях - да. Такими случаями являются:

- наличие в существующих базах данных, включая сегменты аудитории, используемые для таргетинга и подобных услуг, персональных данных, собранных с территории ЕС, без учёта требований GDPR. К примеру, к данной категории относятся все данные, собранные до вступления в силу Регламента, если отсутствуют согласия, соответствующие требованиям GDPR;
- обработка данных, получаемых от поставщиков или клиентов, на которых распространяется действие GDPR. К примеру, получение id пользователей социальных сетей в целях формирования сегмента будет считаться обработкой персональных данных, если нет гарантий, что предоставляемые id исключают собранные на территории ЕС. В случае отсутствия таких гарантий, подобная обработка должна соответствовать GDPR;
- Взаимодействие и обмен данными с некоторыми ключевыми игроками – медиапоставщиками (такими как Google, Facebook и т.д.), подпадающими под действие GDPR, которые требуют безусловного принятия их правил и политик в отношении соблюдения безопасности персональных данных, в том числе путём подписания или принятия условий соглашений об обработке данных (DPA).

ВЕНДОРЫ – WEBORAMA, SIZMEK, CLEVERDATA, MEDIASNIPER/ADSNIPER

WEBORAMA

Попадает ли под действие Регламента: попадание возможно, поэтому внутренние системы выстроены в соответствии с Регламентом.

Какие данные собирают: псевдонимизированные[10] данные.

Кем является по Регламенту: в качестве технологического вендора (при обработке 1st party данных клиентов) Weborama - процессор данных. Однако, так как у Weborama есть своя собственная база данных, относительно последней компания выступает в качестве контроллера.

10. Псевдонимизация - обработка данных в целях невозможности отнесения персональных данных к конкретному субъекту данных без использования дополнительной информации при условии хранения этой информации отдельно и соблюдения других технических и организационных мер обеспечения защиты данных. Псевдонимизация является одним из «соответствующих технических и организационных мер для обеспечения уровня безопасности, соответствующего риску» и рекомендуется, когда это целесообразно и возможно, в соответствии со статьей 32 (1, a) GDPR.

Какое законное основание выбрано для работы с данными: законный интерес (legitimate interest), не предполагающий сбора согласий пользователей для обработки данных.

Какие действия приняты для соответствия Регламенту:

- Проведение аудита дата-активов и PIA (Privacy Impact Assessment);
- Соответствие всех технологических решений принципам Privacy by design (проектируемая конфиденциальность) и Privacy by default (конфиденциальность по умолчанию);
- Назначение DPO (Data Protection Officer) и назначение CSO (Chief Security Officer);
- Проведение обучения всех сотрудников компании принципам обеспечения безопасности данных и приватности данных. А также назначение Privacy Champion в каждом страновом подразделении Weborama, в частности в России;
- Выработка внутреннего регламента по работе с данными;
- Прозрачность и публикация обновленной политики приватности (Privacy Policy) компании (выпуск нового регламента и обновление информации на сайте);
- Документация деятельности по обработке данных (реестр по всем активностям, связанным с обработкой данных);
- Выработка механизма исполнения прав субъектов данных;
- Доработка договоров;
- Присоединение к IAB Europe «Transparency and Consent Framework».

IAB Europe Framework была разработана для предоставления единого стандартизированного решения для определения законного основания для работы с персональными данными, а также открытого обмена этой информацией с партнерами и клиентами.

SIZMEK

Попадает ли под действие Регламента: Попадает.

Какие данные собирают: псевдонимизированные данные.

Кем является по Регламенту: процессор данных.

Какое законное основание выбрано для работы с данными: legitimate interest.

Какие действия приняты для соответствия Регламенту:

- Организация специализированной команды и рабочей группы в составе Sizmek, членами которых являются ключевые фигуры на европейском рынке;
- Назначение Chief Privacy Officer с более чем 20-летним опытом взаимодействия с правительственными организациями и более 15 лет в области защиты данных в интернете;
- Назначение Data Protection Officer, руководителя ePrivacy GmbH, многолетнего эксперта индустрии;
- Перенастройка функционала отчётности для полного соответствия законодательству;
- Интеграция с индустриальными инструментами обработки данных, включая IAB Europe’s GDPR Transparency & Consent Framework;
- Скрытие последнего октета в сырых данных, предоставляемых клиентам;

- Внедрение поддержки обработки запросов на обработку данных от рядовых пользователей;
- Механизм получения согласия пользователя на обработку данных интегрирован в Sizmek Tag Manager.

CLEVERDATA

Попадает ли под действие Регламента: попадает.

Какие данные собирают: псевдонимизированные данные

Кем является по Регламенту: процессор данных.

Какое законное основание выбрано для работы с данными: legitimate interest.

Какие действия приняты для соответствия Регламенту:

- Соответствие всех технологических решений принципам Privacy by design (проектируемая конфиденциальность) и Privacy by default (конфиденциальность по умолчанию);
- Выработка механизма исполнения прав субъектов данных;
- Назначение DPO (Data Protection Officer) и и назначение CSO (Chief Security Officer);
- Выработка внутреннего регламента по работе с данными;
- Доработка договоров на программные продукты;
- Прозрачность и публикация обновленной политики приватности (Privacy Policy) компании (выпуск нового регламента и обновление информации на сайте).

MEDIASNIPER/ADSNIPER

Попадает ли под действие Регламента: в большинстве случаев – нет, но возможны исключения.

Какие данные собирают: псевдонимизированные данные.

Кем является по Регламенту: Mediasniper выступает в качестве контроллера, так как является эксклюзивным селлером технологии Adsniper, тогда как Adsniper – процессор.

Какое законное обоснование выбрано для работы с данными: Legitimate interest

Какие действия приняты для соответствия Регламенту:

- Проведение аудита дата-активов и PIA (Privacy Impact Assessment);
- Соответствие всех технологических решений принципам Privacy by design (проектируемая конфиденциальность) и Privacy by default (конфиденциальность по умолчанию);
- Выработка механизма исполнения прав субъектов данных;
- Назначение DPO (Data Protection Officer);
- Выработка внутреннего регламента по работе с данными;
- Прозрачность и публикация обновленной политики приватности (Privacy Policy) компании (выпуск нового регламента и обновление информации на сайтах Mediasniper и Adsniper).

3. КЕЙСЫ, ИЛЛЮСТРИРУЮЩИЕ ПРИМЕНИМОСТЬ РЕГЛАМЕНТА В РОССИИ

1. Российский паблишер, владелец сайта, посвященного развлечениям и мероприятиям.

Сайт, посвященный развлечениям и мероприятиям в разных городах, размещающий афишу культурных событий в каждом городе, расписание билетов на мероприятия в соответствующих городах, в том числе в городах стран ЕС. Для регистрации на мероприятия и покупки билетов необходимо пройти на сайте регистрацию. Покупка билетов осуществляется в валюте ЕС.

Пользователи стран ЕС получают подборку, сформированную для соответствующего города, также проходят регистрацию на сайте. GDPR будет применяться в части данных пользователей стран ЕС.

Сама по себе возможность доступа на сайт или возможность каким-либо образом связаться с онлайн-сервисом с территории ЕС не означает применение GDPR.

Российский технологический вендор предлагает свои решения европейским организациям, в частности – бесплатный код аналитики (мониторинг поведения на сайте) и полноценное платное решение для работы с данными. Вендор имеет сайт на английском языке, но не имеет физического представительства в ЕС. Обработка данных (по платному и бесплатному решениям) происходит в РФ.

2. Российский технологический вендор попадает под действие Регламента согласно статье 3 Регламента.

Субъект ПД находится в ЕС, а контроллер или процессор учреждены не в ЕС, если деятельность по обработке связана со следующим:

- предложение продуктов и услуг, вне зависимости от необходимости оплаты (возмездная и безвозмездная основы), субъектам в ЕС;
- мониторинг поведения субъектов на территории ЕС.

3. Российский технологический провайдер внедряет решения для автоматизации маркетинга B2C компаниям, предоставляющим услуги и товары гражданам ЕС. Решение провайдера позволяет собирать и обрабатывать ПД о посетителях веб-сайта заказчика для последующей сегментации и использования в персонализированных коммуникациях и онлайн-рекламе. Провайдер решения имеет сайт на английском языке, но не имеет физического представительства в ЕС. Обработка данных происходит в РФ.

- Российский технологический вендор обладает статусом «Процессор» и Попадает под действие Регламента согласно статье 3 Регламента.
- Субъект ПД находится в ЕС, а контроллер или процессор учреждены не в ЕС, если деятельность по обработке связана со следующим:
- предложение продуктов и услуг, вне зависимости от необходимости оплаты (возмездная и безвозмездная основы), субъектам в ЕС;
- мониторинг поведения субъектов на территории ЕС.

4. Российский технологический провайдер внедряет решения для сбора и обработки данных для заказчиков, представленных в странах ЕС. Сбор и обработка данных происходит внутри ИТ-инфраструктуры заказчика с применением программного обеспечения провайдера решения, внедряемого в контур заказчика. В рамках решения реализована возможность автоматического удаления данных отдельного для каждого пользователя, предоставления информации о собранных заказчиком данных и внесения изменений, а также функции отзыва на согласие на обработку данных.

Российский технологический вендор не попадает под действие Регламента и не является процессором данных, так как не обладает физическим доступом к данным.

5. Российская компания – владелец единого сервиса авторизации.

Сервис авторизации (далее - Сервис ID), который могут установить различные сайты, предлагающие товары/ услуги пользователям стран ЕС. Владелец Сервиса ID осуществляет хранение полученных данных пользователей ЕС, прошедших регистрацию посредством функционала такого сервиса авторизации на установивших его сайтах, и имеет доступ к таким данным, тем самым выступая в роли оператора персональных данных. При этом владелец сайта, предлагающий товары/ услуги пользователям стран ЕС, не имеет доступа к данным пользователей, за исключением логина и пароля.

Согласно статье 3 Регламента к владельцу Сервиса ID будут применяться требования GDPR в отношении обработки данных пользователей ЕС, зарегистрировавшихся или авторизовавшихся посредством установленного на указанных сайтах сервиса авторизации.

6. Международный рекламодатель

У международного бренда есть сайт на русском и основных европейских языках. Бренд предлагает свои услуги как в России, так и в странах ЕС (через разные юридические лица). У российской дочерней компании бренда есть CRM-система, которая собирает данные о российских пользователях. Сервер расположен в РФ. Данные о российских пользователях не передаются в материнскую компанию, хранятся и обрабатываются только на территории РФ. Однако, находясь в Европе, российские пользователи из CRM могут посещать сайт и входить в свой личный кабинет.

Бренд также пользуется услугами DSP, у которой сайт на русском и основных европейских языках, и чей пиксель установлен на сайте клиента (+ есть матчинг с CRM). DSP может таргетироваться на российских пользователей из CRM и показывать им рекламу, когда они находятся в странах ЕС.

Международный бренд и DSP попадают под GDPR.