



Персональные данные потребителей: когда частное становится публичным?

Исследование по вопросам
неприкосновенности частной жизни



Содержание

Введение	4
Что приемлемо и неприемлемо для потребителей?	6
Слишком активный сбор данных может оттолкнуть потребителей	8
Кому доверяют потребители?	10
Исходная информация	14
Опасайтесь отрицательной реакции: потребители захотят получить свою долю	16
Где проводят черту регулирующие органы?	21
Отношение к персональным данным: мировые тенденции	22
Отношение к персональным данным: ситуация в различных отраслях	24
Что должны предпринять компании, чтобы выжить?	26
В каком направлении будет развиваться использование персональных данных?	30
Как и чем может помочь КПМГ?	33
Информация об исследовании	34

Введение

Сегодня компании знают о своих клиентах намного больше, чем раньше. Благодаря современным технологиям за сутки компания может собрать о клиентах намного больше информации, чем казалось возможным десять или двадцать лет назад: какие продукты они покупают, куда едут отдыхать, где они ужинали вчера вечером или на чем добрались на работу сегодня утром.

Потребители тоже извлекают из этого пользу: фитнес-приложения подсчитывают количество сделанных нами шагов, благодаря мессенджерам мы можем отправить фотографии с пляжа, а телематические системы в наших автомобилях позволяют снизить страховую премию.

Когда мы используем подобные технологии (на компьютере, смартфоне или в автомобиле с возможностью подключения к сети), то предоставляем информацию о себе в обмен на услугу или продукт, которые делают нашу жизнь проще, лучше, а иногда и дешевле.

Этот компромисс лежит в основе экономики данных, однако у него тоже есть свои границы. Люди все более отчетливо понимают, что организации собирают, используют, сохраняют и сообщают другим лицам информацию о них, в том числе покупая и продавая ее. И их все больше беспокоит вопрос: когда польза от этого превратится в навязчивое вмешательство в частную жизнь?

Чтобы понять, когда потребители спокойно относятся к использованию своих персональных данных, а когда – настороженно, KPMG International провела исследование, в ходе которого было опрошено почти 7 000 респондентов из 24 стран.

Результаты опроса вполне закономерно показали, что границы компромисса в отношении использования личных данных пользователей могут очень сильно отличаться и то, что неприемлемо для одних, будет нормально для других. При этом пол, возраст, состояние, национальность и образование часто очень неожиданно влияют на то, где проходят эти границы.

Так, например, более половины участников исследования готовы указывать в сети интернет информацию о своем поле, образовании и этнической принадлежности, но при этом менее 20% готовы сообщать сведения о своих доходах, местоположении, состоянии здоровья или адресе.

Как выяснилось, в таких азиатских странах, как Индия и Малайзия, лучше, чем в скандинавских странах, относятся к идее персонализированной рекламы. А японские потребители, похоже, значительно меньше доверяют организациям, обрабатывающим персональные данные, чем жители Индии, но при этом они реже других принимают меры для защиты своих персональных данных.

Общество совсем недавно стало задаваться вопросами этического и правового характера относительно того, что в эпоху больших данных является личным, а что – публичным. И это не чисто философский спор, который компании могут игнорировать. Нарушение нормативных предписаний или неправильная оценка позиции потребителей не только несет за собой серьезные финансовые последствия на таких ключевых рынках, как Европейский союз и США, но и грозит потерей доверия и интереса со стороны потребителей, которые считают, что происходит вмешательство в их частную жизнь. Цены акций, прибыль и даже выживание некоторых компаний, вероятно, будут зависеть от более разумного и продуманного подхода к использованию этих данных.

Сегодня очень немногие компании задаются вопросом, используют ли они информацию о потребителях в соответствии с требованиями морали и права. Однако мы считаем, что пришло время это сделать.



Марк Томпсон

Руководитель
Международной группы
по вопросам использования
и защиты персональных данных
KPMG International



Грег Белл

Соруководитель
Международной группы
по вопросам кибербезопасности
KPMG International



Ахилеш Тутя

Соруководитель
Международной группы
по вопросам кибербезопасности
KPMG International

Что приемлемо и неприемлемо для потребителей?

Когда что-то нормальное становится недопустимым?

Когда удобство превращается в навязчивость?

Если компании хотят, чтобы потребители им доверяли, им очень важно понимать, как они относятся к использованию их персональных данных.

Международные результаты исследования:



Более половины респондентов заявили, что они готовы делиться в интернете персональными данными о своем поле, образовании и этнической принадлежности.

<20%

Менее 20% согласны раскрывать информацию об истории своих поисковых запросов в сети интернет, доходе, местоположении, адресе или состоянии здоровья.

55%

55% опрошенных сообщили, что они отказывались от покупки чего-либо в интернете из соображений, связанных с неприкосновенностью частной жизни.



В большинстве стран респонденты считают, что **контроль за конфиденциальностью персональных данных** важнее удобства.



Считается, что социальные сети, а также компании из индустрии азартных игр и развлечений запрашивают чрезмерный объем персональной информации.



На всех рынках, кроме одного, не менее **75%** респондентов отметили, что их беспокоит продажа данных о покупках, совершенных ими в интернете, третьим лицам.

>2/3

Более двух третей опрошенных чувствуют себя некомфортно из-за использования их персональных данных приложениями для смартфонов и планшетов.



Половина участников исследования уже удаляют файлы cookie при использовании интернет-браузеров или управляют настройками конфиденциальности в социальных сетях.



Почти **треть** респондентов при просмотре веб-сайтов используют режим «инкогнито» или режим, позволяющий избежать отслеживания действий пользователя.



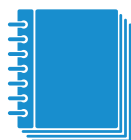
25% используют для защиты своих персональных данных шифрование.

50%

Лишь около **половины** опрошенных согласились бы на получение бесплатной или более дешевой продукции в обмен на раскрытие большего объема персональных данных.



Размер доходов, судя по результатам исследования, не оказывает большого влияния на готовность людей раскрывать больше персональных данных.



Уровень образования не влияет на отношение потребителей к вопросам неприкосновенности частной жизни и на то, что они считают опасным или допустимым.

Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

Слишком активный сбор данных может оттолкнуть потребителей

Многие организации еще не определили, какой уровень вмешательства в различные сферы своей жизни готовы допустить их клиенты. Потребители часто группируют свои отношения с компаниями в зависимости от того, когда и где они с ними взаимодействуют. Когда компании вторгаются в частную жизнь глубже, чем рассчитывали потребители, это может вызвать раздражение последних, и они в конечном итоге могут отказаться от использования данного бренда.

Стремление потребителей к защите своих персональных данных

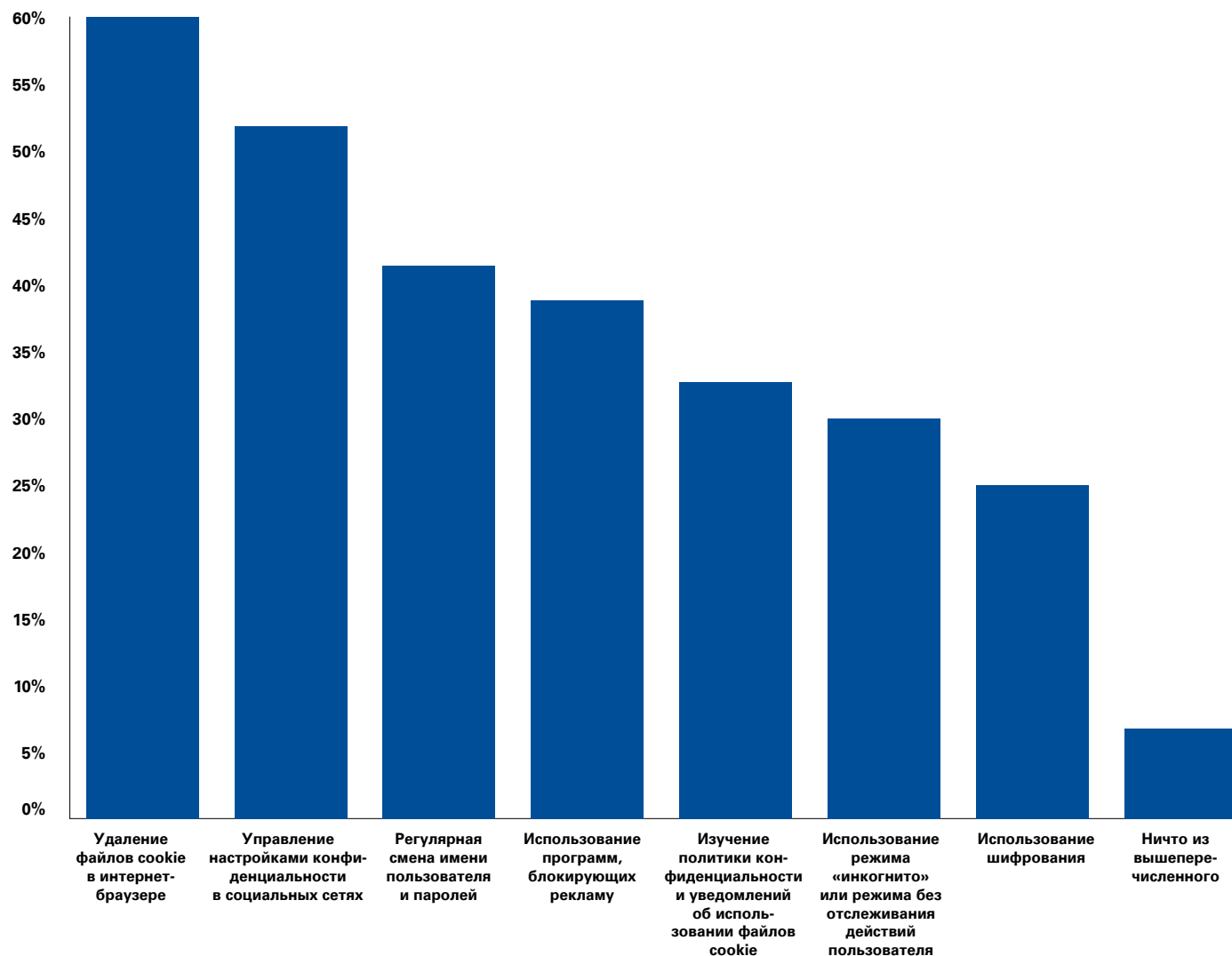
Даже если компании готовы непрерывно собирать персональные данные о своих клиентах, то самим потребителям это может не нравиться. Ожидания людей в отношении их личного пространства дома, на работе или в общественных местах принципиально различны, и они не хотят передавать контроль за своей частной жизнью третьим лицам.

При этом менее 10% потребителей по всему миру считают, что они полностью контролируют то, каким образом организации обрабатывают и используют их персональную информацию. В Испании 55% опрошенных заявили, что у них вообще нет никакого контроля, и даже в Малайзии, где наблюдается наиболее спокойное отношение к контролю за персональными данными, лишь 31% респондентов отметили, что они располагают достаточным или полным контролем за обработкой и использованием их персональных данных.

«Около одной пятой респондентов весьма обеспокоены тем, как организации обрабатывают и используют их персональные данные».

Поэтому беспорядочный сбор персональных данных может оттолкнуть потребителей. И чем некомфортнее чувствуют себя люди, тем выше вероятность того, что они будут принимать меры для защиты своих персональных данных в интернете. Половина участников исследования во всем мире уже удаляют файлы cookie при использовании интернет-браузеров или управляют настройками конфиденциальности в социальных сетях. Почти одна треть (30%) используют режим «инкогнито» или режим, позволяющий избежать отслеживания действий пользователя, а 25% применяют шифрование (**см. рис. 1**).

Рис. 1. Меры предосторожности, которые обычно принимают потребители для защиты своей персональной информации



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

Публичная и частная сфера

Люди инстинктивно опасаются делиться информацией об их жизни дома. Так, в США компании энерго- и водоснабжения уже столкнулись с нежеланием пользователей устанавливать интеллектуальные счетчики в жилых зданиях¹. Согласно результатам исследования, 43% потребителей настораживает присутствие в их домах таких приборов, если на основании полученной ими информации коммунальные компании могут сделать вывод о том, сколько людей живет в доме и что они делают в определенное время дня.

1. <http://bv.com/docs/articles/the-opt-out-challenge.pdf>

Кому доверяют потребители?

Пользуются наибольшим доверием

41%

Банки

39%

Медицинские
учреждения

36%

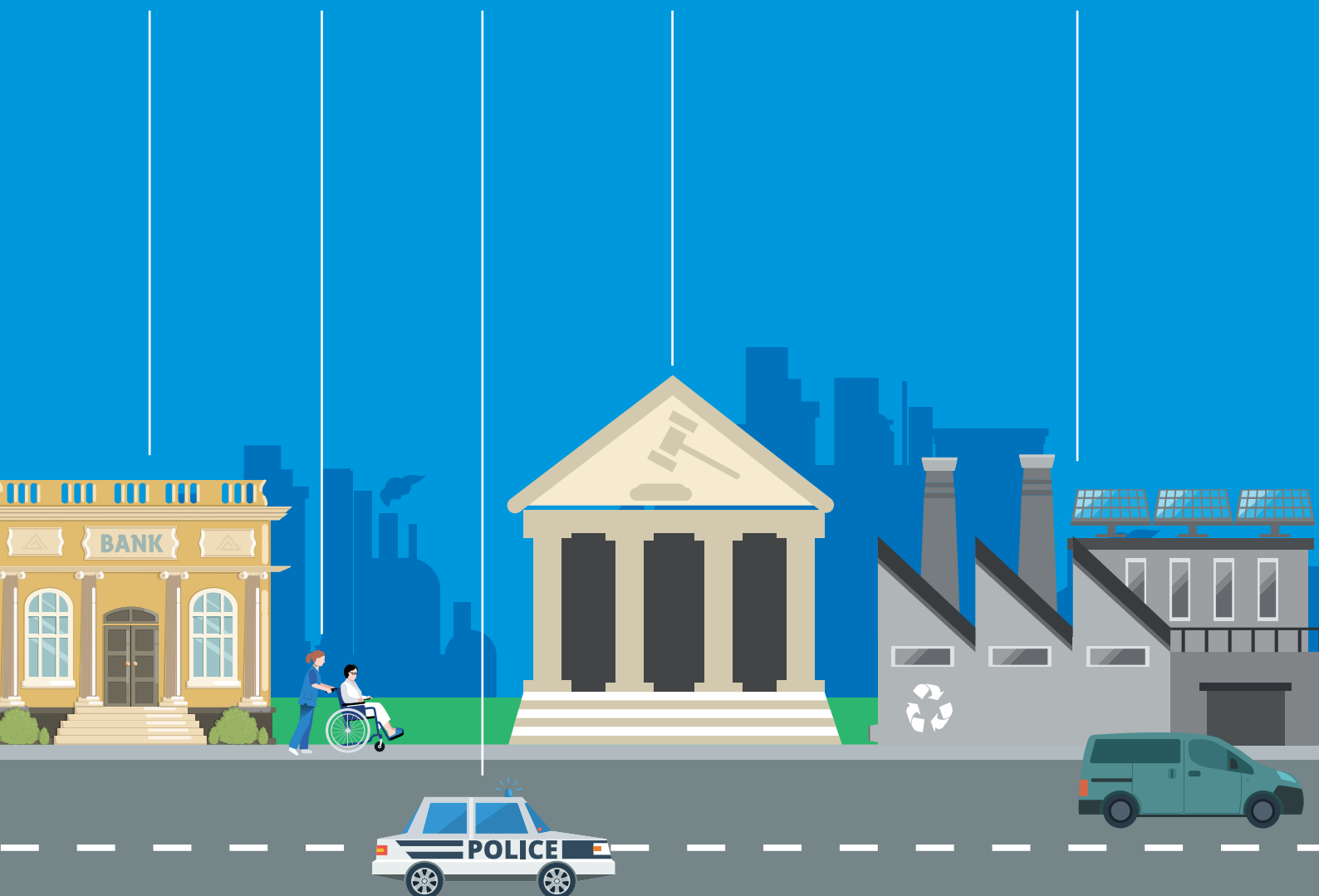
Правоохра-
нительные
органы

33%

Местные
органы
власти

23%

Коммунальные
предприятия



Пользуются наименьшим доверием

21%

Технологические
компании

17%

Супермаркеты

14%

Индустрия
азартных игр

14%

Компании
розничной
торговли

13%

Социальные
медиа



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

© 2016 КПМГ. Все права защищены.

Персональные данные потребителей: когда частное становится публичным? 11

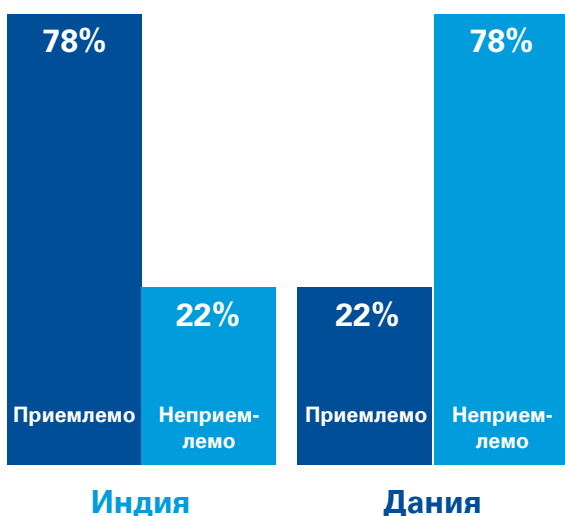
Результаты исследования показали, что отношение к конфиденциальности зависит от типа данных и характера их предполагаемого использования, а также от позиции и местоположения потребителя. Так, например, 78% опрошенных не нравится идея персонализированных электронных рекламных щитов, тогда как 54% респондентов готовы согласиться на отслеживание просматриваемых ими телепрограмм в обмен на снижение платы за телевидение. Или же 49% потребителей не возражают против сбора персональных данных государственными органами в целях борьбы с терроризмом, тогда как на продажу персональных данных третьим лицам интернет-магазинами согласны 28% участников исследования.

Кроме того, разница в отношении сильно зависит и от региона. Так, **78% опрошенных из Индии** считают, что использование данных о геолокации может быть полезно для предложения услуг по перевозке таксомоторных компаний, а **в Дании** такой точки зрения придерживаются лишь **22%**

респондентов (см. рис. 2). Аналогичным образом, **в Китае 60%** участников исследования спокойно относятся к персональной щитовой рекламе, а **88% респондентов из Японии** считают это ненормальным (см. рис. 3).

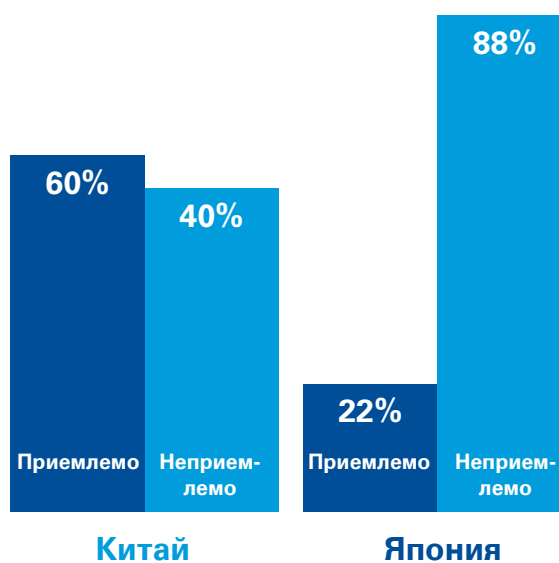
Это дает возможность использовать в отношении персональной информации принципы двойной экономики. Некоторые потребители с радостью передают свои персональные данные (или у них нет другого выбора), тогда как более осторожные могут использовать определенные стратегии – или, возможно, платить – для сохранения конфиденциальности. Это нежелательная перспектива для рекламодателей и компаний, поскольку они используют персональные данные о своих потребителях для эффективной разработки и сбыта своей продукции. В связи с этим организациям как никогда важно научиться грамотно и эффективно использовать данные о потребителях, чтобы последние продолжали свободно делиться своей информацией.

Рис. 2. Использование геолокации таксомоторными компаниями



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

Рис. 3. Персональная щитовая реклама



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

Полезная информация для руководителей: риски, связанные с доверием



Марк Томпсон
Руководитель
Международной группы
по вопросам использования
и защиты персональных данных
KPMG International

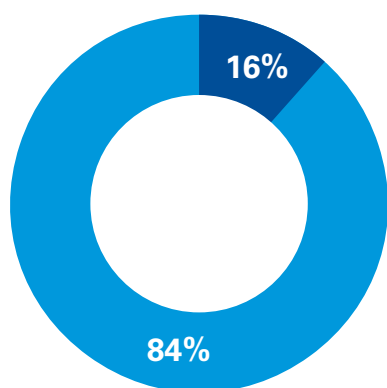
«Чтобы сохранить доверие потребителей, компаниям следует действовать с большей осторожностью при сборе персональных данных о тех сферах, которые, по мнению потребителей, требуют более деликатного обращения. Хотя некоторые из них по-прежнему считают обмен персональных данных на услуги приемлемой ценой, другие будут сильнее стараться сохранить конфиденциальность информации о себе.

Если компании не смогут предложить убедительный аргумент в пользу сбора личных данных, то потребители будут максимально использовать все возможности, чтобы не раскрывать эту информацию. Это может предвещать классовое расслоение в сфере обработки персональной информации. Люди, заботящиеся о неприкосновенности своей частной жизни, вероятно, будут вкладывать средства в разнообразные методы защиты. И, как показывают результаты исследования, многие потребители уже принимают передовые меры для защиты своих личных данных в интернете».

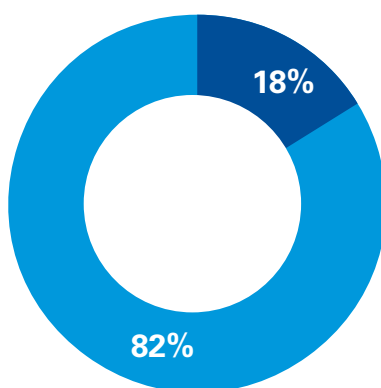


Исходная информация

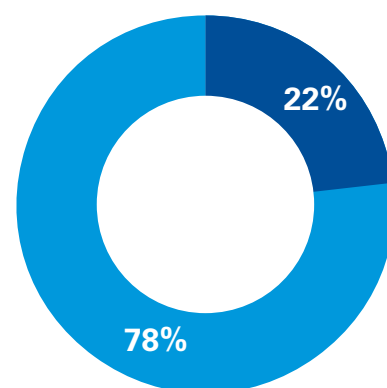
Приемлемое/неприемлемое для потребителей



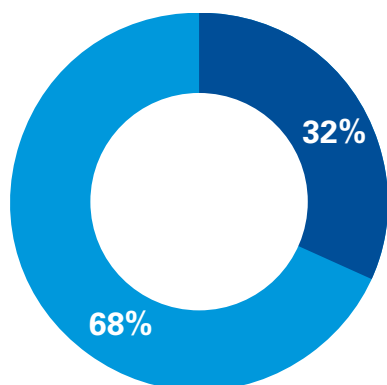
Доступ приложений смартфонов и планшетов, используемых для навигации, общения и получения новостей, к вашим контактам, фотографиям и истории веб-поиска



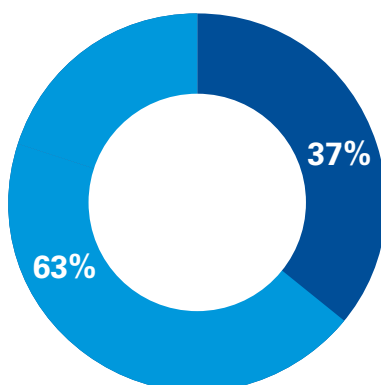
Интернет-магазины, предлагающие скидки, скорость, удобство, широкий ассортимент и доставку, но продающие ваши данные третьим лицам



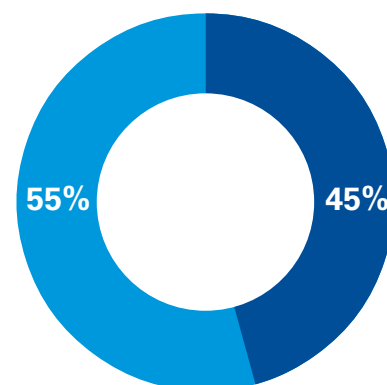
Электронный рекламный щит, приветствующий вас по имени, спрашивающий, понравился ли вам завтрак, и показывающий рекламу ваших любимых хлопьев



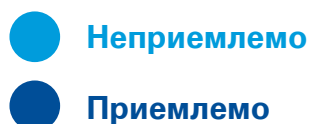
Вы пишете в электронном письме другу о планируемой поездке в Париж. На следующий день, пользуясь интернетом, вы замечаете рекламу отелей, ресторанов и экскурсий в Париже

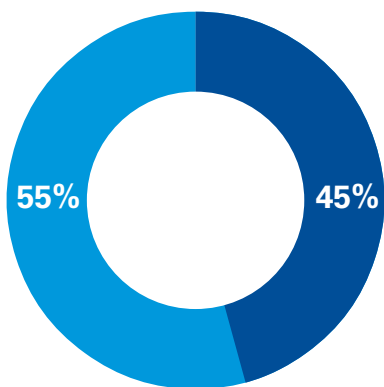


Таксомоторная компания, покупающая ваши геолокационные данные, чтобы иметь возможность автоматически предложить вам поездку на такси, когда вы сходите с поезда

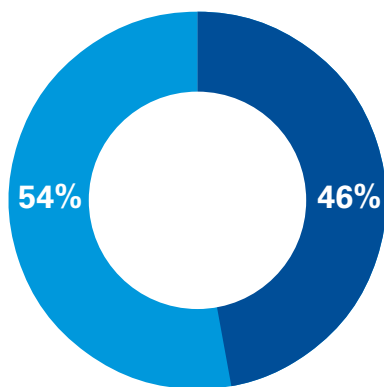


Бесплатный фитнес-трекер, отслеживающий ваше физическое состояние и готовящий ежемесячный отчет для вас и вашего работодателя

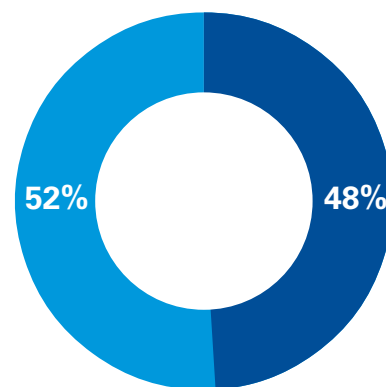




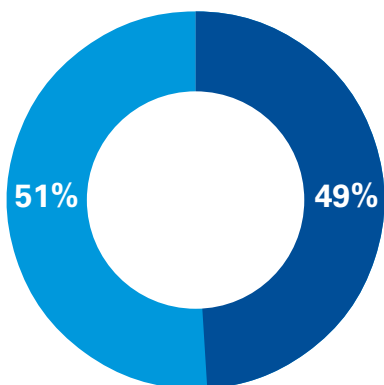
Телематическое устройство, снижающее стоимость страхования, но дающее вашей страховой компании право информировать полицию об опасном вождении вами автомобиля



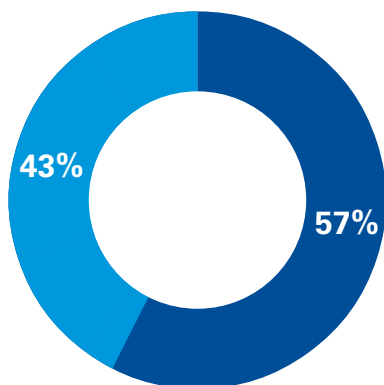
Новый телевизор со скидкой, если вы разрешаете отслеживать ваши зрительские привычки



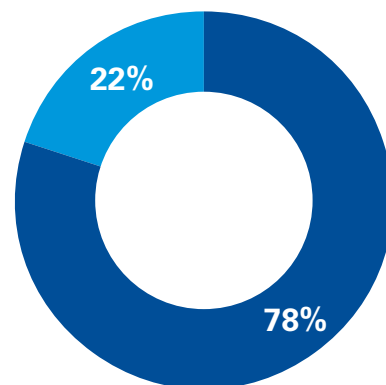
Бесплатный планшет, если вы позволяете технологической компании отслеживать, когда, зачем и каким образом вы его используете



Разрешение собирать информацию о ваших электронных письмах, текстовых сообщениях и истории поисковых запросов в интернете, чтобы помочь правоохранительным органам предотвращать террористические акты



Интеллектуальные счетчики электроэнергии, позволяющие вашему поставщику сделать вывод о том, сколько людей живет в вашем доме, когда вы едите и спите и какие электроприборы вы используете



Телематическое устройство, позволяющее аварийно-спасательным службам отслеживать местоположение вашего автомобиля

Опасайтесь отрицательной реакции: потребители захотят получить свою долю

Ежедневно потребители соглашаются предоставлять организациям свои персональные данные в обмен на бесплатное общение, быстрое получение информации, неограниченные развлечения и беспримерные удобства. Пока потребители чувствуют, что сделка является взаимовыгодной, соглашение продолжает действовать.

Но что произойдет, если значительная часть потребителей, скажем, тех, кому не нравится использование их персональных данных, почувствуют, что их обманывают? Или они получат больше информации о том, каким образом используются их персональные данные? Растущая популярность анонимного просмотра веб-сайтов, блокирование рекламы и удаление файлов cookie – первые признаки того, что эта проблема начинает волновать все большее число людей.

Результаты исследования показали, что 60% потребителей по всему миру уже удаляют файлы cookie при использовании веб-браузеров, а 52% управляют настройками конфиденциальности в социальных сетях.

Информация в разбивке по странам показывает, что в Индии больше всего людей управляют настройками конфиденциальности в социальных сетях и регулярно меняют имя пользователя и пароли для защиты персональной информации.

А респонденты из Японии, наоборот, реже других принимают меры предосторожности для защиты персональной информации.

По мере того как люди начинают больше интересоваться защитой частной жизни, компании рискуют столкнуться с отрицательной

реакцией потребителей, когда они осознают, сколько денег зарабатывают коммерческие предприятия на торговле их персональными данными.

Бизнес-модели крупных поисковых систем и платформ социальных сетей основаны на продаже данных о потребителях. По оценкам Организации экономического сотрудничества и развития (ОЭСР), персональные данные, касающиеся одного европейского потребителя, приносят Facebook чуть менее 5 долл. США в год. Данные об американском потребителе стоят ближе к 10 долл. США². В 2014 г. новая компания – брокер данных Datasoap предложила людям исключительные права на их собственные персональные данные за 8 долл. США в месяц³, предопределив возникновение этически спорной ситуации, когда люди вынуждены выкупать свои собственные данные у третьих лиц.

Персональные данные могут возникать в результате отслеживания действий потребителей в интернете, их покупок и сообщений. Собирающие данные компании считают, что после того как вы поделились своими данными, они больше уже вам не принадлежат.

Британская Государственная служба здравоохранения, например, уже изучила возможность извлечения прибыли из имеющихся у нее на хранении персональных данных. Инициаторы этой программы говорят, что затраты на перевод данных, используемых службой здравоохранения, в цифровой формат окупятся за счет повышения эффективности, а также за счет предоставления компаниям платного доступа к обезличенной медицинской информации.

2. Исследование ОЭСР (2013 г.): "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, No. 220, OECD Publishing. <http://dx.doi.org/10.1787/5k486qtxldmq-en>

3. Статья в издании The Guardian: How much is your personal data worth? | News | The Guardian

Брокеры данных

Вероятно, они знают о вас больше, чем ваша вторая половина, мать или отец – возможно, даже больше, чем вы сами.

Брокеры данных собирают и продают информацию о миллиардах людей по всему миру. Они могут знать ваш адрес электронной почты и номер телефона, что вы искали онлайн несколько месяцев назад, ваши покупательские привычки ... и даже ваши сексуальные предпочтения.

Согласно заявлению одного из ведущих брокеров данных, он располагает информацией о 700 миллионах потребителей со всего мира и о более чем 3 тысячах «пристрастий» почти для каждого американского потребителя.



Раздел выручки

Более справедливая модель распределения доходов от персональных данных предполагает заключение потребителями официального соглашения о разделе выручки с компаниями, которые перепродают персональные данные. Или же другой вариант – компании устанавливают цены на свою продукцию в зависимости от предоставляемых потребителем персональных данных. В определенной мере такая схема уже используется с телематическими устройствами, которые снижают размер платы за страхование автомобиля в обмен на то, что отслеживают стиль вождения автолюбителя. На самом деле 45% опрошенных по всему миру заявили, что страховые компании могут отслеживать их манеру вождения в обмен на более низкую страховую премию, даже при наличии угрозы информирования полиции. А в **Бразилии, Китае и России** на такое отслеживание во время вождения согласно большинство респондентов (64%) (см. рис. 4).

Поэтому вполне реально предположить, что следующим этапом может быть аналогичное соглашение, позволяющее уменьшить премию за страхование здоровья в обмен на ношение устройства, отслеживающего физическую активность.

Согласно результатам исследования, если бы работодатели предложили респондентам самую последнюю версию фитнес-трекера, чтобы отслеживать уровень их физической активности и предоставлять ежемесячный отчет о том, как вести здоровый образ жизни, на такое предложение согласились бы 76% бразильцев и 85% жителей Индии. Однако в Северной Европе подобная договоренность приемлема для меньшего числа опрошенных.

Модель двойного ценообразования может распространиться и на другие устройства, подключаемые к интернету. Телевизор, отслеживающий программы, которые смотрит потребитель, может стоить 100 долл. США. Тот же

самый телевизор без отслеживания данных может стоить 500 долл. США. Учитывая, что нас окружает «Интернет вещей» — совокупность подключенных к Всемирной сети устройств («вещей»), число которых к 2020 г., по оценкам, превысит 20 млрд, — производителям потребительских товаров стоит об этом задуматься⁴.

Главный вопрос цифрового будущего заключается в том, готовы ли потребители делиться персональными данными. Результаты исследования показывают, что в подавляющем большинстве стран от 60 до 87% опрошенных считают, что контроль за неприкосновенностью их частной жизни важнее удобства, а 55% респондентов сообщили, что они отказывались от покупки чего-либо в интернете из соображений, связанных с защитой их персональных данных. Больше других о судьбе своих персональных данных при совершении онлайн-покупок беспокоятся потребители в **Малайзии** (74%), **Финляндии** (72%) и **Сингапуре** (70%) (см. рис. 5).

Однако, возможно, сегодня даже если потребители очень захотят вернуть контроль за персональными данными, они просто не смогут это сделать. Персональная информация любого лица уже распространилась настолько широко, что вернуть контроль над ней в полном объеме практически невозможно. И учитывая ускоряющиеся темпы подключения различных устройств к интернету, можно даже говорить о том, что до сих пор потребители делились лишь небольшой частью персональных данных, потенциально пригодных для обмена.

В более долгосрочной перспективе компании, возможно, будут вынуждены устанавливать более четкие границы в отношении передачи персональных данных третьим лицам и открыто признавать стоимость данных о потребителях. А до тех пор, вероятно, им нужно хотя бы научиться управлять неминуемым недовольством потребителей и сводить к минимуму его отрицательные последствия.

Рис. 4. Отслеживание стиля вождения



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

Рис. 5. Беспокойства относительно персональных данных во время онлайн-шопинга



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

4. <http://www.gartner.com/newsroom/id/3165317>

Полезная информация для руководителей: красный свет для продавцов данных



Грег Белл

Соруководитель
Международной группы по
вопросам кибербезопасности
KPMG International

«Разница в цене в момент покупки, по крайней мере, будет открытым признанием факта сбора персональных данных. Сегодня же потребителям приходится выбирать, пользоваться ли услугой, на основании длинного и сложного перечня условий, которые почти никто не читает.

Одним из потенциальных решений является простая, регулируемая система по принципу «светофора». Веб-сайт, перепродающий все персональные данные, будет помечаться красным цветом, сайт, продающий часть данных, — желтым, а при посещении «зеленого» сайта контроль над персональными данными будет в полном объеме сохраняться за потребителем. Потребители смогут принять взвешенное решение относительно того, является ли обмен, в котором задействованы их персональные данные, справедливым.

Начали появляться первые признаки того, что увеличение прозрачности и контроля приводит к более открытому обмену со стороны потребителей. В итальянском городе Тренто был проведен эксперимент, в котором сотни семей использовали открытую систему обмена. Их информация хранилась безопасным способом, и они могли контролировать, кто получал к ней доступ. Поскольку семьи доверяли этой системе, они в конечном итоге предоставляли значительно больше информации»⁵.

5. Исследование 'With Big Data Comes Big Responsibility', Harvard Business Review, ноябрь 2014 г.



Если потребители ценят конфиденциальность своих персональных данных, почему они их раскрывают?



Брюс Лайонз

Профессор экономики
Университет Восточной Англии
Великобритания

«Люди говорят, что им не нравится делиться своими персональными данными, а затем сами их разглашают. Мы размещаем все больше и больше информации о себе в социальных сетях и при этом волнуемся по поводу нарушения неприкосновенности нашей частной жизни, — отмечает Брюс Лайонз, профессор экономики из Университета Восточной Англии.

Поведенческая экономика дает некоторые возможные ответы на вопрос о том, почему люди отклоняются от рациональных решений и стандартной экономической теории, когда речь заходит о персональных данных:

Предубеждение, связанное с желанием сохранить статус-кво: люди стремятся сохранить то, что у них есть. Компании могут использовать эту неготовность к переменам с помощью своего набора опций по умолчанию. В интернете опцией по умолчанию зачастую является «поделиться».

Предубеждение, связанное с манерой подачи информации: преимущества передачи данных сообщаются сразу же, а отрицательные последствия, такие как нарушение неприкосновенности частной жизни, замалчиваются. Потребители склонны соглашаться, несмотря на испытываемый дискомфорт.

Самоуверенность: мы уверены, что не будем делиться какими-либо сведениями, если позднее мы можем пожалеть об этом. Но значительная часть информации, размещаемой в сетях Facebook и Twitter, говорит об обратном.

Предубеждение, связанное с настоящим временем: мы хотим получить быструю реакцию в виде отметок «Нравится» и «Поделиться» в социальных сетях, но не задумываемся о более долгосрочных последствиях размещения информации в Сети.

Организации хорошо знают стратегии поведения, которые они могут использовать, чтобы оказывать влияние на потребителей, но об этих стратегиях знают и регулирующие органы. Британское Управление по финансовому регулированию и надзору, например, уже отслеживает поведенческие предубеждения, чтобы предупредить эксплуатацию потребителей, а в декабре 2012 г. австралийское Министерство финансов и дерегулирования опубликовало документ, посвященный использованию поведенческих стратегий в целях оптимизации регулирования».

Где проводят черту регулирующие органы?

Организации больше не могут себе позволить думать о персональных данных задним числом. Вопросы кибербезопасности и борьбы с хакерами уже давно занимают верхние строки в повестке дня директоров по информационным технологиям. Но кибербезопасность — это не то же самое, что неприкосновенность частной жизни.

Новые правила, принятые в ЕС (Генеральный регламент о защите данных), предполагают, что при работе с данными о потребителях организации должны в первую очередь думать об их защите. После вступления этого регламента в силу в мае 2018 г. несоблюдение его положений может привести к штрафам в размере до 4% от мирового оборота.

Хотя указанный регламент, вероятно, является наиболее всеобъемлющей попыткой определить логически последовательную нормативно-правовую

базу, регулиющую неприкосновенность частной жизни, правительства по всему миру начинают уделять больше внимания этому вопросу и вводят законодательные нормы, обеспечивающие более сильную защиту потребителей — и более строгие наказания за нарушения.

Ужесточение подхода по всему миру приводит к тому, что вопросы неприкосновенности частной жизни становятся одними из наиболее актуальных для организаций с точки зрения управления рисками. В таких быстро меняющихся условиях компаниям следует подумать о разработке нового подхода к неприкосновенности частной жизни — сделать это нужно быстро, чтобы свести к минимуму риски для своего бухгалтерского баланса и репутации.



Отношение к персональным данным: мировые тенденции

США и Канада

Потребители в США и Канаде больше других беспокоятся по поводу кражи персональных данных хакерами. «Поскольку утечки данных происходят в Северной Америке почти ежедневно, неудивительно, что люди беспокоятся по поводу хакеров. Увеличение числа индивидуальных и групповых судебных разбирательств и ужесточение наказаний за счет принятия таких законодательных актов, как Генеральный регламент о защите данных, потребуют от зарегистрированных в США компаний серьезного пересмотра своих подходов к защите персональных данных», — **Дорон Ротман, КПМГ в США**

Нидерланды

Голландских респондентов мало волнует то, как организации обрабатывают и используют их персональные данные. Россия — единственная страна, где показатель степени обеспокоенности по этому поводу еще ниже. «Возможно, это объясняется голландским практичным менталитетом. С другой стороны, Нидерланды опередили вступление в силу Генерального регламента о защите данных: здесь закон, регулирующий процедуру уведомления об утечках данных и наделяющий полномочиями по наложению штрафов специальный орган, занимающийся вопросами неприкосновенности частной жизни, вступил в силу 1 января 2016 г. Увеличение штрафов уже привело к тому, что голландские организации стали быстрее информировать об утечках данных и более тщательно управлять вопросами неприкосновенности частной жизни», — **Кос Уолтерс, КПМГ в Нидерландах**

Франция

Франция — одна из тех стран, где жители в большинстве своем не согласны на сбор персональных данных государственными органами, даже с целью оказания им содействия в борьбе с терроризмом. «Принимая во внимание происходившие во Франции в прошлом трагические события, французы ценят законы о неприкосновенности частной жизни, которые были впервые приняты почти 40 лет назад. Это свидетельствует о том, что правительствам следует принимать во внимание ожидания граждан в отношении охраны их частной жизни, когда они пытаются решить некоторые из наиболее серьезных проблем современного общества», — **Винсент Маре, КПМГ во Франции**

Бразилия

Проект закона о защите персональных данных был обнародован в январе 2015 г. Он включает меры, связанные с получением согласия, обработкой и передачей персональных данных, информированием об утечках данных и предоставлением людям возможности получать доступ к своим персональным данным. Законопроект предусматривает санкции за нарушение его положений, включая штрафы и запрет на обработку персональной информации на срок до 10 лет. **Леандро Аугусто Антонио, КПМГ в Бразилии**

Италия

Италия — одна из тех стран, где большинство жителей согласны на сбор персональных данных государственными органами. «Это согласуется с опасно низким уровнем осознания итальянцами риска вторжения в частную жизнь. Анализируя полученные данные, мы можем заметить, что Италия — одна из европейских стран, активнее других использующих социальные сети, а также та страна, жители которой меньше других беспокоятся по поводу того, что будет с их персональными данными при совершении онлайн-покупок. Здесь еще многое предстоит сделать с точки зрения повышения информированности о вопросах неприкосновенности частной жизни, но, учитывая активное использование цифровых медиа итальянским обществом, это единственный выбор», — **Лука Боселли, КПМГ в Италии**

Россия

Лишь 11% российских респондентов сильно обеспокоены тем, как компании обрабатывают и используют их персональные данные. «Этот факт свидетельствует о том, что жители России не в полной мере осознают последствия утечки персональных данных. В настоящее время в России появляются правила использования персональных данных, при этом средний гражданин России не так много знает о технических аспектах и своих юридических правах в этой сфере. Кроме того, в России происшествия, связанные с неприкосновенностью частной жизни, редко освещаются в СМИ, что приводит к низкому уровню информированности населения о соответствующих проблемах», — **Илья Шаленков, КПМГ в России**

Германия

Немецкие респонденты входят в число тех, кто с наименьшей вероятностью согласится принять бесплатный фитнес-трекер от своего работодателя. «Это неудивительно, учитывая традиционное для жителей Германии нежелание делиться личной информацией. Это создает реальные проблемы для немецких компаний, начинающих работать в условиях цифровой экономики. Если им не удастся найти золотую середину в отношениях с потребителями, немецкие предприятия рискуют отстать от своих конкурентов», — **Михаэль Фалк, КПМГ в Германии**

Китай

В Китае 60% опрошенных нравится идея именной рекламы на щитах. «Хотя 60% респондентов считают нормальной персонализированную щитовую рекламу, 39% потребителей очень обеспокоены тем, как компании обрабатывают и используют их персональные данные! Жители Китая положительно относятся к использованию китайскими организациями цифровых инноваций для налаживания более тесного взаимодействия с потребителями, однако противоречие между желанием получить новые интересные продукты и доверием представляет собой реальную проблему», — **Генри Шек, КПМГ в Китае**

Япония

В целом в Японии оказался самый низкий процент желающих делиться информацией с организациями в интернете, но при этом японцы реже жителей других стран принимают меры предосторожности для защиты своих персональных данных. «Это создает интересную дилемму для японских компаний, ведущих деятельность в интернете. Но и дает им возможность добиться успеха, если им удастся выработать сбалансированный подход», — **Атсуши Тагучи, КПМГ в Японии**

Индия

«В Индии наблюдается самый высокий уровень доверия к организациям, работающим с персональными данными. В условиях развития цифровой экономики это доверие дает реальную возможность создавать стоимость на индийском рынке. Однако я полагаю, что по мере увеличения информированности населения о проблемах обеспечения неприкосновенности частной жизни доверие и ожидания индийских потребителей изменятся», — **Маюран Паланисами, КПМГ в Индии**

Малайзия

«Азиатские предприятия осуществляют крупные инвестиции в техническую революцию, при этом наблюдается быстрый рост числа новых интернет-компаний и огромные капиталовложения в цифровые и аналитические инновации. Успех будет зависеть от правильного решения возникающих у потребителей вопросов в отношении защиты персональных данных», — **Дани Мишо, КПМГ в Малайзии**

Австралия

В Австралии оказался самый низкий процент опрошенных (среди неевропейских стран), читающих политику конфиденциальности при посещении веб-сайта. «В связи с этим перед австралийскими организациями встает интересная задача. Если потребители, как правило, не читают предоставляемую им информацию, как организации могут обеспечить прозрачное взаимодействие с потребителями? Компаниям придется задуматься о новых передовых и доступных способах обеспечения такой прозрачности», — **Джасинта Манро, КПМГ в Австралии**

Новая Зеландия

Жители Новой Зеландии чаще других используют блокирующие рекламу программы для защиты персональных данных. «Новозеландцы серьезно относятся к вопросам неприкосновенности частной жизни. Организациям следует учитывать это при любом взаимодействии с покупателями и клиентами», — **Суэлла Камминг, КПМГ в Новой Зеландии**

Отношение к персональным данным: ситуация в различных отраслях

Медико-биологический сектор

«Традиционные бизнес-модели фармацевтической отрасли утратили свою жизнеспособность. В медико-биологическом секторе произошли беспрецедентные изменения в результате слияний и поглощений, перехода к персонализированной медицине, смещения акцента на ориентированные на стоимость результаты для пациентов, развития медицинских технологий и их взаимной связанности, а также расширения сотрудничества с коммерческими предприятиями и партнерами из сектора информационных технологий. Информация — основной элемент, стимулирующий разработку и поддерживающий дальнейшее функционирование этих новых бизнес-моделей. Чтобы извлечь пользу из недавнего развития технологий, мы должны выявлять, защищать и регулировать информацию».

Крис Стерлинг, руководитель Международной практики КПМГ по работе с компаниями медико-биологического сектора

Технологии

«В эпоху Интернета вещей всё, от ботинок до телевизоров, следящих за нами, когда они выключены, и копировальных устройств может быть подключено к интернету. Затраты, связанные с нарушением конфиденциальности персональных данных, могут принести организациям реальные и значительные убытки и потребовать от них проведения дорогостоящих и длительных работ по их устранению».

Гэри Матузак, руководитель Международной практики КПМГ по работе с компаниями сектора технологий, СМИ и телекоммуникаций



Потребительский сектор

«Производители потребительских товаров и компании розничной торговли обращаются к потенциальным покупателям со все более персонализированными и своевременными сообщениями. Учитывая большие объемы подробных персональных данных и поведенческой информации, которые эти компании могут получить о своих клиентах или покупателях в интернете, существует особенно высокий риск переступить черту, отделяющую приемлемое от неприемлемого. Чтобы точно понять, когда и где стоит провести границу, компаниям, производящим и продающим потребительские товары, необходимо внимательно следить как за положительными, так и за отрицательными последствиями своих рекламных кампаний».

Вилли Кру, руководитель Международной практики КПМГ по работе с компаниями потребительского сектора

Финансовые услуги

«Финансовые организации традиционно защищают активы и информацию и в качестве приоритетной задачи продолжают активно инвестировать в это. Сложности, с которыми они сталкиваются, заключаются в необходимости удостовериться в том, что те сферы, в которые они инвестируют, будут обеспечивать их клиентам ожидаемый уровень защиты. Кроме того, их инвестиции должны обеспечивать возможность эффективного и рационального управления хозяйственной деятельностью и рисками. Те, кто справится с двумя этими задачами, получат конкурентное преимущество, благодаря которому они смогут стать пользующимися доверием хранителями клиентских данных. А доступ к этим данным позволит им оказывать дополнительные услуги, связанные с идентификацией в интернете и обеспечением неприкосновенности частной жизни».

Джереми Андерсон, Руководитель Международной практики КПМГ по оказанию услуг компаниям финансового сектора и партнер КПМГ в Великобритании

Энергетика и природные ресурсы

«Сейчас энергетические компании получили доступ в дома, при этом новые технологии, такие как интеллектуальные счетчики, дают им очень ценную новую информацию о потребителях, которую они не могли получать раньше. Их основная задача — научиться создавать стоимость на основе этой информации, но при этом очень важно, чтобы эти инновационные виды деятельности не влияли на основную хозяйственную деятельность организации».

Алехандро Ривас-Васкес, руководитель Группы по оказанию услуг в области кибербезопасности компаниям энергетического сектора, КПМГ в Великобритании



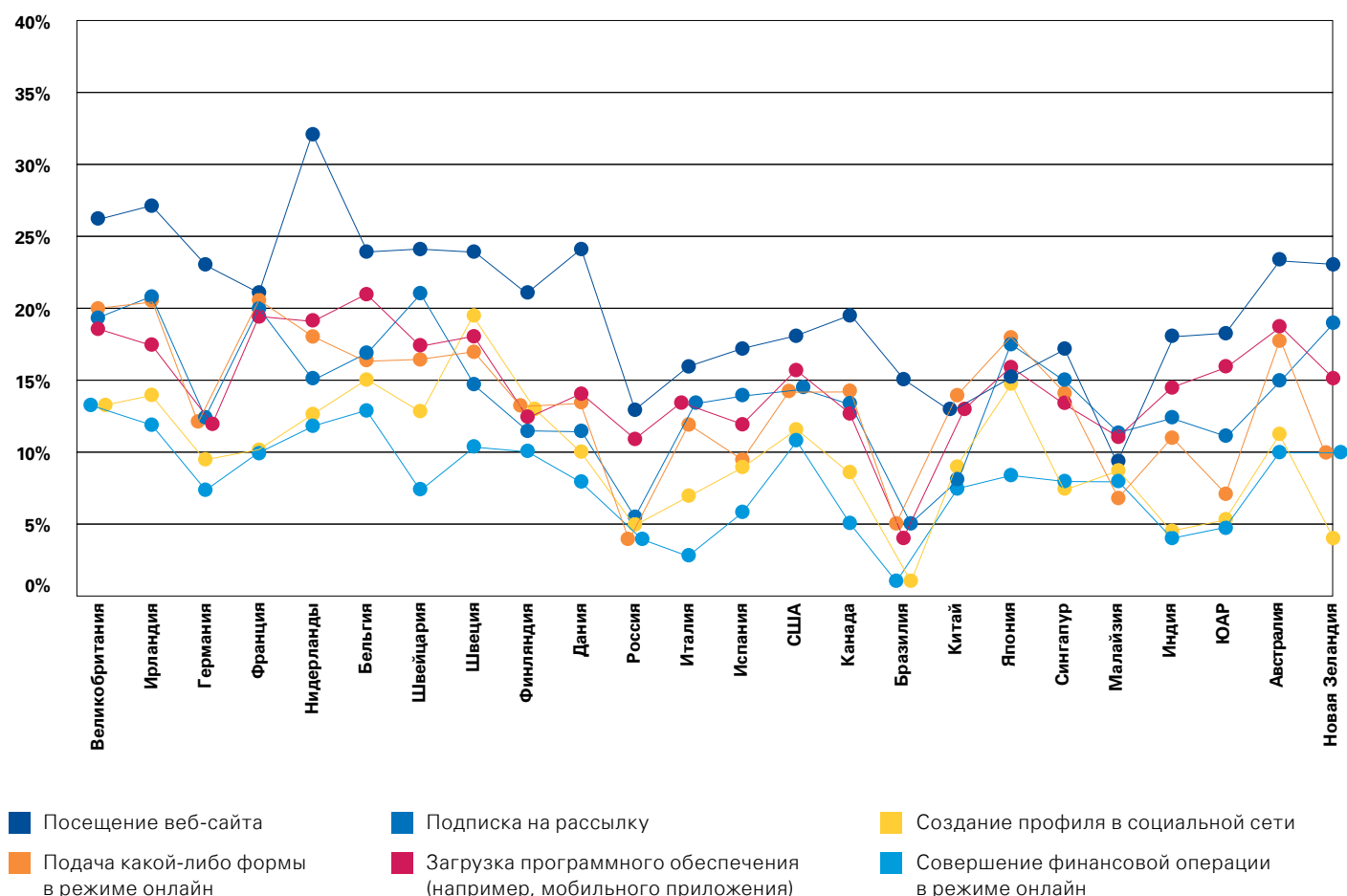
Что должны предпринять компании, чтобы выжить?

В первую очередь следует изменить отношение. То, что, возможно, было приемлемым или по крайней мере терпимым в прошлом, должно быть пересмотрено в свете более строгих международных подходов к законодательному регулированию неприкосновенности частной жизни.

Стратегия, когда компании получают согласие потребителей, озадачив их многословными юридическими формулировками и 20-страничными заявлениями об ограничении ответственности, неэффективна. Как, например, показывают результаты исследования, 57% людей по всему миру не читают или лишь бегло просматривают политику конфиденциальности, посещая различные веб-сайты. Что касается отдельных регионов, то **европейцы** читают политику конфиденциальности реже потребителей **в Северной Америке** и **Азиатско-тихоокеанском регионе (см. рис. 6)**.

Вместо этого руководящим принципом при работе с персональными данными должна быть прозрачность. Организации должны в полном объеме понимать, что они хотят делать с данными клиентов, а также где и как они собираются их хранить, а затем они должны объяснить это потребителям на простом и понятном языке.

Рис. 6. Насколько тщательно потребители читают политику конфиденциальности в указанных случаях



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

Правильный подход к соблюдению конфиденциальности

Организациям может быть сложно обеспечить прозрачность своей политики конфиденциальности, потому что они не знают, каким образом их затронут действующие или будущие нормативно-правовые акты, или же потому что они:

- не имеют политики конфиденциальности;
- собирают персональные данные нерегулярно;
- не знают, где находятся данные.

Не имея представления о том, где находятся данные, управлять ими невозможно. Точно так же, как списки клиентов, используемые в продажах и маркетинге, персональные данные передаются между отделами, занимающимися информационными технологиями, развитием бизнеса, управлением персоналом и финансами, при этом они потенциально хранятся в сотнях различных систем, которые могут быть несовместимы друг с другом.

Они могут храниться на старых серверах данных и без раздумий распространяться среди поставщиков, операторов платежных услуг, аудиторов, регулирующих органов и десятков

других организаций. Вероятно, организациям придется устранить в буквальном смысле тысячи слабых мест.

Меры по локализации данных, зачастую включаемые в новую волну мирового законодательства в сфере защиты неприкосновенности частной жизни, также создают значительные сложности для предприятий. Локализация данных — это необходимость хранить и обрабатывать данные в пределах национальных границ. Учитывая рост популярности облачных вычислений в качестве способа сокращения затрат, увеличения гибкости и повышения эффективности, нормативно-правовые акты, требующие локализовать данные, могут привести к фрагментации мирового рынка и на самом деле поставить пользователей интернета в невыгодное положение.

Организациям следует начать обсуждать вопрос неприкосновенности частной жизни на уровне советов директоров и вкладывать соответствующие ресурсы в свою стратегию работы с персональными данными, а также соответствующие системы и процессы. Те, кто этого не сделают, возможно, будут вынуждены заплатить высокую цену.

Безопасность

По сравнению с проблемой обеспечения неприкосновенности частной жизни, вопросы защиты данных представляют собой более легкую задачу для компаний. Согласно результатам исследования, в среднем 32% опрошенных заявили, что надежные системы безопасности являются наиболее эффективной мерой, позволяющей завоевать доверие, причем на некоторых крупных рынках, таких как **Франция, Малайзия и Испания**, этот показатель достиг 40% и более (см. рис. 7).

Вопросы безопасности, особенно в тех случаях, когда она нарушается, освещаются на первых полосах газет, привлекая к себе такое внимание и ресурсы, которых вопросы неприкосновенности частной жизни до сих пор редко удостоиваются.

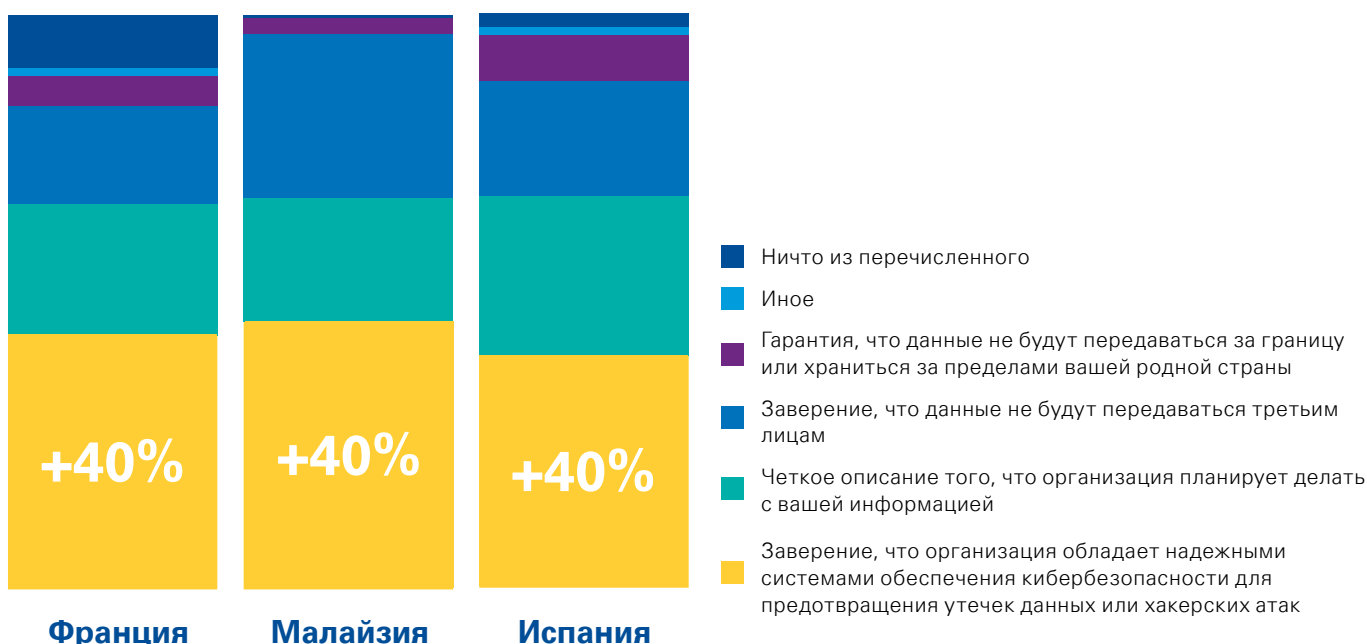
Но на самом деле безопасность — лишь один из многочисленных факторов, которые необходимо принимать во внимание при разработке комплексной системы обеспечения неприкосновенности частной жизни. В организации может быть надежная система

безопасности, но вопрос в том, как эта компания уведомляет потребителей и получает их согласие? Соблюдает ли она правила, касающиеся передачи персональных данных за границу? Готова ли она к любым планируемым нормативно-правовым требованиям? Чтобы создать надежную систему управления вопросами неприкосновенности частной жизни, необходимо проанализировать десятки других элементов, поскольку безопасность — лишь один из них.

Это важная задача мирового уровня даже для крупной группы специалистов, занимающихся исключительно вопросами неприкосновенности частной жизни (а подобным ресурсом располагают очень немногие компании).

Для ее решения потребуются инвестиции, время и знания. При этом задача усложняется нехваткой квалифицированных, опытных специалистов, поскольку это до сих пор относительно новая сфера.

Рис. 7. Наиболее эффективные способы завоевать доверие потребителей



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

Готовность работать с персональными данными

Результаты исследования показали, что в среднем 56% опрошенных «обеспокоены» или «сильно обеспокоены» тем, как компании обрабатывают и используют их персональные данные.

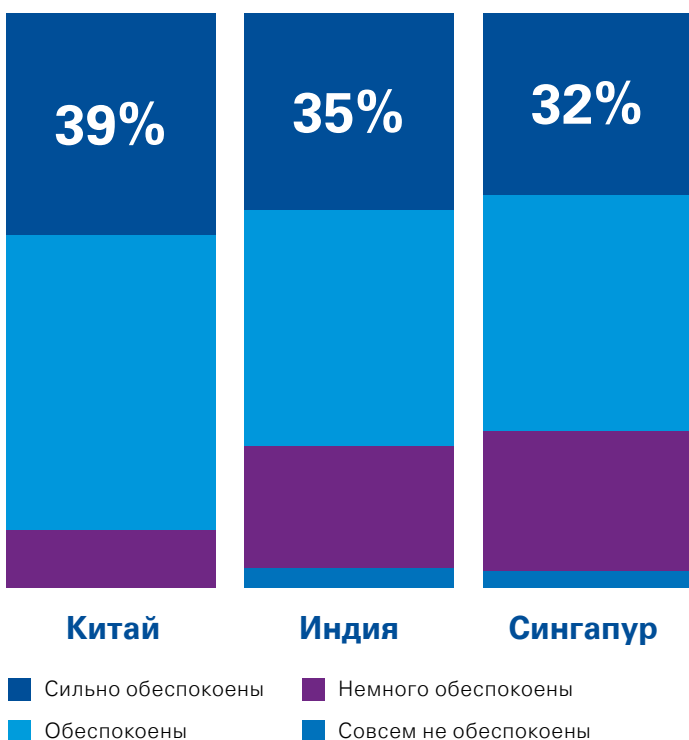
В частности, высокий уровень обеспокоенности по поводу обработки и использования персональных данных наблюдается **в Китае, Индии и Сингапуре**: 39%, 35% и 32% соответственно (см. рис. 8).

В связи с этим необходимо разработать комплексную систему, позволяющую уделять первостепенное внимание вопросам неприкосновенности частной жизни. Международной производственной компании с тысячами работников, возможно, необходимо в первую очередь сосредоточиться на данных сотрудников. С другой стороны, приоритетной задачей для предприятий, работающих с потребителями, должно стать решение любых проблем с данными о потребителях.

Если комплексная система обеспечения неприкосновенности частной жизни сделана правильно, ее следует рассматривать не как тормоз для продаж и маркетинга, а как инструмент, помогающий предприятиям лучше понять своих потребителей, усовершенствовать продукцию и услуги и привести их в соответствие с конкретными запросами покупателей.

Независимо от того, что ими движет — стремление реализовать благоприятные возможности или страх, организациям необходимо понять масштабы и сложность проблемы и действовать быстро. О неприкосновенности частной жизни необходимо помнить во время совершения любой операции с персональными данными — с момента их получения и на протяжении всего их жизненного цикла. Эта задача может показаться очень сложной, но поскольку органы власти по всему миру начинают принимать нормативные акты, регулирующие эту сферу, чем быстрее организации приступят к решению этой задачи, тем лучше.

Рис. 8. Уровень доверия к организациям, работающим с персональными данными



Источник: «Персональные данные потребителей: когда частное становится публичным?», исследование KPMG International, 2016 г.

«Результаты исследования показали, что в среднем **56%** опрошенных «обеспокоены» или «сильно обеспокоены» тем, как компании обрабатывают и используют их персональные данные».

В каком направлении будет развиваться использование персональных данных?

Персональные данные — топливо нашей будущей экономики, источник выручки и двигатель процветания. По мере того как общество начинает все острее осознавать угрозу неприкосновенности частной жизни его членов, появляются новые бизнес-модели для успокоения потребителей, причем для действующих предприятий эти модели означают как благоприятные возможности, так и сложности.

Как правило, доступность персональных данных делает возможным появление революционных технологий. Так, например, приложения, предназначенные для совместной аренды автомобилей, используют в своей работе GPS-данные о местоположении пользователей. По существу, это позволяет избежать необходимости в таком фоновом процессе, как ручной ввод информации о вашем местоположении, что позволяет сократить затраты. Но наблюдается естественное противоречие между бизнес-моделями, построенными на использовании персональных данных, и задачей обеспечения неприкосновенности частной жизни потребителей.

Поскольку 84% людей, согласно результатам исследования, считают, что они обладают недостаточным уровнем контроля за тем, каким образом организации используют их персональные данные, а о полном контроле говорят лишь 10% опрошенных, настало подходящее время для использования новых технологий, которые помогут потребителям исправить это в пользу потребителей⁶.

Люди часто соглашаются поделиться своими персональными данными, если они видят в этом очевидную пользу. Зачастую это принимает форму сниженной или нулевой цены для потребителя. Но преимущества для компаний также очевидны. Например, в секторе финансовых услуг такие новаторы, как компания Kreditech⁷ из Германии и корпорация Fair Isaac Corporation

«84% людей считают, что они обладают недостаточным уровнем контроля за использованием их персональных данных организациями».

(FICO)⁸ из США, отказываются от применения исключительно традиционного кредитного анализа, используя для оценки кредитного риска информацию о людях из интернета и профилей социальных сетей. Традиционный процесс определения критериев кредитования становится менее важным.

Для потребителей использование персональных данных означает движение в сторону «экономики взаимопомощи», где люди могут совместными усилиями собирать средства на предоставление займов, приобретение страховых полисов или осуществление инвестиций. В свою очередь, потенциальные инвесторы, прежде чем предоставить заем, проверяют персональные данные, в том числе с использованием социальных сетей.

6. Исследование Privacy and Cybersecurity: Key findings from Pew Research', Pew Research Center, 15 января 2015 г.

7. Статья в издании Financial Times: 'Kreditech: A credit check by social media', Financial Times, 19 января 2016 г.

8. Статья в издании Forbes: 'Your social media posts may soon affect your credit score', Forbes.com, 23 октября 2015 г.

Преобразование персональных данных в товар

Несложно представить время в не слишком отдаленном будущем, когда персональные данные будут объединяться и продаваться на фондовой бирже, при этом информация о более состоятельных потребителях будет стоить дороже. Компании, возможно, начнут предлагать людям продукцию и услуги по разным ценам в зависимости от объема персональных данных, которые они готовы предоставить.

Увеличение информированности потребителей

Большинство людей по-прежнему не осознают, каким объемом персональных данных о них владеют компании и как это может повлиять на их жизнь, но, возможно, ситуация начинает меняться.

Среди последних разработок можно назвать приложения, отслеживающие тех, кто следит за вами. Они разработаны американскими учеными, и их идея заключается в том, чтобы показать людям, какие именно компании следят за их онлайн-жизнью⁹. Знание такого рода вполне может показать большим группам населения, каким образом используется их информация, и привлечь внимание к любым случаям нарушения неприкосновенности частной жизни.

Брокеры данных для потребителей

Еще один вариант — «биржа идентификационных данных», где третье лицо будет управлять персональными данными потребителя от его имени. Частные инвестиционные компании рассматривают возможность предоставления услуг такого рода. Чтобы реализовать эту идею на практике, пока недостаточно инструментов и нормативно-правовых актов, но учитывая нынешние темпы изменений, недалек тот день, когда это произойдет.

Будут ли потребители по-прежнему терпимо относиться к бизнес-моделям, использующим их персональные данные, пока их будут удовлетворять получаемые ими взамен услуги? Сложно представить, что крупные поисковые системы или разработчики программного обеспечения могут потерять свои лидирующие позиции на рынке в краткосрочной перспективе, однако развитие направления услуг по обеспечению неприкосновенности частной жизни подчеркивает естественное стремление людей не расставаться со своими персональными данными.

В условиях меняющейся рыночной конъюнктуры организации должны признать, что защита данных потребителей — это не простая формальность для успокоения чрезмерно ретивых регулирующих органов. Осведомленность потребителей и рыночные ожидания уже выросли до таких размеров, что любой намек на несерьезное отношение к вопросам защиты данных и неприкосновенности частной жизни может подорвать не только доверие потребителей, но и основополагающую финансовую стабильность самого предприятия.

Полезная информация для руководителей: использование личных брокеров данных



Ахилеш Тутея
Соруководитель Международной группы по вопросам кибербезопасности KPMG International

«Данные не исчезают, но их можно спрятать. Поэтому не сложно представить появление компаний, предлагающих маскирование бренда в режиме онлайн — услугу, помогающую скрыть вашу личность или произвести ее «ребрендинг». Это следующий логический шаг после появления менеджеров, управляющих личным брендом в интернете (а такие специалисты уже существуют).

Кроме того, компании могут столкнуться с ростом популярности личных брокеров, напрямую предлагающих свои услуги потребителям. Личный брокер данных может выступать в качестве посредника между лицом и организациями, желающими использовать его персональные данные. Представьте, что у вас сломалась машина. И для организации эвакуации и ремонта автомобиля вы можете связаться со своим брокером данных, которому уже известно ваше местоположение, марка автомобиля, а также регистрационные данные и банковские реквизиты. Благодаря модели с использованием брокера данных у потребителей есть одно контактное лицо, имеющее в распоряжении всю необходимую информацию и способное решить проблему от начала до конца.

9. Статья в издании New Scientist : 'Privacy apps to help fight back against companies that track you', New Scientist, 25 ноября 2015 г.

Готовы ли вы к тому, что контроль за неприкосновенностью частной жизни усилится?

Органы власти по всему миру усиливают внимание к вопросам неприкосновенности частной жизни, но при этом немногие организации готовы к тому, что их ждет. Штрафы за ненадлежащую обработку, сбор и использование организациями данных о потребителях, которые когда-то исчислялись десятками тысяч, могут увеличиться до сотен миллионов или даже миллиардов.

Многие отраслевые специалисты ожидают, что регулирующие органы захотят как можно скорее ввести новые требования в силу, чтобы донести свою точку зрения, поэтому организациям необходимо быстро определить, где проходит граница, отделяющая приемлемое от неприемлемого, и оперативно принять меры к тому, чтобы эту границу не пересекать.

Семь шагов, чтобы подготовиться к ужесточению контроля за неприкосновенностью частной жизни

Шаг 1

Объясните всем заинтересованным лицам, что неприкосновенность частной жизни значит для вашей организации.

Шаг 2

Оцените уровень риска, связанного с нарушением неприкосновенности частной жизни, которому подвержена ваша организация.

Шаг 3

Проанализируйте ожидания физических лиц, данные которых вы обрабатываете, и разработайте стратегию работы с персональными данными, соответствующую их ожиданиям.

Шаг 4

Оцените уровень зрелости вашей организации в вопросах обеспечения неприкосновенности частной жизни и разработайте четкую стратегию, соответствующую вашему целевому уровню зрелости в указанных вопросах и представлениям ваших потребителей о приемлемых и неприемлемых действиях с персональными данными.

Шаг 5

Разработайте надежный план снижения рисков, связанных с неприкосновенностью частной жизни, и достижения поставленных целей.

Шаг 6

Реализуйте ваш план. Создайте устойчивые структуры, которые помогут управлять рисками, связанными с неприкосновенностью частной жизни, обеспечат соблюдение нормативно-правовых требований, а также послужат прочной основой для гибкого использования персональных данных с целью создания стоимости для организации, ваших клиентов и ваших работников.

Шаг 7

Контролируйте и повторяйте процесс.

Как и чем может помочь КПМГ?

Специалисты КПМГ по вопросам неприкосновенности частной жизни оказывают поддержку клиентам по всему миру в решении сложных задач в этой сфере, от устранения отдельных проблем, характерных для конкретных организаций, до комплексной разработки программ соблюдения нормативно-правовых требований для сложных отраслей с большим объемом государственного регулирования.

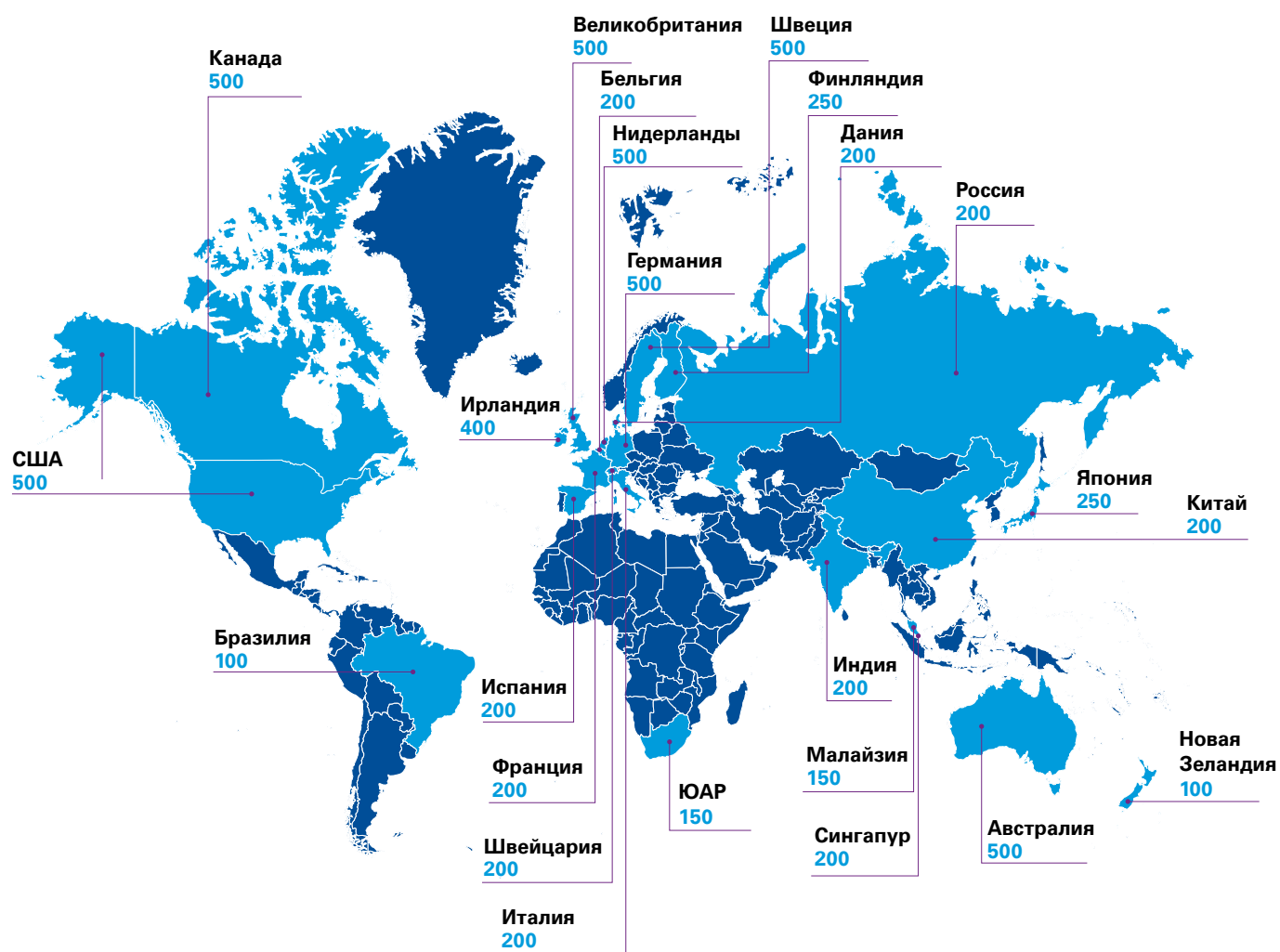
Наши специалисты обладают большим опытом оказания содействия клиентам в решении проблем, связанных с риском нарушения неприкосновенности частной жизни, при этом они используют структурированный и гибкий подход, позволяющий удовлетворить потребности самых разнообразных организаций. Глобальные масштабы деятельности сети фирм КПМГ позволяют эффективно решать задачи на разных территориях, при этом находясь в одной стране.

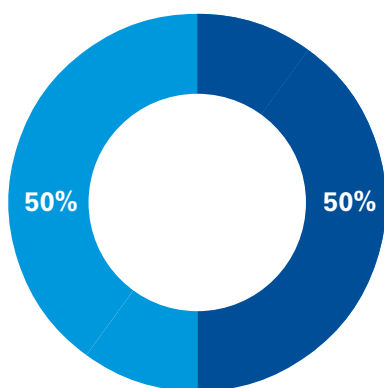
Фирмы – члены сети КПМГ часто привлекаются для оказания, в частности, следующих видов услуг:

- **Оценка:** независимая оценка риска, связанного с неприкосновенностью частной жизни, и разработка мер его снижения.
- **Разработка:** разработка программ соблюдения нормативно-правовых требований в области обеспечения неприкосновенности частной жизни.
- **Реализация:** реализация надежных процессов, правил и средств контроля в области обеспечения неприкосновенности частной жизни.
- **Стратегия:** разработка прагматичных стратегий обеспечения неприкосновенности частной жизни и получение одобрения и поддержки со стороны высшего руководства.
- **Оперативная поддержка:** оказание постоянной поддержки клиентам, чтобы помочь им в эксплуатации системы обеспечения неприкосновенности частной жизни.
- **Мониторинг:** оказание помощи клиентам в обслуживании и отслеживании функционирования режимов обеспечения неприкосновенности частной жизни.

Информация об исследовании

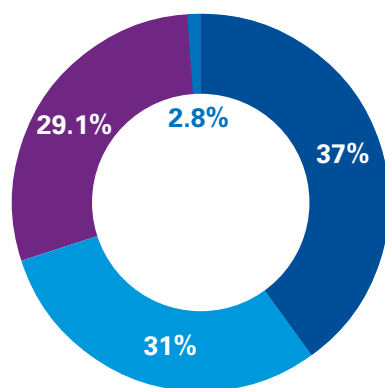
6 900 респондентов в 24 странах:





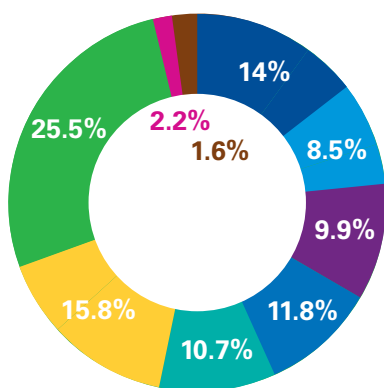
Укажите ваш пол

■ Мужской	(3,451)
■ Женский	(3,449)
Итого	(6,900)



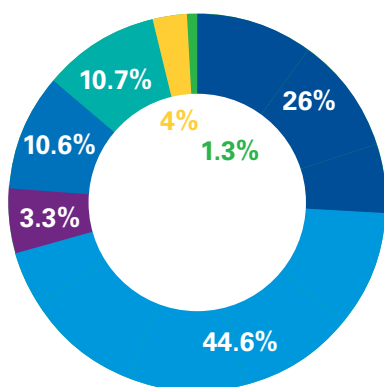
Сколько вам лет?

■ Поколение Миллениума	(2,555)
■ Поколение X	(2,142)
■ Послевоенное поколение	(2,009)
■ 71+	(194)
Итого	(6,900)



Какой из нижеперечисленных вариантов лучше всего описывает жизненный этап, на котором вы находитесь?

■ Молодой взрослый, не имеющий детей	(965)
■ Молодая семья, имеющая детей дошкольного возраста	(585)
■ Семья среднего возраста, имеющая детей 5-9 лет	(683)
■ Семья старшего возраста, имеющая детей 10-16 лет	(811)
■ Иждивенцы старшего возраста, имеющие детей старше 16 лет, которые живут с родителями	(738)
■ Семья, где дети живут отдельно	(1,090)
■ Взрослый(-е) без детей	(1,762)
■ Иное (пожалуйста, уточните)	(155)
■ Предпочитаю не отвечать на данный вопрос	(111)
Итого	(6,900)



Какой из нижеперечисленных вариантов лучше всего вас описывает?

■ Не состою (и никогда не состоял(а)) в браке	(1,792)
■ Состою в браке	(3,077)
■ Состою в однополном браке	(230)
■ Живу с партнером	(729)
■ Вдова/вдовец, в разводе или проживаю отдельно от жены/мужа	(701)
■ Состою в отношениях, но проживаем раздельно	(278)
■ Иное	(93)
Итого	(6,900)

Контакты

Марк Томпсон

Руководитель Международной группы по вопросам использования и защиты персональных данных
KPMG International
E: mark.thompson@kpmg.co.uk

Грег Белл

Соруководитель Международной группы по вопросам кибербезопасности
KPMG International
E: rgregbell@kpmg.com

Ахилеш Түтея

Соруководитель Международной группы по вопросам кибербезопасности
KPMG International
E: atuteja@kpmg.com

Дорон Ротман

КПМГ в США
E: drotman@kpmg.com

Кос Уолтерс

КПМГ в Нидерландах
E: wolters.koos@kpmg.nl

Винсент Маре

КПМГ во Франции
E: vmaret@kpmg.fr

Леандро Аугусто Антонио

КПМГ в Бразилии
E: lantonio@kpmg.com.br

Лука Боселли

КПМГ в Италии
E: lboselli@kpmg.it

Джасинта Манро

КПМГ в Австралии
E: jacintamunro@kpmg.com.au

Суэлла Камминг

КПМГ в Новой Зеландии
E: smcumming@kpmg.co.nz

Илья Шаленков

КПМГ в России
E: ishalenkov@kpmg.ru

Михаэль Фалк

КПМГ в Германии
E: mfalk@kpmg.com

Генри Шек

КПМГ в Китае
E: henry.shek@kpmg.com

Атсуши Тагучи

КПМГ в Японии
E: atsushi.taguchi@jp.kpmg.com

Маюран Паланисами

КПМГ в Индии
E: mpalanisamy@kpmg.com

Дани Мишо

КПМГ в Малайзии
E: danimichaux@kpmg.com.my

Информация, содержащаяся в настоящем документе, носит общий характер и подготовлена без учета конкретных обстоятельств того или иного лица или организации. Хотя мы неизменно стремимся представлять своевременную и точную информацию, мы не можем гарантировать того, что данная информация окажется столь же точной на момент получения или будет оставаться столь же точной в будущем. Предпринимать какие-либо действия на основании такой информации можно только после консультаций с соответствующими специалистами и тщательного анализа конкретной ситуации.

© 2016 КПМГ. КПМГ означает АО «КПМГ», ООО «КПМГ Налоги и Консультирование», компании, зарегистрированные в соответствии с законодательством Российской Федерации, и КПМГ Лимитед, компанию, зарегистрированную в соответствии с Законом о компаниях (о. Гернси) с изменениями от 2008 г. Все права защищены.

KPMG и логотип KPMG являются зарегистрированными товарными знаками или товарными знаками ассоциации KPMG International.

Переведено с разрешения KPMG International.

kpmg.ru



kpmg.com/app

