ЗАЩИТА ДАННЫХ: ВСЕ ТОЛЬКО НАЧИНАЕТСЯ

После введения нового европейского регулирования по защите личных данных (GDPR) 25 мая этого года многие предприятия, особенно малые, оказались в растерянности и задали себе много вопросов. Готова ли компания защищать личные данные своих клиентов? До конца ли введена на предприятии новая регула и как в этом убедиться? Надо ли и дальше уделять внимание GDPR или же это одноразовый процесс? Чем грозит несоблюдение норм? Разобраться в вопросе L'Officiel Hommes помогли эксперты – специалист по защите данных предприятия Squalio Марина Бришкена и партнер адвокатского бюро Sorainen Агрис Репшс.

Текст: ОЛЬГА КНЯЗЕВА

БЕЗОПАСНОСТЬ – НЕ ТОЛЬКО НА ДОРОГЕ

Если коротко, то GDPR (General Data Protection Regulation) – это общий регламент по защите данных, который определяет правила сбора, обработки и хранения личной информации. После его вступления в силу делать все это, и уж тем более передавать (или продавать) личную информацию можно только с согласия пользователя. При этом пользователю нужно объяснить, для каких целей его данные будут использованы.

Для предприятия – неважно, маленького или большого – регламент означал не только введение новых внутренних правил, но и обучение сотрудников обращению с данными, а также проверку надежности IT-систем.

Казалось бы, ничего нового. Ведь и раньше закон выдвигал достаточно строгие требования к защите данных, и разбрасываться ими точно не было позволено. И сейчас в Латвии и в ЕС есть закон о защите данных, исполнение которого у нас отслеживает Государственная инспекция данных. Однако законодательство не до конца учитывало все риски, которые могут возникнуть в момент сбора, хранения, обработки и передачи личных данных. Отсюда растут ноги у многих скандалов, которые разразились из-за массовой утечки данных.

И НА ГИГАНТОВ БЫВАЕТ ПРОРУХА

А скандалов таких было немало. Напомним, в 2016 году хакеры взломали базы данных Uber и получили доступ к именам, фамилиям, адресам электронной почты и номерам

Весной 2017 года стало известно о том, что киберпреступники украли данные пациентов, их фотографии, в том числе в обнаженном виде и фото «до и после», из литовской клиники пластической хирургии Grožio Chirurgija и выставили их на продажу в «темном Интернете».

мобильных телефонов 57 миллионов клиентов, а также к персональным данным 600 тысяч водителей такси, включая информацию о лицензиях. Этот инцидент стал достоянием гласности только в 2017 году – оказывается, Uber заплатил хакерам 80 000 евро, чтобы похищенные данные были уничтожены и никогда не использовались.

Весной 2017 года стало известно о том, что киберпреступники украли данные пациентов, их фотографии, в том числе в обнаженном виде и фото «до и после», из литовской клиники пластической хирургии Grožio Chirurgija и выставили их на продажу в «темном Интернете» (dark web). Цены варьировались от 50 до 2000 евро за карточку пациента, среди которых были как местные, так и международные знаменитости. Даже такой мировой гигант, как аудиторская фирма Deloitte, стал жертвой кибератаки, когда была взломана система ее корпоративной электронной почты. Считается,

что хакеры, вероятно, получили информацию о лучших клиентах компании (blue-chips) – их фамилии, пароли, личные данные, конфиденциальную переписку. А в Швеции в августе прошлого года из-за утечки конфиденциальных данных должностей лишились министр внутренних дел Андерс Игеман, министр инфраструктуры Анна Йохансон и руководитель Национального транспортного агентства Мария Агрен.
Самый последний инцидент случился в начале сентября этого года, когда GDPR уже начал действовать на территории ЕС. На сей раз жертвами хакеров стали клиенты компании British Airways, у которых злоумышленники украли персональные данные и данные кредитных карт. Утечка данных могла затронуть около 380 000 клиентов British Airways.
Если уж у крупных компаний были явные проблемы с защитой данных, то что говорить о малом бизнесе, который редко придавал большое значение тому, как хранится внутренняя информация. После 25 мая этого года ситуация поменялась кардинально.

ПРОЦЕСС ДЛИНОЮ В ЖИЗНЬ

Впрочем, как оказалось, бизнес к этим изменениям не был готов. Опрос более тысячи компаний, проведенный McDermott Will & Emery и Ponemon Institute в апреле этого года, показал, что более 60% технологических компаний не смогут соответствовать требованиям закона к дате начала его действия. Опрос в Латвии накануне вступления закона в силу выявил еще более печальную картину: только 10% предприятий оказались готовы к GDPR. Впрочем, если вы входите в число оставшихся 90%, отчаиваться не стоит. Стоит начать действовать прямо сейчас.
Эксперты считают, что готовность предприятий к GDPR и соответствие ему – это цель, которая не достигается за один раз. Технологии развиваются, вместе с ними меняются возможности киберпреступников получать доступ к данным, поэтому и юридические, и IT-процессы (и их соответствие с GDPR) будет необходимо пересматривать достаточно регулярно. Возможно, раз или два в год, проводя на своем предприятии внутренний аудит.
Самое интересное: многие предприятия (до 25 мая таковых было 41%) считают, что вообще не обрабатывают персональные данные. Это – самая главная ошибка. Потому что, по статистике, GDPR касается 99% предприятий.
Неважно, в какой сфере занято предприятие, сколько у него сотрудников и клиентов. Важно только то, что если у компании есть хоть какая-то информация с личными данными, то оно автоматически попадает под действие нового регламента. Даже если вы составляете список гостей для мероприятия – вы уже обрабатываете личные данные. Если записали своих сотрудников в тетрадку – это тоже личные данные. Другими словами, избежать GDPR не получится.
Например, у предприятия есть база данных клиентов, отзывов или анкет с предложениями, данные программы лояльности клиентов, письма электронной почты, фото, видео с камер наблюдения, или просто списки сотрудников с персональными данными (например, персональными кодами).
Если разобрать личные данные по полочкам, то сюда включаются: имя, фамилия, номер телефона, электронная почта, адрес проживания, регистрационный номер автомобиля, номер банковского счета, номер банковской карты или срок ее действия, данные об истории болезни, группе крови, информация о членах семьи, внешний вид, фото- и видеоматериалы, биометрические данные, все паспортные данные и вся информация о членах семьи. Одним словом – фактически любая информация о человеке.

КОГДА РАЗМЕР НЕ ИМЕЕТ ЗНАЧЕНИЯ

Вопрос, который волнует многие предприятия: кто же тот волшебный человек, который разберется с премудростями сложной европейской регулы? По сути, самый легкий путь – нанять специально обученного человека Data Protection Officer (DPO), который лучше других знает о том, как адаптировать GDPR для конкретного предприятия. Он же будет следить за соблюдением новых норм и, возможно, сэкономит немалые деньги, не допустив серьезных ошибок с личными данными.
Однако эксперты говорят, что сейчас в Латвии таких специалистов – кот наплакал. Дело в том, что в вузах Латвии на Data Protection Officer не учат, и профессия это крайне дефицитная. Причем брать или не брать специалиста на предприятие зависит не от объемов этого предприятия, а от объемов обрабатываемой информации. Бывает, что компания с 10 сотрудниками, но большим количеством клиентов обрабатывает в сотни раз больше данных, чем, положим, предприятие с сотней работников.
Можно обратиться в юридическую компанию, которая специализируется на вопросе защиты данных, и это тоже будет вариантом аутсорсинга. Однако надо быть предельно открытым перед специалистом со стороны, максимально ему довериться, чтобы тот смог навести порядок в сфере защиты данных. Это, признаются эксперты, не всегда удается, поскольку предприятия сами не всегда понимают, что им нужно. А также не всегда способны определить зоны риска и расставить приоритеты.

ПОМОГИ СЕБЕ САМ

Если же данных на предприятии не так много, то можно попробовать обойтись своими силами. Для начала нужно оценить внутренние риски с помощью небольшого аудита. Например, провести опрос работников, чтобы выяснить, какие персональные данные они собирают и обрабатывают, а главное – для каких целей. Если цель неясна, значит и данные эти вам, возможно, не очень нужны. С ними лучше расстаться, а не оставлять «на всякий случай».
Далее нужно выяснить у ваших партнеров, которые обрабатывают данные по заданию вашего предприятия (например, маркетинговые предприятия, которым переданы клиентские данные для повышения активности продаж), и договориться о порядке, как подготовить

поправки к договорам, чтобы отражать требования новой регулы.
Также стоит улучшить и дополнить политику конфиденциальности предприятия, если такая уже есть. Если такой нет, можно подготовить упрощенную версию, которая отражает то, как предприятие обрабатывает личные данные своих клиентов и партнеров. Здесь, скорее всего, нужна будет консультация юриста, который поможет грамотно составить документы.
Также нужно уделить внимание безопасности IT-системы. Начать с самого простого: установить антивирусы и брандмауэры, потому что в конечном счете одна из целей GDPR – снизить утечку данных и несанкционированный доступ к персональным данным. Лучше всего не экономить на программном обеспечении. Может показаться, что нелицензионные программы дешевле, однако долговременные риски гораздо выше. Нелицензионные программы могут содержать в себе скрытые зловредные «сюрпризы» – например, шпионские программы, вирусы и т. д.
И, наконец, у предприятия должны быть регистры данных, которые содержат в себе информацию о том, данные какой персоны обрабатываются, кто и каким способом это осуществляет. Это позволит компании оперативно и понятно ответить на вопросы физических лиц о том, какие их данные обрабатываются.
Кстати, многие предприятия решают проблему с безопасным хранением данных очень просто – доверяют этот процесс облачным технологиям. Во-первых, уменьшаются расходы на содержание системы, и, во-вторых, не надо заботиться о надежном хранении данных. Но, конечно же, «облачные» варианты не решают проблему соответствия внутренних процессов на предприятии требованиям GDPR.

ВАЖНЫЕ ТОНКОСТИ

На самом деле нюансов в новой регуле великое множество. И многие из них могут даже показаться абсурдными. Однако они учитывают невидимые риски, которые могут возникнуть с личными данными. Взять, к примеру, CV, с помощью которых предприятие набирает работников. По новой регуле полученные CV нужно правильно хранить. Прежде всего, предприятие должно будет получить от претендентов согласие на хранение анкет, и более того – уже в объявлении о работе просить претендентов указывать, как долго можно хранить их CV.
Не стоит забывать, что на предприятии могут быть не только компьютеры с личными данными, но и рабочие мобильные телефоны. Если речь идет о списке контактов физического лица в личном телефоне – регламент не относится к такой обработке данных. Он относится к случаям, когда работник хранит список деловых контактов в рабочем телефоне. Поэтому такой телефон не может быть доступен кому попало.
Иногда предприятия «привязывают» чип-карты для входа в офис к

ФОТО: © PANTHERMEDIA.NET / BRIJIT VIJAYAN / REUTERS/SCANPIX/LETA

конкретному человеку, указывая на ней имя и фамилию, название предприятия и даже фото сотрудника. После введения GDPR делать это можно будет и дальше, но уже не просто так, а с обоснованием и с согласия работника. И даже если такое согласие получено, то личные данные работника все равно придется шифровать, поскольку использовать прямую личную информацию на карте больше нельзя.

Отдельные требования теперь относятся и к визитным карточкам. Если на визитной карточке работника значится только его имя, фамилия, должность, название предприятия, рабочий телефон, электронная почта предприятия или рабочая электронная почта – все в порядке! Но если на визитке указывается еще и мобильный телефон или личная электронная почта – это уже личные данные. Перед тем как напечатать такую визитку, надо будет получить разрешение работника. То же касается и полученных визитных карточек – их рекомендуется хранить в надежном месте, чтобы не допустить утечки информации.

И на «сладкое»: дни рождения сотрудников отныне – это не те сведения, которые можно разглашать. Знакомая ситуация: директор предприятия поздравляет своего работника, положим, с юбилеем. Торт, цветы, поздравления... Стоп! Впредь делать это можно будет только после получения особого разрешения работника, поскольку фактически это является распространением личных данных работника, пусть и в пределах предприятия. То же самое касается права работников на его фотографирование (например, для корпоративного сайта или газеты), видеосъемку и публикации.

С ЗАБОТОЙ О КЛИЕНТЕ

Сразу скажем, для пользователя услуг GDPR – благо. Регламент дает возможность каждому человеку во всех подробностях узнать, какие данные о нем хранит предприятие, для каких целей оно использует эти данные и как долго. А также надежно ли хранятся личные данные, где хранятся, с какой целью и кому передаются. У человека появляется полное право запретить использовать данные и даже потребовать удалить их. Другими словами, полный и безоговорочный контроль. Специалисты по защите данных физических лиц сравнивают информацию с деньгами, которые человек доверяет банку и рассчитывает, что никому другому они отданы не будут.

Отныне никто не имеет права терроризировать клиента звонками на личный телефон с предложением товаров или услуг. Личную информацию о клиентах такие предприятия получают, чаще всего перекупая базы данных у других компаний – например, списки людей, которые участвовали в какой-то лотерее. Но делать это теперь категорически нельзя. Если такие звонки вам все-таки будут поступать, у вас есть полное право запретить вам звонить и вычеркнуть ваши данные из базы данных предприятия и всех других компаний, которым оно предоставило сведения о вас.

Кстати, если вам кто-то позвонил и начал предлагать очередной товар «только сейчас и только для вас», то по вашему запросу он обязан ответить, откуда он взял ваш номер и на каком основании он вообще звонит без разрешения.

PRIVACY POLICY – ПРОСТО И ПОНЯТНО

Узнать о том, как компания обрабатывает и хранит личную информацию, теперь подробно можно из Политики конфиденциальности (Privacy Policy). Этот раздел в обязательном порядке есть на всех сайтах предприятий.

До принятия GDPR нормальным было создавать Privacy Policy с максимально размытыми положениями и размещать ее там, где никто искать не станет. Однако после 25 мая требования к Privacy Policy сильно ужесточились. Например, статья 12 GDPR обязывает предоставлять информацию об обработке персональных данных в четкой, краткой и доступной форме, простым и понятным для обычного человека языком. Это значит, что Privacy Policy не должна содержать сложных формулировок, юридического жаргона, запутанных и размытых понятий. Процесс использования данных должен описываться так, чтобы обычный человек понимал, что там написано.

Дни рождения сотрудников фирмы отныне можно отмечать только с их разрешения, поскольку данная дата – тоже конфиденциальная информация.

Предприятие, в свою очередь, должно указать название контролера, его контактные данные и контактные данные его представителя (если необходимо). Также указываются контакты уполномоченного в компании по защите данных (Data Protection Officer), если таковой есть.

Более того, согласно GDPR, компания обязана раскрыть всех третьих лиц, которым предприятие передает данные пользователей.

И напоследок надо напомнить: нарушение регулы влечет за собой очень суровые штрафы: административный штраф в размере до 10 млн евро, или 2% от общего оборота, либо штраф в размере до 20 млн евро или до 4% от оборота (для групп предприятий учитывается общий оборот). Эти штрафы могут быть применены к управляющему данными (юридическому или физическому лицу) и обработчикам, и, кроме того, возможно, придется платить компенсации физическим лицам.