Международное руководство
по проведению мобильных исследований

ESOMAR
Международные исследования

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA • AMRA

ESOMAR (Европейское общество по изучению общественного мнения и маркетинговым исследованиям) – международный представитель сообщества исследователей и специалистов по сбору и анализу данных и инсайтов, выступающий от имени свыше 500 специалистов и 500 компаний, которые оказывают или заказывают услуги по анализу данных и проведению исследований в более чем 130 странах и которые согласились соблюдать положения Международного кодекса ICC/ESOMAR.

GRBN, Глобальная сеть исследовательских ассоциаций, объединяет 45 исследовательских ассоциаций и более 3500 исследовательских компаний на пяти континентах. www.grbn.org

Оглавление

1 ВВЕДЕНИЕ И СФЕРА ПРИМЕНЕНИЯ

Настоящее Руководство ESOMAR/GRBN по мобильным исследованиям поможет исследователям, в особенности тем, кто работает в малых и средних исследовательских организациях, учесть юридические, этические и практические факторы при проведении исследований с использованием мобильных устройств. В нем объясняется, как применять основополагающие принципы проведения маркетинговых и социальных исследований, а также принципы изучения общественного мнения в рамках действующего законодательства и нормативно-правовой среды по всему миру. Кроме того, оно заменяет собой предыдущие отдельные руководства, опубликованные ESOMAR и GRBN в 2012 г. и 2014 г. соответственно. Настоящий документ скорее представляет собой заявление о глобальных принципах, нежели простое перечисление действующих положений.

Настоящее Руководство не заменяет собой ознакомления с Международным кодексом по практике проведения маркетинговых и социальных исследований, изучения общественного мнения и анализа данных или отдельными кодексами 45 ассоциаций, входящих в состав GRBN, и усвоения информации из этих документов. Наоборот, его следует использовать как толкование основополагающих принципов, содержащихся в указанных кодексах, при проведении исследований, в рамках которых отдельные лица обмениваются информацией или данными в тех или иных условиях или в той или иной форме, которые могут позволить установить личность физического лица.

Наконец, в настоящем Руководстве признается, что технологии и государственное регулирование продолжают развиваться, а также то, что в разных странах могут быть разные законы и положения. Поэтому в нем содержится призыв соблюдать три основных требования:

1. Следовать духу и букве действующих законов.
2. Учитывать отраслевые этические и профессиональные принципы в соответствии с нашими профессиональными кодексами.
3. Быть в достаточной степени открытым и гибким, чтобы учитывать как существующие, так и будущие тенденции в сфере мобильных исследований.

1.1. Сфера применения

Настоящее Руководство описывает сбор и использование личных данных с помощью мобильных устройств (мобильными телефонами, планшетами и иными аналогичными мобильными устройствами) в целях проведения маркетинговых и социальных исследований, изучения общественного мнения и анализа данных (далее «исследования»). В нем признается, что существует целый ряд других сфер применения этих устройств, включая, среди прочего, использование сети Интернет, размещение сообщений в социальных сетях, потребление различных типов медиа и совершение онлайн-покупок. Эти данные также можно использовать в исследованиях.

Руководство описывает ответственность исследователей при работе как с первичными данными, собранными для исследования, так и с вторичными данными, которые могли быть собраны для иной цели, но в конечном счете использовались в исследовании. Оно описывает практики, необходимые для соблюдения соответствующих отраслевых кодексов, руководств и применимых требований законодательства регионов, в которых проводится исследование.

В настоящем Руководстве также признается, что третьи лица могут быть задействованы в качестве субподрядчиков по сбору, подготовке, анализу, хранению и доставке данных. При работе с личными данными эти третьи лица несут те же обязательства, что и исследователи.

Многие практики, описанные в настоящем Руководстве, особенно те, что касаются согласия и защиты личных данных, аналогичны практикам, применяемым при проведении онлайн-исследований. Исследователям настоятельно рекомендуется ознакомиться с Руководством по проведению онлайн-исследований ESOMAR/GRBN, Руководством по обеспечению качества онлайн-выборки ESOMAR/GRBN и Контрольным списком по защите данных ESOMAR, которые более подробно описывают многие из требований и/или рекомендаций.

В настоящем документе слова «должен (-ны), необходимо» используются для описания обязательных требований. Мы используем слова «должен (-ны), необходимо» при описании принципов или практик, которые исследователи обязаны соблюдать. Слово «следует» используется при описании порядка внедрения. Таким образом признается тот факт, что исследователи могут внедрять принцип или практику по-разному, в зависимости от дизайна исследования.

2 ОПРЕДЕЛЕНИЯ

В настоящем Руководстве следующие термины имеют особое значение:

Под термином **«Онлайн-панель»** понимается база данных потенциальных респондентов, которые заявили, что готовы сотрудничать при сборе данных в будущем, если они будут отобраны для проведения исследования.

Под термином **«Дети»** понимаются лица, для участия которых в исследовании необходимо получить разрешение от родителя или ответственного взрослого. Определения, в каком возрасте лицо признается ребенком, могут существенно отличаться и устанавливаются национальным законодательством и кодексами саморегулируемых организаций. При отсутствии соответствующего определения в национальном законодательстве ребенком считается лицо в возрасте не старше 12 лет, а подростком – лицо в возрасте с 13 до 17 лет.

Под термином **«Клиент»** понимается любое физическое лицо или любая организация, которые запрашивают, поручают весь исследовательский проект или любую его часть или подписываются на вышеупомянутый проект или его часть.

Под термином **«Согласие»** понимается предоставление физическим лицом добровольного и информированного согласия на сбор и обработку его/ее личных данных.

Под термином **«Субъект данных»** понимается любое физическое лицо, чьи личные данные используются в исследовании.

Под термином **«Идентификатор устройства»** понимается номер, присвоенный мобильному телефону или аналогичному мобильному устройству. Идентификаторы устройства не тождественны серийным номерам оборудования. Зачастую термин «идентификатор устройства» используется в исследованиях для описания снятия «цифровых отпечатков пальцев».

Под термином **«Дедуктивное установление личности»** понимается умозаключение о личности субъекта данных, основанное на перекрестном анализе, небольших выборках данных или их сочетании с иными данными (такими как записи клиента или общедоступные вторичные данные).

Под термином **«Снятие цифровых отпечатков пальцев»** понимается массив конфигурационных данных об устройстве участника исследования (например, о компьютере, мобильном телефоне или планшете), которое можно использовать для создания «отпечатка пальцев» компьютера или устройства. Такие системы подразумевают, что «цифровые отпечатки пальцев» позволяют однозначно установить настройки и характеристики пользователя устройства, связанные с отдельным устройством, или же потенциально определить учетную запись отдельного пользователя.

Под термином **«Кодирование лицевых движений»** понимается метод кодирования движений лицевых мышц человека для определения эмоциональных реакций на различные стимулы, например рекламу или новую концепцию товара. Этот метод отличается от распознавания лица, цель которого – установить личность определенного физического лица по цифровому снимку.

Под термином **«Геолокация**» понимается географическое местоположение устройства, например компьютера, мобильного телефона, планшета и т. д.

Под термином **«Система глобального позиционирования (GPS)»** понимается любая спутниковая система навигации, которая предоставляет сведения о местоположении и времени при любых погодных условиях в любой точке планеты или на околоземной орбите, где имеется четыре или более GPS-спутника в зоне прямой видимости.

Под термином **«Вред»** понимается материальный или физический вред (например, телесное повреждение или финансовый убыток), нематериальный или моральный вред (например, ущерб репутации или престижу) или чрезмерное вторжение в частную жизнь, включая рассылку не согласованных с получателем персонифицированных маркетинговых сообщений.

Под термином **«Интернет вещей (IoT)»** понимается сеть физических устройств, средств передвижения, сооружений и иных предметов со встроенной электроникой, программным обеспечением, датчиками, приводами и возможностью сетевого подключения, которые позволяют этим объектам собирать данные и обмениваться ими.

Под термином **«Мобильное устройство»** понимается небольшое, легкое, ручное вычислительное устройство (например, мобильный телефон или планшет), у которого обычно есть экран с сенсорным вводом и/или миниатюрная клавиатура.

Под термином **«Мобильный телефон»** (также именуемым «сотовый телефон», «сотовый» и «мобильный») понимается устройство, с помощью которого можно совершать и принимать телефонные звонки по линии радиосвязи, перемещаясь при этом по обширной территории.

Под термином **«Тайный покупатель»** понимается использование сборщиков данных, обученных наблюдать за процессом работы с клиентами, а также испытывать и измерять его, выступая в качестве реального или потенциального клиента и выполняя ряд заранее

намеченных заданий по оценке соблюдения стандартов обслуживания клиентов или сбору информации о предложениях конкурентов.

Под термином **«Деятельность, не связанная с исследованиями»** понимаются прямые действия в отношении физического лица, чьи данные были собраны или проанализированы, с целью изменения отношения, мнения или действий такого лица.

Под термином **«Параданные»** понимаются данные о процессе, с помощью которого данные были собраны, включая поведение субъектов данных во время сбора данных.

Под термином **«Пассивный сбор данных»** понимается сбор данных путем наблюдения за действиями или поведением физического лица, а также путем их измерения или записи.

Под термином **«Личные данные»** (иногда называемые «информацией, позволяющей установить личность», или PII – Personally Identifiable Information) понимается любая информация, касающаяся конкретного физического лица (в дальнейшем именуемого «субъект данных»), которую можно использовать для установления его личности, например основываясь на прямых идентификационных данных (таких как имя, определенное географическое местоположение, номер телефона, изображение, звуко- или видеозапись) или не прямо, путем обращения к физическим, физиологическим, психическим, экономическим, культурным или социальным характеристикам такого лица. В некоторых юрисдикциях идентификатор устройства и «цифровые отпечатки пальцев» также считаются личными данными.

Под термином **«Первичные данные»** понимаются данные, полученные исследователем от физического лица или собранные о нем в целях проведения исследования.

Под термином **«Правила защиты личных данных»** понимается опубликованная сводная информация о практиках обеспечения организацией защиты личных данных (иногда называемая политикой защиты личных данных), описывающая порядок, в котором организация собирает, использует, раскрывает данные физического лица и осуществляет управление такими данными.

«Исследование», включающее в себя все формы маркетинговых и социальных исследований, изучения общественного мнения и анализа данных, означает систематический сбор и интерпретацию информации о физических лицах и организациях. В исследованиях используются статистические и аналитические методы и подходы, применяемые прикладными общественными и поведенческими науками и теорией анализа данных для получения инсайтов и содействия принятию решений поставщиками товаров и услуг, органами власти, некоммерческими организациями и общественностью в целом.

Под термином **«Исследователь»** понимается любое физическое лицо или организация, занимающиеся проведением исследований либо выступающие в качестве консультанта в рамках исследования. К данной категории также относятся лица, работающие в организациях-заказчиках, а также задействованные в исследованиях субподрядчики.

Под термином **«Вторичные данные»** понимаются данные, изначально собираемые для других целей, но впоследствии используемые в исследованиях.

Под термином **«Сензитивные данные»** понимаются любые сведения о расовом или этническом происхождении, здоровье или интимной жизни, судимости, политических

убеждениях, религиозных или философских воззрениях физического лица, личность которого может быть установлена. В отдельных юрисдикциях к сензитивным данным также могут быть отнесены дополнительные сведения (например, местоположение или финансовая информация).

Под термином **«SMS (Служба коротких сообщений)»** понимается служба коротких текстовых сообщений, интегрированная в систему телефонной, веб- или мобильной связи и использующая стандартные протоколы связи, которые позволяют обмениваться короткими текстовыми сообщениями между стационарными или мобильными телефонами.

Под термином **«Данные социальных медиа»** понимается информация (например, комментарии или фотографии), которую пользователи создают или которой они обмениваются при использовании социальных медиа.

Под термином **«Носимые устройства»** понимаются электронные устройства (датчики), которые носятся под одеждой, вместе с одеждой, а также поверх или как часть одежды и которые могут собирать данные и обмениваться ими без вмешательства человека.

Под термином **«История посещения сайтов в сети Интернет»** понимается список веб-страниц, которые пользователь недавно посетил, а также такие сопутствующие данные, как заголовок страницы и время посещения, сохраняемые веб-браузером на определенный период времени.

3 СУБЪЕКТЫ ДАННЫХ: ВЗАИМООТНОШЕНИЯ И ОБЯЗАТЕЛЬСТВА

3.1. Непричинение вреда

Исследователи должны принять все меры предосторожности, чтобы исключить причинение субъектам данных вреда, являющегося результатом использования их данных в исследовании. С этой целью они должны тщательно соблюдать особые требования исследования, ознакомиться с местными требованиями законодательства/ограничениями, правилами и обычаями, а также учитывать практические последствия исследований для субъектов данных. В любом случае исследователи должны спрашивать у субъектов данных только то, что, по мнению субъекта данных, является приемлемым, безопасным и правомерным.

Исследователи также должны удостовериться, что программное обеспечение, передаваемое субъектам данных, было тщательно протестировано, соответствует согласованным требованиям к защите личных данных, не препятствует работе мобильного устройства или не повреждает его. Подробнее в Разделе 6 «Недопустимые практики».

3.1.1. Меры предосторожности

При обзвоне номеров мобильных телефонов исследователи могут иногда вступать в контакт с потенциальными субъектами данных, которые занимаются какой-либо деятельностью или находятся в ситуации, которая, как правило, не встречается при звонках на номера стационарных телефонов. К таким видам деятельности и ситуациям можно отнести управление транспортным средством, эксплуатацию оборудования или нахождение в общественных местах. Исследователь должен убедиться, что физическое лицо находится в ситуации, в которой разрешено, безопасно и удобно отвечать на

телефонный звонок. Если исследователь не получает соответствующего подтверждения, то звонок следует завершить и попытаться позвонить в другое время.

Некоторые методы мобильных исследований включают в себя просьбу к респондентам выступить в роли сборщиков данных – посетить определенные места или выполнить определенные задания. В таких случаях исследователи должны предостеречь их от совершения каких-либо действий, которые могут подвергнуть их риску, нарушить закон или неприкосновенность личной жизни других людей. Например, предостеречь их от набора текстовых сообщений или иного использования своего мобильного устройства во время вождения или же от фотографирования или видеосъемки в местах, где фото- или видеосъемка запрещена (например, в административных зданиях, банках, школах, зонах безопасности в аэропортах, на территории частных владений, включая магазины, в которых размещены объявления о запрете фото- или видеосъемки).

3.1.2. Конфиденциальность и сензитивные данные

Исследователь может вступать в контакт с потенциальным субъектом данных, который занимается какой-либо деятельностью или находится в ситуации, при которой его разговор с исследователем могут случайно услышать другие лица. В этом случае исследователь должен принять во внимание характер исследования с учетом возможности, что разговор с субъектом данных могут услышать другие лица; личные данные или поведение могут быть непреднамеренно раскрыты или же ответы могут быть изменены в результате сложившейся ситуации. Звонок, при необходимости, следует перенести на другое время или в другое место, исключающее разглашение конфиденциальных сведений.

Исследователи также должны проявлять осторожность и учитывать риск причинения вреда или страданий, задавая субъектам данных вопросы на деликатные темы. В некоторых странах на сбор сензитивных данных требуется разрешение соответствующего органа государственной власти.

3.1.3. Расходы

В отличие от большинства других методов исследований субъекты данных могут нести определенные расходы в результате своего участия в мобильном исследовании, включая плату за загрузку данных, доступ к сети Интернет, текстовые сообщения, превышение квот тарифного плана, плату за роуминг, получение сообщений на голосовую почту и обычные телефонные расходы. Исследователи должны таким образом разрабатывать дизайн своего исследования, чтобы субъекты данных не несли никаких расходов без прямого согласия. Если же это не представляется возможным, исследователи должны предложить компенсацию в виде наличных денежных средств, мобильных денег, минут или в иной стоимостной форме.

3.1.4. Разграничение исследований и деятельности, не связанной с исследованиями

Исследователи должны четко разграничивать исследовательские цели и деятельность, не связанную с исследованиями. Кроме того, они не должны допускать использования личных данных, которые они собирают для проведения исследований, в каких-либо иных целях без предварительного согласия субъекта данных.

Настоящее требование не запрещает, однако, исследователям принимать участие в деятельности, не связанной с исследованиями, на том условии, что при сборе личных

данных для целей, не связанных с исследованиями, субъекты данных будут о них проинформированы; указанные цели будут четко отграничены от исследований, в которых субъекты данных принимают участие; и согласие на использование данных в целях, не связанных с исследованиями, будет получено до начала сбора данных.

3.2. Дети и иные незащищенные лица

При проведении исследований с участием детей или иных незащищенных лиц исследователи должны ознакомиться с национальным законодательством и кодексами саморегулируемых организаций в юрисдикциях, в которых планируется провести сбор данных, с тем чтобы определить, когда требуется согласие родителей или в каких случаях стереотипы национального мышления требуют особого отношения к таким лицам. Если при контакте с потенциальными субъектами данных по телефону становится очевидно, что субъект данных – ребенок, исследователь должен прекратить интервьюирование до тех пор, пока не будет получено согласие родителя или ответственного взрослого на участие ребенка в исследовании. Если физическое лицо недееспособно, то в некоторых юрисдикциях исследователю, вероятно, придется использовать другой метод проведения исследования.

Исследователи должны проявлять особую осторожность при фотографировании или проведении видеосъемки детей. Если согласие получить не удается, то изображения детей необходимо подвергнуть пикселизации или удалить.

Большинство мобильных операционных систем имеют функции, которые, если их активировать, позволяют запрашивать предварительное родительское согласие на установку приложения. Исследователи должны использовать эти настройки при разработке или заказе разработки приложения, используемого для проведения исследований.

3.3. Порядок уведомления, добросовестность, согласие и добровольный характер исследований

Перед сбором личных данных исследователи должны получить согласие субъектов данных и сообщить следующую информацию:

- имя;
- какую информацию они планируют собрать;
- общую цель сбора данных;
- метод сбора данных;
- продолжительность участия субъекта данных в исследовании;
- каким образом данные будут защищаться; и
- кому данные могут быть переданы и в какой форме.

Настоящая информация должна быть четкой, лаконичной и значимой. См. также Раздел 3.7.1 Правила защиты личных данных. При этом если какие-либо из вышеперечисленных сведений изменятся, необходимо получить новое согласие субъектов данных. Запрещается вводить в заблуждение, обманывать, лгать или принуждать субъекты данных к каким-либо действиям.

Участие в исследованиях всегда носит добровольный характер, и субъектам данных должно быть позволено в любой момент времени отказаться от участия в исследовании и потребовать удаления их личных данных.

И, наконец, исследователи должны соблюдать все соответствующие законы, положения и местные профессиональные правила поведения.

3.3.1. Минимизация объема данных и разумная нагрузка

Исследователи должны ограничивать сбор и/или обработку личных данных только теми сведениями, которые касаются целей исследования. Они также должны следить за тем, чтобы задание (например, опрос, дневник или форум) было предоставлено субъекту данных в форме, подходящей для мобильного устройства, и имело приемлемую продолжительность по времени.

Небольшой размер экрана некоторых мобильных устройств означает, что необходимо уделять особое внимание тому, чтобы инструкции, вопросы или формы были четкими, удобочитаемыми и лаконичными. Это, в частности, подразумевает оптимизацию формата на различных устройствах и исключение из исследования отдельных устройств, если опрос слишком длинный или слишком сложный для такого устройства. Такие практики зачастую обозначаются такими терминами, как «сначала мобильные», «аппаратно-независимый» и «адаптивный дизайн».

Несмотря на неуклонное развитие исследовательских методов, имеющийся опыт показывает, что субъекты данных, участвующие в мобильных исследованиях, рассчитывают на меньшее по продолжительности взаимодействие с исследователями, чем при использовании других методов, таких как телефонные опросы или традиционные фокус-группы.

Аналогичные меры предосторожности следует применять при разработке опросов, проводимых по мобильному телефону с привлечением интервьюера, так как при проведении такого рода исследований удержать онлайн субъектов данных значительно сложнее, чем при звонках на номера стационарных телефонов.

3.3.2. Контакты с потенциальными субъектами данных

Мобильные технологии и системы связи стремительно развиваются, а нормативно-правовая база только формируется. Такие положения и правила оказывают опосредованное воздействие и теоретически могут истолковываться как образующие юридическую ответственность исследователя при контакте с потенциальным субъектом данных посредством мобильного устройства, будь то телефон, электронная почта или текстовые сообщения. Например, в некоторых странах использование автоматизированных систем рассылки текстовых сообщений запрещено без получения прямого согласия.

Исследователям запрещается прибегать к каким-либо ухищрениям для получения адресов электронной почты или номеров мобильных телефонов потенциальных субъектов данных. Настоящий запрет также распространяется на использование публичных веб-сайтов, технологий или техник без ведома физических лиц или на сбор личных данных под видом некой деятельности помимо проведения исследования. И наконец, звонки на номера мобильных телефонов следует настроить таким образом, чтобы субъект данных мог видеть номер вызывающего абонента; запрещается намеренно отключать функцию отображения номера.

Исследователи совместно с поставщиком выборки (будь то собственно поставщик выборки или клиент) должны удостовериться, что в выборки включены только физические лица,

которые рассчитывают получать электронные письма или текстовые сообщения с приглашением принять участие в исследовании.[1]

Подробное описание приемлемых практик смотрите в Разделе 3.5 Руководства по проведению онлайн-исследований ESOMAR/GRBN.

3.3.3. Телефонные исследования

При обзвоне номеров мобильных телефонов исследователи должны учитывать, что даже в тех случаях, когда законодательство ограничивает совершение не согласованных с получателем звонков в коммерческих, а не исследовательских целях, важно сверяться и не использовать имеющиеся исследовательские списки лиц, с которыми запрещен контакт по мобильному и стационарному телефону.

В некоторых странах законодательство или стандарты устанавливают определенные часы, в которые разрешается совершать любые не согласованные с получателем звонки, так что эти временные рамки необходимо соблюдать и при проведении опросов по мобильному телефону.

Исследователи должны предвидеть, что лицо, которому адресован звонок, может находиться в другом часовом поясе, а потому должны проверять удобство времени, места и ситуации для приема звонка. В отсутствие таких требований исследователи должны соблюдать те же временные рамки, что были установлены для проведения исследований с использованием стационарного телефона. При проведении маркетинговых исследований корпоративных клиентов подразумевается, что приемлемым временем для обзвона субъектов данных являются рабочие часы соответствующей компании. Такое же внимание следует уделять рассылке текстовых сообщений на мобильные телефоны, чтобы избежать ситуации, когда участник исследования получает уведомление в «неположенное время».

Одни страны ограничивают использование устройств для автоматического набора телефонных номеров и иной аналогичной аппаратуры, включая предиктивные номеронабиратели. Другие разрешают использовать такое оборудование, только если субъект данных даст свое предварительное прямое согласие (например, в качестве участника онлайн-панели) на прием звонков с аппаратуры для автоматического набора телефонных номеров. В тех странах, в которых устройства для автоматического набора телефонных номеров разрешены и используются, не допускаются прерванные или безмолвные звонки без интервьюера-человека.

3.3.4. Вознаграждения

В тех случаях, когда исследователи предлагают вознаграждения за участие в мобильных исследованиях, они должны четко проинформировать субъекты данных о следующем:

- какие вознаграждения будут предложены;
- кто будет их распределять;
- когда субъекты данных их получат; и
- имеются ли какие-либо условия для получения вознаграждений (например, выполнение определенного задания, доступ к пассивным данным, успешное

[1] Иные технологии обмена сообщениями, такие как рассылка уведомлений в мобильном приложении, могут иметь схожие с текстовыми сообщениями характеристики и возможности.

прохождение проверок качества, минимально необходимое количество времени в качестве активного члена сообщества и тому подобное).

Исследователи должны тщательно обдумывать использование вознаграждений, предоставляемых клиентом (например, товаров клиента или предметов с логотипами клиента), так как в некоторых юрисдикциях это могут счесть маркетинговой деятельностью.

Подробное описание вознаграждений, включая использование лотерей и розыгрышей бесплатных призов, смотрите в Разделе 3.6 Руководства по проведению онлайн-исследований ESOMAR/GRBN.

3.4. Пассивный сбор данных

Мобильные приложения способны собирать широкий спектр личных данных без непосредственного взаимодействия с субъектами данных. В числе примеров можно назвать использование сети Интернет и историю посещений сайтов, статистику использования приложений, данные о картах постоянного покупателя, геолокацию, данные из социальных сетей, данные с носимых устройств и IoT, а также иные данные, сгенерированные или полученные с мобильных устройств.[2]

Кроме того, определенные технологии, такие как онлайн-отслеживание, применяются в исследованиях как один из видов пассивного сбора данных, который обычно включает в себя следующее:

- улучшение достоверности онлайн-выборок;
- предотвращение мошенничества; или
- исследовательские приложения, включая, среди прочего, измерение онлайн-аудитории, анализ содержания и тестирование рекламы.

В этих и аналогичных обстоятельствах исследователи должны принять все необходимые меры для получения согласия в соответствии с Разделом 3.3. Если получение согласия не представляется возможным (например, при измерении трафика веб-сайта), исследователи должны иметь юридически допустимые основания для сбора данных, а также оперативно изъять или скрыть любые идентификационные характеристики настолько быстро, насколько это позволяет операционный процесс (см. Раздел 3.7.2 «Обезличивание персональных данных»).

3.4.1. Биометрические данные

Сбор пассивных и поведенческих данных также предполагает прямое взаимодействие с субъектами данных. Например, кодирование лицевых движений предусматривает запись лицевых движений субъекта данных во время прохождения опроса или выполнения подобного задания. Аналогичным образом можно использовать отслеживание движений глаз, гарнитуру виртуальной реальности и иные носимые устройства. Все они могут подразумевать сбор личных данных и, в ряде случаев, данных, которые в некоторых юрисдикциях считаются сензитивными и требуют выполнения определенных процедур проверки соблюдения применимого местного законодательства и отраслевых кодексов.

[2] Хотя и существует возможность пассивного определения типа устройства, которым пользуется субъект данных, полученные таким образом данные не являются личными, поскольку цель заключается в том, чтобы оптимизировать производительность приложения и рендеринг опросов.

3.4.2. Фотографии и записи

Фотографии, видео- и аудиозаписи считаются личными данными, и, следовательно, их необходимо собирать, обрабатывать и хранить как личные данные. Исследователи могут передавать клиенту фотографии, видео- и аудиозаписи после получения предварительного согласия субъекта на такую передачу и использование данных с определенной целью. В тех случаях, когда информация, потенциально позволяющая установить личность, удаляется (например, с помощью технологии пикселизации или изменения голоса) таким образом, что она больше не считается личными данными, исследователям разрешается передавать подобную информацию клиенту при условии, что клиент соглашается воздерживаться от любых попыток установить личность участника исследования.

Исследователи не должны давать субъектам данных (или тем лицам, которые могут выступать в качестве сборщиков данных) указаний о проведении наблюдения за физическими лицами или общественными местами. Исследователи должны давать субъектам данных определенные ограниченные задания (например, фиксация взаимодействия с друзьями с их согласия или съемки объектов или экранов), не предусматривающие наблюдения за определенной зоной, в которой личные данные собирались бы без согласия присутствующих физических лиц. При фиксации наблюдения в определенном месте следует разместить четкие и удобочитаемые знаки, предупреждающие об осуществлении наблюдения. Вместе со знаками следует разместить контакты исследователя или исследовательской организации, отвечающей за проведение исследования, а изображения физических лиц должны быть подвергнуты пикселизации или удалены в кратчайшие сроки. Камеры следует расположить таким образом, чтобы они осуществляли мониторинг только тех зон, которые предназначены для наблюдения.

3.4.3. Отслеживание поведения посетителей в торговых точках

Отслеживание поведения субъектов данных в торговых точках является формой пассивного сбора данных, при использовании которой фиксируются движения посетителей во время совершения покупок. Специфические области применения подразделяются на две широкие категории.

В рамках первой категории исследователи просят субъектов данных взять с собой устройство или загрузить приложение, которое синхронизируется с аппаратным обеспечением (например, с маячком), чтобы отслеживать и фиксировать передвижения внутри торговой точки. При использовании такого подхода применяются стандартные требования к порядку уведомления и получения согласия (см. Раздел 3.3 «Порядок уведомления, добросовестность, согласие и добровольный характер исследований»).

В рамках второй категории исследователям необязательно прямо сообщать субъектам данных, что за ними наблюдают, а поведенческие данные собираются, пока субъекты находятся внутри торговой точки. В таких случаях исследователи должны убедиться в следующем:

- местное законодательство разрешает мониторинг и сбор данных;
- имеется четкий знак, предупреждающий о ведении записи поведения посетителей; и
- любые идентификационные характеристики изымаются или скрываются настолько быстро, насколько это позволяет операционный процесс.

3.5. Тайный покупатель

Субъекты данных (обычно сотрудники), принимающие участие в исследованиях, проводимых на основе метода «Тайный покупатель», как правило, не знают, что за ними наблюдают. Исследователи должны обеспечивать защиту личных данных физических лиц и исключить причинение субъектам данных вреда, являющегося прямым следствием их участия в исследовании в качестве тайных покупателей. Их личные данные должны быть защищены. Исследователи не должны передавать клиенту фотографии или записи без разрешения субъектов данных, которое обычно предоставляется на основании договора найма.

Метод «Тайный покупатель» отличается от метода сбора данных в ситуации покупки, призванного зафиксировать реакцию субъекта данных на условия совершения покупки и их влияние на решение о покупке, что представляет собой форму этнографического исследования, которое проводится с согласия субъекта данных.

3.6. Использование вторичных данных

Эпоху развития цифровых технологий отличает постоянный рост объема данных, которые образуются как побочный продукт ежедневных операций и процессов. Например, поставщики услуг мобильной связи зачастую собирают подробные сведения о своих клиентах и об их особенностях использования мобильных устройств. Мобильные телефоны фиксируют не только то, кому пользователи звонят и кто звонит им, но и генерируют геолокационные данные о местоположении и посещаемых веб-сайтах, а также к каким вышкам сотовой связи подключались устройства и т. д. Кроме того, мобильные телефоны могут записывать информацию об использовании отдельных приложений и фиксировать сообщения, размещаемые в социальных сетях.

Эти и другие аналогичные данные предоставляют исследователям новые возможности для изучения человеческого поведения. Нередко исследователи разрабатывают отдельные проекты по сбору таких данных с помощью традиционных методов, в то время как большая их часть может уже существовать в виде вторичных данных, которые можно использовать повторно.

Тем не менее перед использованием этих данных исследователи должны убедиться в следующем:

- планируемое использование данных юридически допустимо по условиям соглашения с субъектами данных, заключенного до сбора данных, и не было в явном виде исключено правилами защиты личных данных, действовавшими в момент первоначального сбора данных;
- данные не были собраны с нарушением ограничений, установленных законом, обманным путем или способами, которые были не очевидны для субъекта данных или им не воспринимались и не предполагались;
- субъекты данных имели разумные основания ожидать, что данные могут быть использованы для какой-либо иной цели, например для проведения исследования;
- обращения отдельных субъектов данных, содержащие запрет на использование их данных в иных целях, удовлетворяются; и
- организация, предоставляющая данные, имеет законное право на передачу таких данных.

Исследователи также должны убедиться, что дальнейшее использование данных не причинит вред субъектам данных при применении дедуктивного метода установления

личности. Если такой риск существует, исследователи должны предусмотреть меры предосторожности, чтобы минимизировать риск причинения такого вреда. Такие меры включают, среди прочего, недопущение раскрытия личности отдельных субъектов данных без их предварительного согласия и запрет на осуществление не связанной с исследованиями деятельности, направленной на таких субъектов данных, как следствие использования их данных в исследовании.

3.7. Защита информации и обеспечение конфиденциальности

При работе с личными данными исследователи должны соблюдать универсальные принципы защиты[3] данных. Эти принципы гласят, что любые собираемые или используемые личные данные:

- должны быть собраны с определенной целью и не должны использоваться несоответствующим заявленной цели образом;
- должны быть адекватными, соответствующими и не должны быть излишними применительно к цели, для которой они были собраны и/или использованы;
- не должны быть собраны с нарушением ограничений, установленных законом, обманным путем или способами, которые были неочевидны для субъекта данных или им не воспринимались и не предполагались;
- не должны использоваться способами, которые могут причинить вред субъектам данных, включая применение мер защиты от такого вреда;
- должны быть защищены от таких рисков, как утрата, несанкционированный доступ, уничтожение, использование не по назначению, изменение или раскрытие; и
- должны храниться не более срока, необходимого для целей, ради которых они были собраны или использованы.

Исследователи могут использовать различные стандарты и принципы при разработке необходимых стандартов и политик защиты данных. Для получения дополнительной информации рекомендуем исследователям ознакомиться со Стандартом ISO 27001: Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Требования или Контрольным списком по защите данных ESOMAR.

Исследователи должны тщательно обдумывать решение о размещении личных данных в облаке. Они должны оценить меры безопасности поставщика облачных услуг и его стандартные условия, а также быть готовыми внедрить компенсирующие меры, если меры безопасности поставщика окажутся недостаточными. Подробнее в Разделе 7.7 Руководства по проведению онлайн-исследований ESOMAR/GRBN, Контрольном списке по защите данных ESOMAR и Практическом руководстве по облачным вычислениям.

3.7.1. Правила защиты личных данных

Законы и положения о защите личных данных, как правило, предписывают, чтобы исследовательские компании предоставляли субъектам данных правила защиты личных данных. Из-за ограничений размеров экрана мобильных устройств исследователям следует рассмотреть возможность использования многоуровневых правил защиты личных данных. Обычно они представляют собой краткую версию, содержащую основные сведения, например название организации и способ использования личных данных, а также развернутую версию таких правил.

[3] Например, смотрите Принципы сохранения конфиденциальности ОЭСР.

Предоставление согласия требует, чтобы субъекты данных получили достаточную информацию, ознакомившись только с краткой версией правил. При этом в краткой версии правил должны описываться практики работы и методы использования данных, которые могут быть не очевидны для субъектов данных, такие как звук и изображения, геолокация, вторичное использование, обмен данными, хранение данных, а не такие очевидные типы собираемых данных, как имя, возраст и мнения.

Краткая версия должна содержать ссылку на второе, более подробное описание. При этом вся информация должна быть хорошо видна без необходимости «прокручивать» текст на экране, предназначенный для просмотра с настольного компьютера.

В правилах защиты личных данных должно быть указано, в соответствии с каким (-и) законом (-ами) собираются данные. При сборе данных в нескольких странах исследователь должен соблюдать законы стран, на территории которых проводится сбор данных. В тех случаях, когда представляется возможность установить страну проживания субъектов данных, исследователи должны соблюдать требования законодательства такой страны, принимая во внимание существование значительных правовых различий в зависимости от юрисдикции.

3.7.2. Обезличивание персональных данных

Исследователи должны убедиться, что данные, которые они передают клиентам или иным потребителям данных, в достаточной мере обезличены, чтобы гарантировать неразглашение персональных данных. Существует целый ряд методов удаления идентификационной информации, каждый из которых предлагает различные уровни защиты против раскрытия личных данных и/или дополнительные меры безопасности. Они включают в себя широкий спектр манипуляций с данными, в том числе изъятие прямых идентификационных признаков, изъятие косвенных идентификационных признаков (признаков, которые потенциально могут привести к субъекту данных путем соответствующих умозаключений) и преобразование данных (например, хэширование, шифрование, агрегирование).

Псевдонимизация представляет собой особенно популярный метод обезличивания информации в ходе обработки данных и в случаях, когда требуется воссоздать исходные данные для таких целей, как сопоставление или валидизация. Как правило, псевдонимизация подразумевает отделение личных данных от данных исследования с сохранением различных идентификаторов в отдельных файлах и создание третьего файла, связывающего два идентификатора вместе, который можно использовать для воссоздания исходных данных при необходимости. Доступ к связывающему файлу предоставляется только ограниченному кругу лиц. Исследователям настоятельно рекомендуется псевдонимизировать данные в кратчайшие сроки после их получения.

Анонимизация предусматривает использование целого ряда иных методов, при которых личные данные либо удаляются, либо изменяются таким образом, что повторное установление личности отдельных субъектов данных больше не представляется возможным даже с помощью умозаключений. К таким методам можно отнести изъятие или шифрование отдельных элементов данных, размытие изображений для сокрытия лиц на фотографиях и в видеозаписях, добавление шумов и отражение в агрегированных статистических данных только результатов исследования.

3.7.3. Безопасность устройств

Теоретически посторонние лица могут получить доступ к личным данным, хранящимся локально на мобильном устройстве субъекта данных, если устройство будет похищено или попадет в распоряжение другого лица. К таким данным можно отнести сведения, хранящиеся в приложениях по сбору данных для целей исследования или деятельности, не связанной с исследованиями, установленных на устройстве; фотографии, снятые при проведении этнографического или иного исследования; и SMS, электронные письма или иные сообщения, которые можно было бы использовать для передачи сведений об исследовании, включающих в себя личные данные.

При сборе данных с носимых и иных IoT-устройств исследователи должны убедиться, что все данные были зашифрованы перед передачей на другие устройства.

Субъекты данных должны быть проинформированы об указанных рисках, а исследователи должны внедрять практики по защите личных данных. К примерам таких мер можно отнести шифрование данных (в том числе шифрование данных в местах хранения и передаваемых данных), защиту устройства с помощью пароля, инструктаж субъектов данных о способах удаления всех личных сведений после завершения исследования и иные меры предосторожности или безопасности.

3.7.4. Использование статических и динамических идентификаторов

В определенных случаях заказчики исследований и поставщики выборок прибегают к использованию статических идентификаторов субъектов данных (статические идентификаторы), которые призваны помочь управлять субъектами данных и распределять их в рамках ad hoc и лонгитюдных исследований. Настоящий подход помог обобщить сведения о каждом субъекте данных и заполучить уникальных субъектов данных в рамках отдельно взятого лонгитюдного исследования и/или уложиться в сроки проведения исследования.

Некоторые поставщики выборок предпочитают динамические идентификаторы (идентификаторы, изменяющиеся при каждом последующем использовании) для защиты личности отдельных субъектов данных.

Исследователи должны тщательно обдумывать использование каждого из типов идентификаторов, уравновесив защиту личных данных и качество исследования в контексте проведения определенного исследовательского проекта.

3.7.5. Использование параданных и управление ими

Исследователи должны использовать параданные только в тех случаях, когда поставщик выборки и клиент подписали двустороннее соглашение о регулировании, ограничении и защите сбора, использования и дальнейшей передачи этих данных о процессе сбора данных для последующих исследований и анализа. В некоторых юрисдикциях параданные считаются сензитивными данными.

3.7.6. Трансграничная передача данных

Непосредственно перед передачей личных данных из страны сбора данных в другую страну исследователь должен убедиться, что передача данных носит законный характер, а также

что были предприняты все разумные меры обеспечения защиты и безопасности этих данных. Настоящее правило применяется, если сервер сбора данных и субъект данных находятся в разных странах. Оно также применяется, если для хранения данных, находящихся в другой стране, используются облачные технологии.

Исследователь должен иметь представление о законах и положениях о защите личных данных, действующих в стране отправления и стране назначения данных и регулирующих такую трансграничную передачу данных, принимая во внимание существование альтернативных механизмов передачи данных.

3.7.7. Уведомление об утечке данных

Исследователи должны соблюдать все соответствующие законы и положения, регулирующие порядок уведомления об утечке данных, и требования протокола, применяемые к стране, на территории которой осуществляется сбор данных.

Исследователи должны без каких-либо необоснованных задержек сообщать о нарушениях требований безопасности или утечках данных в первую очередь соответствующим органам власти, если таковые имеются, а затем всем затронутым лицам, включая клиентов, субъектов данных и субподрядчиков. Сообщение об утечке данных должно включать в себя описание типов данных, утечка которых имела место, а также список мер, которые субъектам данных следует предпринять для защиты от потенциального вреда, причиненного утечкой.

3.8. Передача личных данных клиенту

Если для проведения исследования планируется сбор личных данных, которые могут быть также использованы в целях, не связанных с исследовательской деятельностью, исследователи должны четко сообщить об этом субъектам данных до начала сбора данных, а также получить их согласие на использование данных в целях, не связанных с исследовательской деятельностью, если только применимые законы и/или положения о неприкосновенности частной жизни не устанавливают более высокие требования.

Исследователям запрещается передавать своим клиентам информацию, позволяющую установить личность субъектов данных, до тех пор пока от субъекта не будет получено соответствующее согласие на такую передачу и использование данных с определенной целью.

Даже при предоставлении клиентам обезличенных массивов данных исследователи должны получить от клиента письменную гарантию, что он будет воздерживаться от любых попыток повторно установить личность субъектов данных, если только не будут выполнены вышеуказанные условия.

3.8.1. Наблюдатели

Некоторые формы исследований предусматривают участие физических лиц, которые могут иметь доступ к личным данным на том основании, что они наблюдают за сбором данных в режиме реального времени или позднее посредством видео или дэшборда клиента.

К таким лицам можно отнести членов команды клиента, которые не являются ни исследователями, ни субподрядчиками клиента, например рекламные агентства. В таких случаях исследователи должны получить:

- согласие субъектов данных на наблюдение со стороны таких лиц (включая их аффилированные лица) в ходе или после окончания сбора данных; и
- формальное согласие всех клиентов и иных наблюдателей воздерживаться от раскрытия личных данных субъекта или их использования в каких-либо иных целях, помимо проведения исследования, без соответствующего согласия.

4 КЛИЕНТЫ: ВЗАИМООТНОШЕНИЯ И ОБЯЗАТЕЛЬСТВА

4.1. Привлечение субподрядчиков

Исследователи должны до начала работ уведомлять клиентов, что определенные части работ были переданы субподрядчикам, не входящим в структуру организации исследователя. Исследователи должны по первому требованию раскрывать клиентам личность такого субподрядчика.

В тех случаях, когда личность субподрядчика, задействованного для формирования выборки, можно на законных основаниях счесть служебной информацией, поставщик выборки должен предоставить следующее:

- описание типа используемых источников выборки; и
- оценку долей выборки, сформированных из источников панельных и непанельных данных, в процентном выражении.

Исследователи также обязаны убедиться, что любые личные данные, передаваемые субподрядчику, ограничены объемом, необходимым для выполнения субподрядного (-ых) задания (-ий); субподрядчик внедрил необходимые процедуры безопасности для защиты данных; а также что ответственность субподрядчика за защиту данных четко задокументирована и согласована.

4.2. Методологическая корректность

Если исследователи хотят, чтобы пользователи мобильных исследований считали полученные данные пригодными для использования, они должны предоставить клиентам соответствующую информацию о том, каким образом проводилось исследование, позволить им оценить корректность результатов, в том числе ограничения методологии, которые могли привести к выводам, не подкрепленным данными. Такая информация должна включать в себя следующее:

- объем, источник и управление выборкой;
- структуру и определение выборки;
- метод сбора данных;
- применявшуюся очистку, взвешивание или корректировки данных после проведения полевого этапа; и
- в тех случаях, когда уровень проникновения мобильной связи составляет менее 100 %, меры, принятые для репрезентации целевой аудитории исследования.

С дополнительными требованиями в каждой из вышеуказанных сфер можно ознакомиться в Руководстве по обеспечению качества онлайн-выборки ESOMAR/GRBN и Разделе 6 Руководства по проведению онлайн-исследований ESOMAR/GRBN.

4.3. Прозрачность, искажение данных и исправление ошибок

Вся деятельность в ходе исследовательских проектов должна тщательно, открыто и объективно учитываться и документироваться. При обнаружении ошибок после предоставления данных исследователь должен незамедлительно уведомить о них клиента и своевременно внести необходимые исправления.

5 ШИРОКАЯ ОБЩЕСТВЕННОСТЬ: ВЗАИМООТНОШЕНИЯ И ОБЯЗАТЕЛЬСТВА

5.1. Поддержание общественного доверия

Исследователи должны быть добросовестны, честны, объективны, а также должны обеспечивать проведение исследований в соответствии с уместными научно-исследовательскими принципами, методиками и приемами.

Исследователи должны всегда руководствоваться этическими нормами и воздерживаться от любых действий, способных нанести ущерб репутации маркетинговых и социальных исследований, опросов общественного мнения и анализа данных. В своей деятельности они должны всегда помнить основные принципы Кодексов ICC/ESOMAR и GRBN, а также воздерживаться от работ и практик, которые могли бы подорвать общественное доверие к маркетинговым и социальным исследованиям и опросам общественного мнения.

5.2. Публикация результатов исследования

Подробнее об обязательствах исследователя, возникающих в тех случаях, когда клиент планирует опубликовать результаты исследования, смотрите в Разделе 5.2 Руководства по проведению онлайн-исследований ESOMAR/GRBN.

6 НЕДОПУСТИМЫЕ ПРАКТИКИ

Исследователи не должны использовать или устанавливать программное обеспечение или приложения, которые:

- не были надлежащим образом протестированы;
- без согласия субъекта данных изменяют мобильные настройки сверх того, что необходимо для проведения исследования;
- вызывают конфликты с операционной системой или приводят к тому, что иное установленное программное обеспечение ведет себя неустойчиво или непредсказуемо;
- скрыты внутри другого программного обеспечения, которое может быть загружено или же которое сложно удалить;
- содержат рекламный контент, если только он не требуется для проведения законного рекламного исследования;
- изменяют собранные данные, не уведомляя субъекта данных и не предлагая ему возможности отказаться от таких изменений;
- приводят к необычному ускорению разряда аккумулятора устройства без особого разрешения;

- приводят к образованию у субъекта данных расходов, которые он несет без соответствующего согласия и которые исследователь ему не возмещает;
- используют геолокационное программное обеспечение без согласия субъекта данных;
- передают личные данные в незашифрованном виде;
- изменяют характер технологий распознавания и отслеживания без уведомления и согласия субъекта данных;
- не уведомляют субъекта данных об изменениях в практиках защиты личных данных после обновлений;
- собирают личные данные, которые могут быть использованы поставщиком приложения для целей, не связанных с исследованиями, без соответствующего согласия; или
- извлекают информацию из мобильного устройства или телефона, если только получение такой информации не входит в цели исследования и соответствующее согласие не было получено.

После завершения исследования приложения, использование которых больше не требуется, должны быть деактивированы. Исследователи должны сообщить субъектам данных и проинструктировать их о том, как безопасно удалить приложение с устройств (-а).

7 КОЛЛЕКТИВ РАЗРАБОТЧИКОВ

- Редж Бейкер, сопредседатель ESOMAR, исполнительный директор, консультант Международного института по маркетинговым исследованиям (MRII) и Комитета по профессиональным стандартам ESOMAR, США.
- Гай Рольф, сопредседатель GRBN, ведущий специалист по мобильным инновациям и новым технологиям, Kantar, Великобритания.
- Марио Каллегаро, старший научный сотрудник по вопросам исследования общественного мнения, Google, Великобритания.
- Симон ван Дёйвенворде, коммерческий директор, Wakoopa, Нидерланды.
- Стив Гаттерман, главный исполнительный директор Mobile Accord, Inc., США.
- Бетси Лейчлитер, Leichliter Associates, LLC, США.
- Ориоль Ляурадо, руководитель службы защиты информации, Netquest, Испания.
- Питер Милла, консультант Insights Association, США.
- Пол Квинн, старший директор по управлению товарным производством, Confirmit, Великобритания.
- Лиза Салас, руководитель отдела маркетинга и производства, TEG Rewards, Австралия.
- Майкл Шлютер, помощник директора по вопросам глобальных инноваций, GfK, Великобритания.
- Нэвин Уильямс, главный исполнительный директор, Mobile Measure, Сингапур.

ESOMAR: Кэти Джо, директор по международным стандартам и взаимодействию с государственными структурами, и Ян Виллем Книббе, директор по вопросам политики и отраслевым проектам