Сложность в деталях

новый Закон ЕС о защите данных обещает отдать контроль в руки пользователей

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

Через четыре года после внесения на рассмотрение проекта Европейская Комиссия наконец пришла к согласию в отношении Общего регламента о защите данных (GDPR) и организации во всем мире ожидают, что в скором времени они узнают его подробности.

Сторонники соглашения в Брюсселе (Бельгия) считают, что этот закон отвечает эпохе цифровых технологий и что его главная задача позволить пользователям контролировать свои данные и гармонизировать правила получения или сохранения частных данных в границах 28 стран-участниц блока. GDPR призван обновить устаревший закон о конфиденциальности от 1995 года, который был составлен за три года до появления Google. В попытке угнаться за новыми технологиями и решить стоящие перед европейским сообществом проблемы обеспечения конфиденциальности Европейский Парламент пришел к согласию в отношении принятого в декабре 2015 года Закона Европейского Союза о защите данных, который в ближайшее время будет представлен широкой публике и вступит в силу в 2018 году.

Майкл Вандерпул, CISA, CISSP
Аудитор в сфере ИТ компании Credit Suisse в г. Вроцлав (Польша). Более 12 лет работает в сфере информационных технологий, главным образом в том, что касается информационной безопасности, рисков и соблюдения нормативно-законодательных требований. Благодаря знаниям и опыту работы в технологическом и финансовом секторах Вандерпул проводил оценки рисков в ИТ, аудиты и проверки контрольных мер для международных корпораций и банков на базе международных методологий и стандартов таких, как COBIT®, COSO and ISO 27001. До прихода в Credit Suisse Вандерпул работал в UBS и IBM.

Поскольку, в соответствии с описанием, новое законодательство касается всех организаций, которые предоставляют товары или услуги в любой точке ЕС, то, вряд ли, можно недооценить масштаб и значение нового регламента. GDPR – это не просто новая версия закона 1995 года, это абсолютно новый свод правил, которые организациям придется быстро понять, внедрить и соблюдать или же их будут ожидать серьезные финансовые последствия.

Главная цель нового регламента состоит в том, чтобы обеспечить пользователям возможность контролировать сведения о них, хранящиеся в Интернете. «Новое законодательство вернет пользователям право принимать решения, касающиеся своих личных данных» говорит Ян Филипп Альбрехт, член инициативной парламентской группы Европейского Парламента.[1] Одним из важных аспектов нового законодательства является популярное право быть забытым, существующее в Европе с 2006 года, которое позволяет пользователям требовать удаления своих фотографий, видео или персональных сведений из Интернет-записей, в которых они могут быть найдены поисковыми системами. Это право изначально было внедрено для поисковых систем, но теперь оно будет распространяться на веб-службы, включая веб-сайты социальных медиа такие, как Facebook.

Право знать, что личные данные были скомпрометированы, также является популярным компонентом GDPR и требует от организаций в течении 72 часов сообщать центральным органам власти о любых нарушениях законодательства о защите данных, которые представляют риск для владельцев данных. Пользователи, в отношении которых высок риск нарушения, также должны быть уведомлены об этом как можно раньше, хотя двусмысленность этого речевого оборота вызывает скептические замечания в отношении применимости директивы.

Критики нового законодательства о защите данных выражают недовольство целым рядом статей. Одним из наиболее противоречивых аспектов является наказание за несоблюдение – за нарушение требований любой из статей GDPR организациям грозят штрафы в размере до 4% их годового глобального дохода. «Столь высокие

санкции лишают мотивации бизнесменов и инвесторов» говорит Дэвид Хоффман, руководитель глобального подразделения по вопросам конфиденциальности компании Intel.[2] Скептики уже назвали закон новым испытанием для Силиконовой долины и считают, что он усилит конфликт с такими технологическими гигантами, как Google, Facebook и Microsoft.

Также вызывает беспокойство двусмысленность в некоторых рекомендациях и формулировках GDPR. Например, некоторым организациям рекомендуется нанимать сотрудника, ответственного за защиту данных. В соответствии с новым законом малые и средние предприятия освобождаются от обязанности назначать сотрудника, ответственного за защиту данных в тех случаях, когда обработка данных не является их основной деятельностью. Освобождаются ли в таком случае компании, занимающиеся проверкой сведений о кандидатах на работу? Именно эти организации зачастую становятся мишенью тех, кто ворует данные, поэтому крупномасштабные нарушения в таких компаниях не такое уж редкое явления, однако, если определить основную деятельность такого предприятия, как «управление персоналом» или «подбор кадров», то оно может требовать себе освобождения даже, если хранит ценные персональные сведения, иногда на постоянной основе. «Юридическая неопределенность и большие штрафы-опасный коктейль» отмечает Аллан Соренсен[3], член совета правления в Европе Interactive Advertising Bureau. Большие штрафы с учетом глобальных операций за нарушение законодательства в сочетании с (порой) нечеткими формулировками наводят некоторых на мысль о том, что данный закон направлен не столько на защиту данных пользователей, сколько на попытки ЕС «урвать» еще немного денег у Google. В ответ на это сторонник GDPR Ян Филипп Альбрехт утверждает, что единственные, кто выиграет от того, что принятие этого закона будет постоянно откладываться, – это крупные компании из Силиконовой долины.

> **“Довольно много заинтересованных лиц попадают под прицел GDPR.”**

Медицинские исследовательские организации выступают против закона, заявляя, что это замедлит или даже остановит текущие исследования с использованием данных. Свыше 50 патентных организаций и благотворительных организаций, занимающихся медицинскими исследованиями, написали членам Европейского Парламента, выразив обеспокоенность в связи со слишком сильными ограничениями в законах о защите данных. Некоторые организации заявляют, что изменения к закону будут нерабочими в лучшем случае или же незаконными – в худшем, особенно для крупномасштабных проектов.[4]

Несмотря на то, что многие медицинские исследовательские организации удовлетворены последними изменениями в формулировке GDPR, все равно довольно много заинтересованных лиц попадают под его прицел. Даже у организаций, делающих первые попытки привести свою работу в соответствие с новым законодательством, хлопот по горло. Каждая из 28 стран-участниц блока будет самостоятельно интерпретировать этот регламент ЕС и в некоторых случаях сможет воспользоваться некоторой свободой в трактовке при формулировке своего фактического законодательства. Например, минимальный возраст, с которого ребенок может пользоваться социальными сетями без согласия родителей, должен определяться между 13 и 16 годами, но каждая страна вправе установить свой возраст.

Ранее заявленная цель, заключающаяся в разработке принципа «одного окна» (one-stop shop), т.е. единого центра для обслуживания всех жалоб на компанию, подразумевала, что независимо от основного места расположения компании в ЕС, именно регулирующий орган этой страны будет заниматься разбором жалобы. Тем не менее, в связи с озвученными сомнениями, теперь регулирующему органу любой страны разрешается разбирать жалобу в зависимости от места проживания заявителя и места подачи жалобы. Как сказал Йоханн Каспар, глава органа по защите данных города Гамбурга (Германия): «Механизм, изложенный в законодательстве о защите данных устанавливает гипербюрократическую процедуру, которая приведет к еще более сложным и долгим процедурам».[5]

Доступ к собственным данным позволит пользователям видеть, какие именно данные сохраняются веб-сайтом и как они используются. Право переносить данные (многие критики считают его бессмысленным) позволяет пользователям загружать персональные данные и предпочтения с целью импортировать и использовать на другом веб-сайте. Право переносить данные содержит противоречия и многие считают, что это не только не упрощает защиту данных, но и не

имеет отношения к данному регламенту. Это право уже реже упоминается в последних кратких изложениях регламента и многие ожидают, что его совсем уберут из окончательной формулировки текста. По одному сценарию в соответствии с этим требованием клиенты, совершающие покупки на веб-сайте, должны иметь возможность загрузить свои предпочтения и выложить их на веб-сайт конкурента. В зависимости от категорий, иерархий и номенклатуры продукции в каждом веб-магазине этот процесс, который может казаться очень простым в стенах Парламента, создает реальные барьеры для архитекторов процессов, и критики считают, что он никоим образом не соответствует основной цели законодательства о защите данных пользователей.

Для иллюстрации требования о переносимости данных представьте себе торгующую пиццей компанию «А», которая принимает заказы через Интернет. Клиенты заполняют профиль в Интернете, в котором содержится адрес, телефон и история заказов, чтобы можно было быстрее и эффективнее организовать очередную доставку. Клиент Джон Смит звонит и просит предоставить ему его профиль и историю заказов, потому что он хочет заказать пиццу у компании «В». В соответствии с новым регламентом эта информация должны быть ему отправлена. Добавляет ли этот процесс ценности торгующей пиццей компании «А»? Способствует ли он защите данных Джона Смита? И, за исключением случая, когда предложения компании «В» полностью идентичны предложениям компании «А», история заказов не очень поможет компании «В» при принятии первого заказа. При этом процесс подвергает риску данные Джона Смита (из-за дополнительной пересылки информации по электронной почте) и создает дополнительную нагрузку для компании «А», которая в соответствии с этим новым регламентом обязана предоставлять услугу по предоставлению данных (не приносящую дохода) своим бывшим клиентам.

Технологические компании уже не первый раз сталкиваются с проблемами при соблюдении директив Европейской Комиссии. С момента публикации в 2012 году Статьи 17 Регламента о защите данных, технологические компании пытаются соблюдать требование о праве быть забытым и одновременно предоставлять своим пользователям положительный опыт взаимодействия в Интернете. Например, компания eBay пытается внедрить строгое требование о необходимости немедленно удалять данные пользователей, что безумно трудно из-за количества баз данных, в которых эти данные хранятся.

Также сомнительной является практика с использованием профилей пользователей, которая широко распространена в сети и позволяет веб-сайтам собирать и разбивать на категории информацию о своих посетителях, с целью сделать пользование веб-сайтом более удобным и демонстрировать более релевантную рекламу. Помимо рекламы, эта технология используется страховыми компания для отслеживания и вознаграждения безопасного вождения и сайтами социальных сетей для распознавания и проставления меток на фотографиях, на которых изображены лица их пользователей. Теперь им придется спрашивать разрешения для каждого случая применения, а всем компаниям придется раскрывать данные каждому посетителю веб-сайта:

- Почему сведения о пользователях собираются в профиль
- В соответствии с какими категориями(«корзинами») они хранятся
- У кого есть доступ к этим данным
- Логика, которая применяется для определения этого
- Последствия такой обработки данных

Несмотря на то, что некоторые из этих требований уже довольно часто указывают в формулировках отказов от ответственности, типа: «Мы используем сведения о вас для того, чтобы сделать процесс покупки еще более удобным», требуемое раскрытие фактического логического алгоритма является принципиально новым. Исполнительный директор Центра по проблемам защиты личных данных и технологиям при юридическом центре Джорджтаунского университета (штат Вашингтон, США) сказал: «В настоящее время значительная часть нашей жизни в сети определяется абсолютно непрозрачными алгоритмами. Поэтому право доступа к «логике», лежащей за обработкой данных, могло бы стать ощутимым шагом вперед в открытии этого черного ящика». Технологические компании, такие как Google, часто считают свои алгоритмы коммерческой тайной. Многие считают раскрытие конкретных логических формул плохо замаскированной попыткой Европейской Комиссии увидеть изнанку работы этих компаний.

Территориальное применение GDPR остается одним из наиболее противоречивых пунктов. В соответствии с заявлением о том, что данный регламент будет распространятся на любую организацию, предоставляющую свои товары и услуги любому субъекту в ЕС, то Европейский Союз вскоре сможет контролировать Интернет. Такие популярные веб-сайты, как Google и Facebook либо должны будут предлагать европейским клиентам отдельные условия, либо вносить изменения в свои услуги по всему миру, чтобы соблюсти эти требования. А поскольку единичное нарушение

Enjoying this article?

- **Читать *Keeping a Lock on Privacy: How Enterprises Are Managing Their Privacy Function* (*«Личные данные* *под замком: Как предприятия управляют функцией защиты личных данных»).*** *www.isaca.org/2015-privacysurvey-*
- **Learn more about, discuss and collaborate on privacy/data protection in the Knowledge Center.** *www.isaca.org/topic-privacy-data-protection*

этого законодательства грозит штрафом в размере 4% от дохода (для компании Google в настоящее время эта цифра составляет 3 млрд долларов США), то в ближайшие месяцы компаниям придется принимать трудные решения.

Многие критики считают, что регламент совершенно не справился со своей целью, заявленной как «укрепление прав на защиту личных данных и активизация цифровой экономики ЕС». Несмотря на то, что некоторые части регламента позволяют эффективно решать проблемы обеспечения защиты личных данных, другие его элементы безумно дороги и трудно исполнимы, что вынудит технологические компании в ближайшие месяцы принимать трудные решения в отношении своих европейских клиентов. Даже те, кто для соответствия новому законодательству примет решение внести изменения в свои услуги, в ближайшие 24 месяца вероятнее всего столкнутся с серьезными трудностями. «Масштабность изменений, внесенных в законодательство ЕС о защите личных данных, повлечет за собой непредсказуемые последствия для бизнеса и любой компании, которая владеет или использует личные данные, как в ЕС, так и за его пределами» объясняет Стюард Рум, директор подразделения по защите личных данных компании PwC, «Большинство компаний будут шокированы масштабом новых правил и тем, количеством работы, которую придется провести до того, как этот закон вступит в силу через два года, – это очень маленький срок, учитывая размах требуемых внутренних изменений».

Как и со многими постановлениями Европейского Союза, данный регламент теперь должен быть дополнительно рассмотрен и изучен после того, как в ближайшие месяцы 28 стран-участниц блока внесут отдельные требования в национальное законодательство. Так как регламент GDPR должен вступить силу в 2018 году, не трудно представить, что это может случится намного позже, если отдельные страны-участницы не смогут прийти к согласию по поводу внедрения и применения этих правил.

В частности, любопытно посмотреть, как этот регламент будет приниматься в Ирландии, поскольку Ирландия является европейской базой для многих иностранных технологических компаний. В 2013 году критика регламента президентом Ирландии в основном сводилась к тому, что при составлении регламента практически не применялся подход, основанный на оценке рисков. Ирландцы хотели ослабить регулирование там, где фактический риск был ниже. Ирландский президент также выразил озабоченность «потребностями микро-, малых и средних предприятий (SMEs)».”[7]

Таким образом, поскольку 28 стран ЕС в ближайшие недели получат полный текст проекта регламента, никого не удивит возникновение новых дебатов по поводу GDPR, изначально предложенных еще в 2012 году. В общем, все сводится к деталям, а в деталях, как известно, кроются неприятные сюрпризы.

Примечания

1 Новости Европейского Парламента, New EU Rules on Data Protection Put the Citizen Back in the Driving Seat, («Новый регламент ЕС о защите данных возвращает право управления гражданам»), пресс-релиз, 17 декабря 2015 года, www.europarl.europa.eu/news/en/newsroom/ 20151217IPR08112/New-EU-rules-on-dataprotection-put-the-citizen-back-in-the-driving-seat

2 Деловые новости от Dow Jones, (“EU Privacy Law Has Broad Implications” («Подводные камни закона ЕС о конфиденциальности»), Nasdaq, 17 декабря 2015 года, www.nasdaq.com/article/eu-privacy-law-hasbroad-implications-20151217-00441

3 Dwoskin, E.; “EU Data-Privacy Law Raises Daunting Prospects for U.S. Companies” («Закон ЕС о защите личных данных открывает перед американскими компаниями неприглядные перспективы»), The Wall Street Journal, 16 декабря 2015 года, www.wsj. com/articles/eu-data-privacy-law-raises-daunting-prospects- for-u-s-companies-1450306033

4 Европейский парламент, стенограмма дебатов, Страсбург, Франция, 11 марта 2014 года, www.europarl.europa.eu/sides/getDoc.do?type =CRE&reference=20140311&secondRef=ITEM-013&language=EN&ring =A7-2013-0402

5 Fioretti, J.; “EU Data Protection Reform May Promise More Than it Delivers” («Реформа ЕС в сфере защиты данных – много обещаний, мало дела»), Reuters, 5 января 2016 года, www.reuters.com/article/us-eudataprotection-idUSKBN0U41CQ20160105

6 Новости BBC, ”EU Data Laws Threaten Huge Fines” («Законодательство ЕС о защите данных грозит огромными штрафами»), 16 декабря 2015 года, www.bbc.com/news/ technology-35110909

7 Hunton & Williams, ”Irish Presidency Reports on Progress of the Proposed EU Regulation” («Ирландский президент о ходе разработки предложенного регламента ЕС») Huntonprivacyblog.com, 26 марта 2013 года, https:// www.huntonprivacyblog.com/2013/03/26/irishpresidency-reports-on-progress-of-the-proposedeu-regulation/