

Уведомления об утечке данных: зарубежный опыт правового регулирования

<i>Страна</i>	<i>Источник</i>	<i>Основные положения</i>	<i>Ответственность</i>
<i>Австралия</i>	Федеральный закон «О конфиденциальности» 1988 г. Federal Privacy Act	<p>Обязательное уведомление о нарушении данных включает нарушения данных, которые касаются:</p> <ul style="list-style-type: none"> – персональные данные; – информация о кредитной отчетности; – информация о праве на получение кредита; – номера налоговых файлов. <p>В определенных обстоятельствах организации могут иметь дополнительные обязательства по уведомлению других регуляторов о нарушениях данных.</p> <p>В случае с кибератаками должно информироваться Австралийское управление разумного регулирования (Australian Prudential Regulatory Authority) – в течение 72 часов после того, как стало известно об инциденте информационной безопасности, и не позднее 10 рабочих дней после того, как стало известно о существенном недостатке контроля информационной безопасности.</p>	<p>Максимальный штраф – 2,1 млн долларов</p> <p>(Законопроект о безопасности в Интернете предлагает увеличить данную сумму до 10 млн долларов или 10% от годового оборота организации в Австралии).</p>
<i>Беларусь</i>	Закон о защите персональных данных 2021 г.	<p>Обязательно направление уведомления об утечках в Национальный центр защиты персональных данных.</p> <p>Срок – в течение трех дней с момента обнаружения утечки.</p>	Отсутствуют
<i>Ботсвана</i>	Закон о персональных данных 2018 г.	Контролеры и операторы персональных данных обязаны немедленно уведомлять Комиссара	Невыполнение этого требования является преступлением:

	Data Protection Act	персональных данных о любом нарушении безопасности персональных данных.	- штраф в размере не более 100 000 BWP (~550 000 руб); или - тюремное заключение на срок не более трех лет; или - и штраф, и тюремное заключение.
Бразилия	Общий закон о защите данных 2018 г. Lei Geral de Proteção de Dados Pessoais	Контроллер должен сообщить об утечке в Национальное управление по защите данных (ANPD) и субъекту данных в разумные сроки, если нарушение может привести к риску или ущербу для субъектов данных. Сроки установлены руководством ANPD 2021 г. – уведомление должно быть направлено в течение двух рабочих дней, считая с даты получения информации об инциденте.	Не предусмотрена
Соединенное Королевство	Регламент Великобритании о защите данных (UK GDPR)	Предусматривается общая обязанность по направлению уведомления об утечке данных в Управление комиссара по информации (ICO) и в некоторых случаях субъектам данных. Срок – в течение 72 часов с момента обнаружения утечки.	Штраф суммой до 8,7 миллионов фунтов или до 2% годовой общемировой выручки за предыдущий год, в зависимости от того, что выше.
ЕС	Общий регламент по защите данных (GDPR)	<i>Для членов ЕС:</i> контроллеры обязаны направлять уведомления об утечке данных регулятору и в некоторых случаях субъектам данных. Срок – в течение 72 часов с момента обнаружения утечки.	<i>Для членов ЕС:</i> Штраф суммой до 10 миллионов евро или до 2% годовой общемировой выручки за предыдущий год, в зависимости от того, что выше.

Египет	<p>Закон о защите персональных данных</p>	<p>Контролер и оператор обязаны уведомить Центр о любом нарушении персональных данных в течение семидесяти двух часов с момента такого нарушения.</p> <p>Контролер и оператор обязаны уведомить субъекта данных в течение трех дней с даты уведомления Центра о нарушении и принятых в связи с этим мерах.</p>	Не предусмотрена
Израиль	<p>Закон о защите конфиденциальности 1981 г.</p> <p>Protection of Privacy Law</p>	<p>Владелец базы данных должен документировать любой инцидент и немедленно, но не позднее 72 часов с момента его возникновения, проинформировать регулятора и сообщить о принятых мерах.</p>	Не предусмотрена
Индия	<p>Правила информационных технологий (правила Индийской группы реагирования на компьютерные чрезвычайные ситуации) 2013 года</p> <p>The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules)</p>	<p>При возникновении любой утечки контролеры обязаны уведомить Cert-In в разумные сроки.</p>	Штрафы в размере примерно до 32.000.000 рублей.
Индонезия	<p>Закон об информационных технологиях 2000 г.</p> <p>Information Technology Act</p> <p>Правила о конфиденциальности 2011 г.</p>	<p>В случае неспособности защитить персональные данные, субъекту персональных данных должно быть направлено соответствующее уведомление направляется не позднее, чем через 14 дней после обнаружения сбоя.</p>	Не предусмотрена

	<p>Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules)</p> <p>Постановление Правительства о внедрении электронных систем и транзакций 2019 г.</p> <p>Government Regulation on the Implementation of Electronic Systems and Transactions</p>	<p>Также при первой возможности необходимо немедленно сообщать о любом сбое/серьезном вмешательстве/нарушении работы системы сотруднику правоохранительных органов и соответствующему Министерству или ведомству.</p>	
<p>Канада</p>	<p>Закон об электронной документации и защите персональных данных 2000 г. (PIPEDA)</p> <p>Закон провинции Альберта о защите персональных данных 2003 г. (PIPA)</p> <p>Закон провинции Квебек о конфиденциальности (вступает в силу 22/09/2022)</p>	<p>PIPEDA требует от организаций уведомлять как пострадавших лиц, так и федеральный регулирующий орган, если нарушение создает реальный риск причинения значительного вреда лицам. Кроме того, согласно PIPEDA, организации должны вести учет всех нарушений информационной безопасности (даже незначительных).</p> <p>PIPA: Организация должна без необоснованной задержки уведомить Уполномоченного по защите данных о любом инциденте, связанном с потерей, несанкционированным доступом или раскрытием персональных данных. Уполномоченный может потребовать от организации уведомить лиц, которым существует реальный риск причинения значительного вреда из-за утечки. Отличие от PIPEDA в том, что, согласно PIPA, субъект данных</p>	<p>Лицо, нарушившее положения PIPEDA об уведомлении о нарушении, может быть признано виновным в преступлении, наказуемом при вынесении приговора в порядке ускоренного производства (summary offence) и подлежащем штрафу в размере не более 10 000 канадских долларов (~500 000 рублей), или в преступлении с обвинительным заключением (indictable offence) и подлежащем штрафу в размере не более 100 000 канадских долларов (~5 000 000 рублей).</p>

		<p>уведомляется не сразу, а только если посчитает нужным Уполномоченный.</p> <p>Новый Закон о конфиденциальности Квебека предусматривает обязательство уведомлять Комиссию по доступу к информации и пострадавшее лицо, если инцидент представляет риск серьезного ущерба.</p>	
Каймановы острова	<p>Закон о защите персональных данных 2017 г.</p> <p>Data Protection Act</p>	<p>Контролер обязан уведомить об утечке данных Омбудсмана и субъекта персональных данных</p> <p>Срок – как можно скорее, но не более чем через пять дней после того, как контролер должен был узнать о нарушении</p> <p>Оператор данных должен своевременно уведомлять контролера.</p>	<p>Контроллер данных, нарушивший требования об уведомлении об утечке, совершает преступление и в случае признания виновным может быть оштрафован на 100 000 долларов Каймановых островов (~ 7 750 000 рублей).</p>
Катар	<p>Закон о защите персональных данных 2016 г.</p> <p>Law Concerning Personal Data Protection</p>	<p>Контролер обязан уведомить Департамент комплаенса и защиты данных и субъекта данных о любых нарушениях мер по защите данных.</p> <p>Уведомление Департамента и субъекта данных должно быть сделано как можно скорее с момента, когда контролеру стало известно о нарушении, но не позднее чем через 72 часа.</p>	<p>Штраф до 76.500.000 рублей.</p>
Китай	<p>Закон о защите персональных данных 2021 г.</p>	<p>PIPL: Об инциденте незамедлительно должны быть уведомлены:</p> <ul style="list-style-type: none"> - должностные лица компании – сотрудники по защите данных; 	<p>Не предусмотрена</p>

	<p>Personal Information Protection Law (PIPL)</p> <p>Проект Положения о безопасном управлении сетевых данных 2021 г.</p> <p>Draft Network Data Security Management (DNDSM)</p>	<p>- регулятор.</p> <p>Если контролер может предотвратить утечку данных в связи с инцидентом, то субъекты данных уведомлять не надо.</p> <p>DNDSM: Если нарушение данных затрагивает данные более чем 100 000 человек, оператор данных должен будет также уведомить регулятора или компетентный орган власти:</p> <ul style="list-style-type: none"> • в течение восьми часов после нарушения данных; и • в течение пяти рабочих дней после завершения расследования нарушения. 	
Колумбия	<p>Закон об общих положениях о защите персональных данных 2012 г.</p> <p>Ley por cual se dictan Disposiciones Generales para la Protección de Datos Personales</p>	<p>Контролер и оператор обязаны уведомлять Управление промышленности и торговли (Superintendencia de Industria y Comercio) о любых инцидентах или рисках утечки данных.</p> <p>Срок – в течение 15 рабочих дней с момента обнаружения.</p>	<p>Меры ответственности для организации, вовлеченной в утечку данных:</p> <ul style="list-style-type: none"> - приостановка деятельности; - штраф в размере, эквивалентном двум тысячам установленных законом MROT*, действующих на момент наложения штрафа. <p><i>*по состоянию на май 2022 года один MROT составляет 1 000 000 колумбийских песо (~15 000 рублей).</i></p>
Коста-Рика	<p>Положение к Закону о защите физических лиц в отношении обработки их персональных данных 2010 г.</p>	<p>Контроллер данных должен уведомить субъектов данных и регулятора – Агентство по защите персональных данных (PRODHAВ) в течение пяти рабочих дней после обнаружения нарушения.</p>	<p>Несоблюдение требований об уведомлении о нарушении данных не влечет за собой никаких штрафов. Однако такое уведомление настоятельно</p>

	Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales	В течение этого же срока (пять рабочих дней), контроллер данных должен инициировать тщательную проверку, чтобы определить степень ущерба, причиненного нарушением, и указать меры, которые должны быть приняты.	рекомендуется, поскольку обработка персональных данных без принятия соответствующих мер безопасности может повлечь за собой штраф в размере до 5 000 долларов США.
Новая Зеландия	Закон о конфиденциальности 2020 г. The Privacy Act	Обязательным является уведомление Комиссара по вопросам конфиденциальности и затронутых субъектов данных как можно скорее после того, как стало известно об утечке. Если уведомление пострадавшего субъекта данных не является практически целесообразным, можно опубликовать публичное уведомление. Основная организация несет ответственность за информирование физических лиц об о нарушении, если таковое возникло у компании на аутсорсинге. Разрешается отложить уведомление субъекта данных или его представителя или отложить публичное уведомление, если есть разумные основания полагать, что задержка необходима, поскольку уведомление может быть связано с рисками для безопасности персональных данных и эти риски перевешивают преимущества информирования затронутых лиц.	Не предусмотрена
Норвегия	Общий регламент по защите данных (GDPR)	Контролеры обязаны направлять уведомления об утечке данных регулятору и в некоторых случаях субъектам данных.	Штраф суммой до 10 миллионов евро или до 2% годовой общемировой выручки за предыдущий год, в зависимости от того, что выше.

		Срок – в течение 72 часов с момента обнаружения утечки.	
Республика Корея	<p>Закон о защите персональных данных (PIPA)</p> <p>Закон о содействии использованию информационно-коммуникационных сетей и защите информации, Закон о сети (Network Act)</p>	<p>Согласно PIPA, в случае нарушения персональных данных контроллер должен незамедлительно уведомить субъектов данных о деталях и обстоятельствах, а также о планируемых мерах по исправлению ситуации.</p> <p>Если число затронутых субъектов данных составляет 1 000 или более, контроллер должен немедленно сообщить об уведомлении субъектов данных и результатах принятых мер в Комиссию по защите персональных данных (PIPC) или Корейское агентство Интернета и безопасности (KISA).</p> <p>Кроме того, существует специальное положение для поставщиков онлайн-услуг относительно уведомления о нарушении данных. В случае утечки данных, пострадавший поставщик онлайн-услуг обязан предоставить индивидуальные уведомления пользователям онлайн-услуг и подать отчет об утечке персональных данных с подробной информацией об утечке и планируемых мерах по устранению последствий в PIPC или KISA, независимо от количества пострадавших субъектов данных.</p> <p>Кроме того, согласно Закону о сети, поставщик онлайн-услуг должен, в случае взлома системы/базы данных:</p>	<p>За несоблюдение требований по уведомлению о нарушениях может быть наложен штраф в размере 30 миллионов KRW (~13 млн рублей).</p>

		<p>- сообщить об этом в Министерство науки и ИКТ (MSIT) или KISA в течение 24 часов с момента обнаружения взлома, и</p> <p>- проанализировать причины взлома и предотвратить распространение ущерба, если взлом был успешен.</p>	
<i>Сингапур</i>	<p>Закон о защите персональных данных 2012 г. Personal Data Protection Act</p> <p>Положение о защите персональных данных (Уведомление об утечке данных) 2021 г. Personal Data Protection (Notification of Data Breaches) Regulations</p> <p>Уведомление об управлении технологическими рисками (дополненные Руководством по аутсорсингу и Руководством по управлению технологическими рисками) – для финансовых учреждений Notice on Technology Risk Management</p>	<p>Согласно Закону, если у организации есть основания полагать, что произошло нарушение, затрагивающее безопасность персональных данных, она должна провести оценку того, является ли нарушение данных «уведомляемым».</p> <p>Нарушение данных является «уведомляемым», если:</p> <ul style="list-style-type: none"> - оно приводит или может привести к значительному ущербу для затронутых лиц; или - имеет значительный масштаб (т.е. затрагивает 500 или более лиц). <p>Организация должна уведомить Комиссию как можно скорее, но в любом случае не позднее трех календарных дней после того, как организация проведет вышеуказанную оценку уведомляемого нарушения.</p> <p>Если нарушение данных приводит или может привести к значительному ущербу для затронутого лица (лиц), организация также должна уведомить каждого субъекта персональных данных.</p> <p>Если нарушение обнаружено посредником, он должен уведомить организацию (т.е. контролера данных) без неоправданной задержки с того момента, когда у посредника данных появились убедительные основания полагать, что произошло нарушение.</p>	Не предусмотрено

		<p>После получения уведомления от посредника организация должна провести оценку того, является ли нарушение данных уведомляемым.</p> <p>Финансовые учреждения обязаны уведомлять Денежно-кредитное управление о нарушениях безопасности и конфиденциальности данных клиентов в следующие сроки:</p> <ul style="list-style-type: none"> - в течение часа после обнаружения инцидента, который оказывает серьезное воздействие на деятельность финансового учреждения или существенно влияет на обслуживание финансовым учреждением своих клиентов; - как можно скорее о любом неблагоприятном развитии событий, возникающих в результате аутсорсинговых соглашений. 	
Турция	<p>Закон о защите персональных данных 2020 г. (LPPD)</p> <p>Решение Правления Органа по защите персональных данных (KVKK) № 2019/10 от 24.01.2019 о процедурах и принципах уведомления о нарушении персональных данных</p>	<p>Контролеры обязаны в кратчайшие сроки уведомить субъекта данных и KVKK.</p> <p>Согласно Решению № 2019/10, контролер должен уведомить KVKK не позднее 72 часов с момента обнаружения утечки. После определения лиц, которых затрагивает утечка, контроллер должен незамедлительно уведомить их.</p>	Отсутствуют
ЮАР	<p>Закон о защите персональных данных 2013 г. Protection of Personal Information Act (POPIA)</p>	<p>Обязательно уведомление регулятора и субъекта данных, если личность такого субъекта данных не может быть установлена.</p>	<p>Если регулятор определит, что было нарушение положений POPIA, он может выдать уведомление о принудительном</p>

		<p>Уведомление должно быть направлено как можно скорее после обнаружения утечки.</p> <p>Уведомление субъекта данных может быть отложено, если правоохранительные органы или Регулятор определит, что уведомление будет препятствовать проведению уголовного расследования.</p>	<p>исполнении, предписывающее действия, которые должна предпринять ответственная сторона для исправления ситуации.</p> <p>Ответственная сторона, не выполнившая предписание, может быть оштрафована на сумму, не превышающую 10 миллионов рандов (34.400.000 рублей) или лишена свободы на срок не более десяти лет.</p>
<p>Япония</p>	<p>Руководство по утечке данных Guidelines for Data Leakages</p>	<p>Контролер обязан незамедлительно уведомить регулятора.</p> <p>Понятие «незамедлительно» (яп. <i>sumiyakani</i>) не определено, однако семантика данного слова подразумевает срок в 4-5 дней.</p> <p>Субъекты данных должны быть уведомлены, если была утечка:</p> <ul style="list-style-type: none"> -чувствительных данных или был риск ее утечки; - данных, которые могут повлечь финансовые потери у субъекта данных; - данных более 1000 человек. <p>Если инцидент, связанный с персональными данными, возник у оператора, вышеуказанные обязательства по уведомлению ложатся на контролера</p>	<p>Не предусмотрена</p>

США¹			
Айдахо	<p>Свод законов штата Айдахо §§ 28-51-104 to -107</p> <p>Idaho Statute . §§ 28-51-104 to -107</p>	<p>Госорганы обязаны направить уведомление в Офис генерального прокурора штата Айдахо в течение 24 часов с момента обнаружения утечки данных.</p>	<p>Штраф до 25000\$.</p>
Алабама	<p>Закон штата Алабама об уведомлении об утечках данных 2018 г.</p> <p>Alabama Data Breach Notification Act of 2018</p> <p>Закон Алабамы о вводящей в заблуждение торговой практике 1975 г.</p> <p>Alabama Deceptive Trade Practices Act</p>	<p>Обязательно уведомлять субъектов данных в случаях, если утечка может нанести им существенный вред. Срок – в течение 45 дней с момента обнаружения утечки.</p> <p>Если утечка произошла у третьих сторон (агентов), такие агенты обязаны уведомить контролера. Срок – в течение 10 дней с момента обнаружения утечки.</p> <p>В случае утечки данных более 1000 жителей штата, контролер и его агенты обязаны направить уведомление в Офис генерального прокурора штата Алабама.</p>	<p>Такие нарушения считаются незаконной торговой практикой в соответствии с Законом 1975 г.</p> <p>Сознательное невыполнение требования об уведомлении – штраф в размере до \$2,000 за одно нарушение, но не более \$500,000 за всю утечку.</p>
Аляска	<p>Закон о защите персональных данных штата Аляска 2009 г.</p> <p>Alaska Personal Information and Protection Act of 2009</p> <p>Закон Аляски о защите прав потребителей</p> <p>Alaska Consumer Protection Act</p>	<p>В случае утечки более 1000 жителей штата, обязательно уведомление пострадавших субъектов и всех агентств штата, которые предоставляют информацию о потребительских кредитах.</p>	<p>Если утечка произошла в органе местного самоуправления, а пострадавшие граждане не были уведомлены, орган может быть оштрафован на 500\$ за каждого неуведомленного гражданина. Общая сумма штрафа не может превышать 50.000\$.</p>

¹ Указаны те штаты и территории США, где имеются конкретные сроки уведомления и предусмотрена ответственность.

			Несоблюдения требований об уведомлении частными компаниями квалифицируется как недобросовестная торговая практика, согласно Закону о защите прав потребителей. Сумма штрафа не может превышать 50.000\$
Вирджиния	<p>Кодекс Вирджинии §§ 18.2-186.6, 32.1-127.1:05</p> <p>Virginia Code §§ 18.2-186.6, 32.1-127.1:05</p>	<p>Обязательно уведомить офис генерального прокурора штата и каждого пострадавшего жителя Вирджинии, как только утечка обнаружена.</p> <p>В случае утечки информации любое физическое или юридическое лицо, которое не владеет персональной/медицинской информацией и не имеет на нее лицензии, но хранит ее, обязано уведомить об этом офис генерального прокурора и владельца персональных данных (организацию, для которой хранились данные).</p> <p>В случае утечки более 1000 жителей штата, обязательно уведомление пострадавших субъектов и всех агентств штата, которые предоставляют информацию о потребительских кредитах.</p> <p>В случае утечки медицинских данных обязательно незамедлительное уведомление генерального прокурора штата и Комиссара по вопросам здравоохранения.</p>	Штраф за неуведомление не может превышать 150.000\$
Гавайи	Пересмотренный свод законов штата Гавайи 487N	Если утечка затронула более чем 1000 жителей, незамедлительно должно быть направлено	Генеральный прокурор Гавайев или Гавайское управление по

	<p>Hawaii Revised Statute 487N</p>	<p>письменное уведомление в Управление по защите прав потребителей штата Гавайи.</p> <p>Если уведомляется более 1000 жителей, уведомление должно быть направлено без необоснованной задержки во все агентства по предоставлению информации о кредитоспособности потребителей.</p>	<p>защите прав потребителей могут подать иск о взыскании штрафа в размере 2500\$.</p>
<i>Джорджия</i>	<p>Свод законов штата Джорджия §§ 10-1-910, -911, -912; § 46-5-214</p> <p>Georgia Code §§ 10-1-910, -911, -912; § 46-5-214</p>	<p>Организация, которая хранит данные от имени другой организации, должна направить уведомление в течение 24 часов после обнаружения утечки.</p> <p>Если уведомляется более 10 000 жителей, уведомление должно быть направлено без необоснованной задержки во все агентства по предоставлению информации о кредитоспособности потребителей.</p>	<p>Штрафы не должны превышать 100\$ за нарушение, связанное с конкретным потребителем.</p>
<i>Индиана</i>	<p>Свод законов штата Индиана §§ 4-1-11, 24-4.9</p> <p>Indiana Code §§ 4-1-11, 24-4.9</p>	<p>Если уведомляется более 1000 жителей, уведомление должно быть направлено без необоснованной задержки во все агентства по предоставлению информации о кредитоспособности потребителей.</p>	<p>Лицо или организация, не соблюдающие положения о раскрытии информации могут быть привлечены к ответственности только генеральным прокурором. Генеральный прокурор может применить гражданский штраф в размере не более 150 000 за обманное действие или судебный запрет для запрета будущих нарушений при условии расследования обманного действия</p>

Калифорния	Гражданский кодекс Калифорнии: ст. 1798.29(a) (для госорганов) ст. 1798.82(a) (для частных компаний)	Уведомление об утечке направляется, если пострадало более 500 жителей штата. Копия уведомления направляется генеральному прокурору штата.	Штраф в размере 100\$ в день, если уведомление не было направлено в течение 15 дней после обнаружения утечки.
Колорадо	Пересмотренный свод законов штата Колорадо, раздел 6-1-716 Colo. Rev. Stat. § 6-1-716	Уведомление пострадавших жителей штата и генерального прокурора штата должно быть направлено в кратчайшие сроки, но не позднее 30 дней с момента обнаружения утечки. Если пострадало более 1000 человек, необходимо также уведомить все агентства по предоставлению информации о кредитоспособности потребителей.	Точные суммы штрафа не указаны. Сумма определяется судом по поданному генеральным прокурором иску.
Коннектикут	Свод законов штата Коннектикут, раздел 36a-701b, 4e-70 Connecticut General Statute §§ 36a-701b, 4e-70	Уведомление пострадавших жителей штата и генерального прокурора штата не позднее, чем через 60 дней после обнаружения утечки.	Точные суммы штрафа не указаны. Сумма определяется судом по поданному генеральным прокурором иску.
Луизиана	Пересмотренный свод законов штата Луизиана §§ 51:3071 Louisiana Revised Statute §§ 51:3071	Уведомление пострадавших от утечки субъектов-жителей штата должно быть сделано в кратчайшие сроки без необоснованной задержки, но не позднее 60 дней с момента обнаружения утечки. Также должен быть уведомлен Отдел защиты прав потребителей Генеральной прокуратуры штата. Уведомление Генеральной прокуратуры будет считаться «своевременным», если оно получено в течение 10 дней после уведомления жителей.	Несвоевременное уведомление Генерального прокурора наказывается штрафом до 5000\$ за каждое нарушение. Каждый день неполучения уведомления Генеральным прокурором считается отдельным нарушением.

		<p>Лица, на которых распространяется Закон о безопасности страховых данных (La. Rev. Stat. §§ 22:2501 - 2511), должны уведомить страхового комиссара (государственный чиновник штата, который регулирует страховую отрасль) не позднее 3 рабочих дней с момента обнаружения утечки.</p>	
<p><i>Мичиган</i></p>	<p>Свод законов штата Мичиган 2006 г. §§ 445.63, 445.72</p> <p>Michigan Compiled Laws of 2006 §§ 445.63, 445.72</p>	<p>Уведомление об утечке должно быть направлено пострадавшему жителю штата письменно без необоснованной задержки.</p> <p>Если сообщение в течение 3 рабочих дней после письменного уведомления не удалось связаться с пострадавшим, контролер данных обязан связаться с ним по телефону.</p>	<p>Непредоставление уведомления об утечке квалифицируется как уголовный проступок.</p> <p>За первое нарушение предусматривает штраф в размере не более \$250 или тюремное заключение на срок не более 93 дней или и то, и другое.</p> <p>За второе нарушение - штраф в размере не более \$500 или тюремное заключение на срок не более 93 дней или оба наказания.</p> <p>За третье нарушение может быть наложен штраф в размере не более \$750 или лишение свободы на срок не более 93 дней или оба наказания.</p> <p>За множественные нарушения, возникшие в результате одного и того же нарушения безопасности,</p>

			штраф не должен превышать 750000\$.
Мэриленд	<p>Кодекс штата Мэриленд по торговому праву 2017 г.</p> <p>Maryland Code Commercial Law of 2017</p>	<p>Пострадавшие должны быть уведомлены не позднее чем через 45 дней после обнаружения утечки.</p> <p>Обязательно уведомление генерального прокурора штата до направления уведомления пострадавшим от утечки жителям.</p> <p>Организация, которая хранит персональные данные в качестве третьего лица, должна уведомить владельца или лицензиата данных как можно скорее, но не позднее чем через 45 дней после обнаружения нарушения.</p>	<p>Конкретные штрафы отсутствуют.</p> <p>Возможно привлечение к ответственности в соответствии с Законом о защите потребителей.</p>
Нью-Мексико	<p>Свод законов штата Нью-Мексико 2017 г. § 57-12C-1—57-12C-12</p> <p>New Mexico Statutes of 2017 § 57-12C-1—57-12C-12</p>	<p>Об утечке должен быть уведомлен каждый пострадавший житель штата. Срок – в течение 45 дней с момента обнаружения утечки.</p> <p>В случае если данные хранились у третьих лиц, такие лица обязаны уведомить контролера данных об утечке в течение 45 дней с момента обнаружения утечки.</p> <p>Если число пострадавших от утечки жителей штата превышает 1000 человек, контролер обязан направить уведомление генеральному прокурору штата и во все агентства по предоставлению информации о кредитоспособности потребителей. Срок – в течение 45 дней с момента обнаружения утечки.</p>	<p>Генеральный прокурор может подать иск о нарушении закона.</p> <p>Осознанное или неосторожное нарушение может повлечь за собой дополнительные штрафы в размере до \$25 000 или \$10 за одно несостоявшееся уведомление на сумму до \$150 000.</p>

<p>Огайо</p>	<p>Пересмотренный свод законов штата Огайо §§ 1349.19-192</p> <p>Ohio Revised Code §§ 1349.19-192</p>	<p>Уведомление должно быть направлено пострадавшим жителям штата не позднее 45 дней с момента обнаружения утечки.</p> <p>Кроме того, любое лицо, которое хранит или записывает данные от имени другой стороны, обязано уведомить другую сторону в случае утечки данных в ускоренном порядке.</p>	<p>Генеральный прокурор имеет право предъявлять иски лицам, которые не выполняют требования об уведомлении об утечке данных.</p> <p>Предусматриваются следующие формы ответственности:</p> <ul style="list-style-type: none"> - временный судебный запрет; - постоянный судебный запрет; - штраф в размере до \$ 1000 в день в течение первых 60 дней несоблюдения; <ul style="list-style-type: none"> • штраф увеличивается до \$5000 в день после 60 дней несоблюдения. • штраф увеличивается до \$10000 в день после 90 дней несоблюдения. •
<p>Пуэрто Рико</p>	<p>Законы Пуэрто Рико, глава 310</p> <p>Laws of Puerto Rico chapter 310</p>	<p>О любой утечке данных необходимо направить уведомление в правительство Пуэрто Рико в течение 10 дней с момента обнаружения утечки.</p>	<p>Штрафы от 500\$ до 5000\$ за неуведомление.</p>
<p>Род Айленд</p>	<p>Общие законы штата Род Айленд, раздел 11-49.3.1</p> <p>Rhode Island General Laws title 11-49.3.1</p>	<p>Уведомление должно быть направлено пострадавшим жителям штата не позднее 45 дней с момента обнаружения утечки.</p> <p>Если число пострадавших от утечки жителей штата превышает 500 человек, контролер обязан направить уведомление генеральному прокурору штата и во все агентства по предоставлению информации о кредитоспособности потребителей</p>	<p>Штраф от 100 до 200\$ за одно нарушение.</p>

<p><i>Техас</i></p>	<p>Кодекс предпринимательской деятельности и торговли штата Техас §§ 521.002, 521.053</p> <p>Texas Business and Commerce Code §§ 521.002, 521.053</p>	<p>Пострадавшие лица должны быть уведомлены как можно быстрее, но не позднее чем через 60 дней после обнаружения утечки.</p> <p>Если уведомляется более 250 жителей, необходимо также уведомить генерального прокурора штата. Срок – в течение 60 дней после обнаружения утечки.</p> <p>Если число пострадавших от утечки жителей штата превышает 10000 человек, контролер обязан направить уведомление во кредитные учреждения и агентства по предоставлению информации о кредитоспособности потребителей</p>	<p>Ответственность в форме штрафа в размере от \$2000 до \$50000 за каждое нарушение.</p> <p>Кроме того, несоблюдение положений об уведомлении может привести к штрафу в размере до 100\$ для каждого лица, в отношении которого должно быть направлено уведомление, за каждый день, когда контролер не предпринимает разумных действий для соблюдения положений об уведомлении.</p> <p>Нарушения также считаются недобросовестной торговой практикой.</p>
<p><i>Флорида</i></p>	<p>Свод законов штата Флорида §§ 501.171, 282.0041, 282.318(2)(i)</p> <p>Florida Statute §§ 501.171, 282.0041, 282.318(2)(i)</p>	<p>Если утечка затронула 500 или более лиц обязательно уведомить Департамент по правовым вопросам штата Флорида не позднее чем через 30 дней после обнаружения утечки.</p> <p>Если нарушение затронуло более 1000 жителей, должны быть уведомлены все агентства по предоставлению информации о кредитоспособности потребителей</p> <p>Третьи стороны, которые хранят данные от имени контролера, должны уведомить его не позднее чем через 10 дней после обнаружения утечки.</p>	<p>Организация может быть привлечена к гражданской ответственности в виде штрафа в размере: \$1,000 в день в течение первых 30 дней, \$50,000 за каждый последующий 30-дневный период до 180 дней, и общая сумма не должна превышать \$500,000, если нарушение продолжается более 180 дней.</p>

Южная Дакота	<p>Закон, предусматривающий уведомление об утечке определенных данных и ответственность за неуведомление 2018 г.</p> <p>SB62 of 2018</p>	<p>Пострадавшие от утечки должны быть уведомлены не позднее 60 дней с момента обнаружения утечки данных.</p> <p>Если необходимо уведомить более 250 жителей штата, обязательно направить об этом уведомление генеральному прокурору штата и всех агентств по предоставлению информации о кредитоспособности потребителей</p> <p>Уведомление может быть отложено, если правоохранительные органы определяют, что уведомление будет препятствовать уголовному расследованию. Любое отложенное уведомление должно быть сделано в течение тридцати (30) дней после того, как будет сочтено, что такое уведомление не окажет негативного влияния на уголовное расследование.</p>	<p>Генеральный прокурор Южной Дакоты может инициировать расследования в отношении физических или юридических лиц, которые не сообщают об утечках данных, поскольку это квалифицируется как введение в заблуждение.</p> <p>Кроме того, генеральный прокурор от имени штата может подать гражданский иск на сумму не более 10000\$ в день за нарушение.</p>
-------------------------	--	---	---