Russian

Защита персональных данных от кражи: практические рекомендации для бизнесов

Мы уверены, что вы заботитесь об интересах своих клиентов. Защита личной информации клиентов от кражи — это не просто правило деловой этики, но и требование закона. Департамент по делам потребителей (DCA) г. Нью-Йорка предлагает вашему вниманию общий обзор законодательства и передового опыта в этой сфере, с тем чтобы вы могли удовлетворить требования, предъявляемые как вашими клиентами, так и федеральным или местным законодательством (либо законами штатов). Несоблюдение этих требований может привести к нарушению лицензионного законодательства или закона о защите прав потребителей г. Нью-Йорка.

Знакомство с законодательством

Программы по защите от кражи персональных данных. С ноября 2009 года кредитно-финансовые учреждения должны иметь действующие «программы по защите от кражи персональных данных», оформленные в письменном виде. Эти программы должны описывать, каким образом кредитно-финансовые учреждения определяют и выявляют «индикаторы потенциальной опасности» (так называемые «красные флажки»), связанные с характерной моделью или методами поведения либо конкретной деятельностью, которые могут указывать на кражу личных сведений, а также как они на них реагируют. Для получения более подробной информации см.:

- Fair and Accurate Credit Transactions (FACT) Act of 2003, (FACT (Закон о добросовестных и достоверных кредитных операциях) от 2003 года), Положение об индикаторах потенциальной опасности: 16 CFR 681.2

Утилизация записей. Утилизация записей на бумажных и цифровых носителях с информацией о клиентах должна осуществляться должным образом. Для записей на бумажных носителях приемлем метод уничтожения бумаг посредством их измельчения. Для безвозвратного удаления данных с компьютеров следует использовать утилиты для полного уничтожения данных на накопителях — простое удаление данных через «корзину» в данном случае недостаточно. Для получения более подробной информации см.:

- New York City Administrative Code § 20-117 (g) (Административный кодекс г. Нью-Йорка, § 20-117 (g))
- New York State General Business Law Article 26 § 399-H (Section GBS) (Общий закон о предпринимательской деятельности штата Нью-Йорк, статья 26, § 399-H (раздел GBS))
- Federal Trade Commission Disposal Rule, (Положение об утилизации Федеральной торговой комиссии США), 16 CFR, часть 682

Утечка информации. Если вам станет известно о несанкционированном доступе к информации о клиентах, вы должны предупредить об этом пострадавших клиентов и компетентные органы, включая Департамент по делам потребителей. Для получения более подробной информации см.:

- New York City Administrative Code § 20-117 (Административный кодекс г. Нью-Йорка, § 20-117)
- New York State Information Security Breach and Information Act, (Закон штата Нью-Йорк о нарушении информационной безопасности) New York State Technology Law § 208 (Section STT) (Закон о технологиях штата Нью-Йорк, § 208 (раздел STT))

Правила конфиденциальности. Все финансовые учреждения должны разработать правила защиты конфиденциальности частной информации и ознакомить с этими правилами своих клиентов. Согласно законодательству, понятие «финансовые учреждения» в широком смысле включает компании, предлагающие физическим лицам финансовые продукты или услуги, такие как кредиты, финансовые или инвестиционные консультации, страхование. Сюда также относится предпринимательская деятельность, непосредственно связанная с какими-либо финансовыми операциями и сделками (например, банковская) или с оказанием содействия при осуществлении подобных операций и сделок, к примеру, это может быть обработка платежных поручений, инкассирование чеков, посредническая деятельность при предоставлении кредитов (например, агенты по продаже подержанных автомобилей, мебельные магазины и т.п.), агентская деятельность по взысканию долгов, оформление налоговой документации и т.д. Для получения более подробной информации см.:

- Gramm-Leach-Bliley (GLB) Act (GLB (Закон Грэмма-Лича-Блайли))
- Federal Trade Commission Safeguards Rule, (Положение о безопасности Федеральной торговой комиссии США), 15 U.S.C.,§ 6801-6809

Платежные квитанции. Все коммерческие предприятия, принимающие платежи посредством кредитных карт, должны убирать из платежных квитанций клиентов дату окончания срока действия кредитной карты и номер кредитной карты, за исключением последних пяти цифр. Для получения более подробной информации см.:

- FCRA (Закон об объективной кредитной отчетности), § 605 (g)
- Общий закон о предпринимательской деятельности штата Нью-Йорк, статья 29-A, § 520-a (раздел GBS)

Передовой опыт

Протоколы системы защиты. Проверьте, как ваша организация обеспечивает защиту информации о клиентах, — а именно: где хранится эта информация и кто имеет к ней доступ — и внесите необходимые изменения в протоколы для повышения уровня ее зашиты. Обеспечьте необходимый уровень подготовки персонала, чтобы сотрудники понимали правила компании о защите конфиденциальности личной информации клиентов и могли реализовывать ее положения на практике.

Проверка идентификационных документов. Если клиенты производят платежи с помощью кредитных карт, следует запрашивать у них предъявления идентификационных документов. При наличии подозрения относительно проводящейся операции при помощи украденной кредитной карты необходимо уведомить службу обработки кредитных карт о том, что вступает в действие «код 10». Данная фраза предназначена для того, чтобы предупредить компанию, проводящую операции по кредитным картам, о потенциальной опасности, связанной с кражей персональных данных.

Сбор меньшего количества информации. Собирайте только ту информацию, которая необходима для проведения операции, и храните ее, пока вы в ней нуждаетесь. Чем меньше информации о клиентах у вас хранится, тем меньше вам приходится тратить усилий на ее защиту.

Ограничение доступа. Примите меры, чтобы ограничить общий или служебный доступ к документам, содержащим идентифицирующую клиентскую информацию, таким как заявки или копии квитанций по операциям с кредитными картами. Место для хранения, снабженное замком, обеспечивает хорошую защиту.

Обеспечение безопасности компьютеров. Установите на компьютеры антивирусное программное обеспечение и программные средства сетевой защиты и регулярно их обновляйте. Проследите за тем, чтобы во время простоя компьютеров запускались защищенные паролем экранные заставки.

Обеспечение надлежащих мер безопасности при работе в режиме онлайн. Ваш ИТ-менеджер должен быть в курсе новых проблем или вопросов, относящихся к работе в онлайновом режиме. На веб-сайте Федеральной торговой комиссии США **(ftc.gov)** вы сможете найти рекомендованные ресурсы для обновления соответствующих технологий.Воспользуйтесь виртуальными планировщиками для малого бизнеса, предоставляемыми Федеральной комиссией связи США **(**по адресу: **fcc.gov/cyberplanner),** для разработки специализированного плана по обеспечению информационной безопасности вашей компании.

NYC
Bill de Blasio
Mayor

Department of
Consumer Affairs

Protect your Money

Более подробную информацию можно найти на веб-сайте nyc.gov/consumers.
Для получения информации о федеральном законодательстве и законах штатов, на которые приводятся ссылки, вы можете связаться с соответствующими организациями, указанными в настоящем документе.