Штраф до € 20 млн. Как аукнется компаниям нарушение требований о защите персональных данных в ЕС

Фото с сайта publicdomainpictures.net

В мае следующего года вступает в силу регламент, который заставит некоторые компании России, Беларуси, Украины и других стран соблюдать ряд требований о защите персональных данных граждан ЕС. В каких случаях это может произойти и о каких требованиях идет речь — рассказывают адвокат, председатель совета директоров минского офиса юридической фирмы

Cerha Hempel Spiegelfeld Hlawati Сергей Макарчук и старший юрист фирмы Никита Толканица.

— В последние годы те или иные нормативные акты все чаще и чаще носят экстерриториальный характер, что связано с развитием новых средств коммуникации и, особенно, Интернета. В результате компании одного государства могут подпадать под требования законодательства другого.

Сергей Макарчук

Председатель совета директоров минского офиса CHSH Cerha Hempel Spiegelfeld Hlawati

Никита Толканица

Старший юрист CHSH Cerha Hempel Spiegelfeld Hlawati

Например, уже в 2018 году некоторые компании из стран СНГ могут столкнуться с необходимостью соблюдения ряда требований о защите персональных данных, но не своих граждан, а жителей ЕС. В частности, 27 апреля 2016 Европейский Парламент и Совет Европейского Союза совместно приняли General Data Protection Regulation — Общий регламент по защите данных (далее — «Регламент»). Регламент (и соответственно, предусмотренные им требования) вступит в силу 25 мая 2018.

Кто под ударом

Регламент направлен на защиту персональных данных физических лиц, проживающих в ЕС, что само по себе не является новой идеей. Однако его знаковая особенность — попытка защитить этих лиц не только на территории ЕС, но и за его пределами. Иными словами,

исполнять его требования должны не только европейские компании, но в некоторых случаях и компании из других регионов, в том числе из Беларуси, России, Украины, Казахстана и т.д.

Так, компании-нерезиденты ЕС могут столкнуться с необходимостью соблюдения Регламента в двух случаях.

1. Компания из СНГ обязана соблюдать Регламент, если ее товары и услуги на постоянной основе предлагаются потребителям из стран ЕС. При этом необязательно, чтобы такие продукты были платными. Достаточно просто позиционировать товары и услуги как направленные на жителей Европы. Например, создать вебсайт, где предлагаются продукты, на языке страны-участницы ЕС или принимать в качестве оплаты валюту, эмитированную в Европе (например, евро для Франции и Германии, злотый для Польши).

По указанному признаку под действие Регламента могут попасть онлайн-магазины, социальные сети, различные онлайн-сервисы, браузерные игры с возможностью внутриигровых покупок за наличные деньги и т.д.

2. Компания из СНГ обязана соблюдать Регламент, если она осуществляет мониторинг действий в сети Интернет лиц, проживающих в ЕС. При этом такой мониторинг предполагает создание профилей пользователей для анализа их привычек и предпочтений. Соответственно, даже использование cookie-файлов для последующей таргетированной рекламы может быть рассмотрено как основание для соблюдения Регламента.

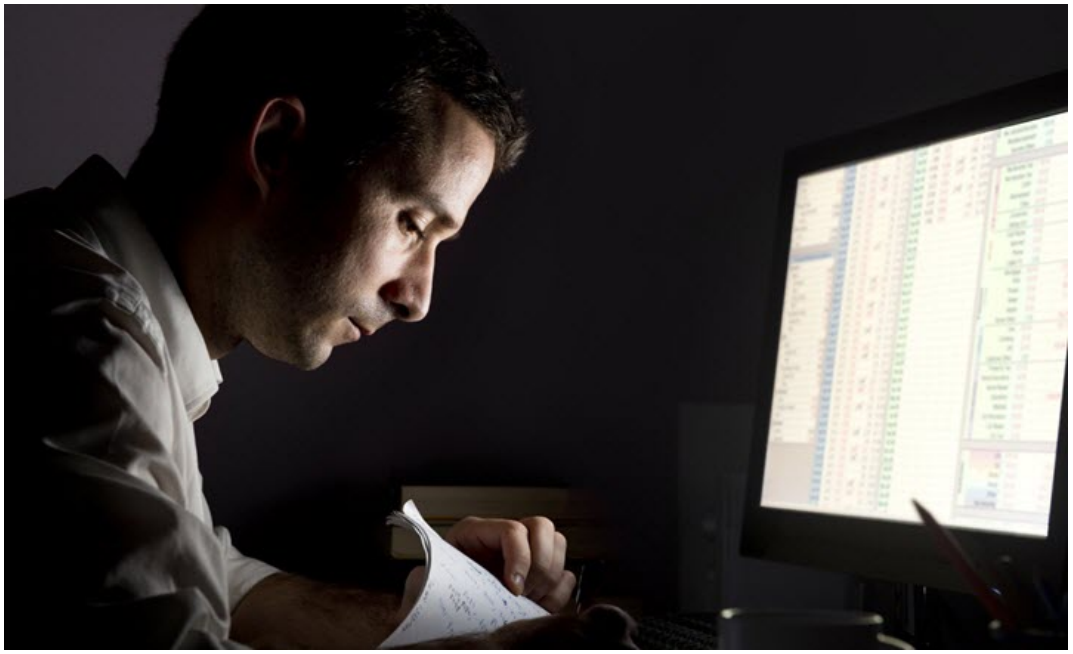

Фото с сайта 24warez.ru

При этом Регламент регулирует не только деятельность лиц, которые непосредственно распоряжаются персональными данными и используют их (так называемые контролеры данных). Соблюдать его должны и подрядчики контролера данных (операторы данных), которые выполняют одну или несколько из следующих функций:

- Собирают данные
- Записывают и хранят их
- Структурируют сведения по определенным критериям
- Выступают посредниками при передаче информации и т.д.

Следовательно, даже если компания из Беларуси, России, Казахстана или иной третьей страны просто предоставляет европейскому контрагенту сервер для хранения персональных данных лиц из ЕС,

то она может быть рассмотрена как оператор, обязанный соблюдать требования Регламента.

Однако в некоторых случаях **соблюдать Регламент для компании из СНГ нет необходимости**:

1. Если компания осуществляет сбор данных о юридических лицах из ЕС, а не о физических лицах

2. Нет необходимости соблюдать Регламент, если собираемые персональные данные анонимны, т.е. их невозможно по тому или иному критерию соотнести с конкретным лицом. Примером таких данных могут служить статистические данные, данные анонимных опросов и исследований и т.д.

Основные требования

Как было указано выше, принятие Регламента обязывает как компании из ЕС, так и компании из третьих стран, соблюдать определенные требования. Среди всех требований можно выделить наиболее значимые:

Не пропустите

Сексизм на сексизме — подборка скандальной белорусской рекламы

10 вдохновляющих цитат, которые заставят вас по-новому взглянуть на свою жизнь

1. Назначение должностного лица в ЕС, ответственного за защиту этих данных (так называемый Data Protection Officer). Это требование

распространяется не на все компании, а только на те, что обрабатывают в больших объемах «особо важные» личные данные. Так, например, данное требование будет распространяться на компании, собирающие сведения о расовой и этнической принадлежности человека, его политических и религиозных убеждениях, его профсоюзном участии, биометрические и генетические данные, а также данные о привлечении к уголовной ответственности.

Фото с YouTube.com

Вместе с тем, Регламент допускает назначение одного такого должностного лица головной компанией для целой группы дочерних предприятий. Однако для этого головная компания должна обеспечить возможность прямой связи любого дочернего предприятия с таким должностным лицом. Таким образом, оператор данных из стран СНГ, т.е. обрабатывающая персональные данные компания, может не назначать должностное лицо, если оно уже назначено материнской компанией в ЕС, и с ним налажено должное взаимодействие.

2. Ведение документации о сборе персональных данных, которая в случае необходимости раскрывается госорганам ЕС. Обязанность соблюдать это обязательство лежит лишь на компаниях с количеством работников свыше 250 человек, хотя в некоторых случаях и предприятия с меньшим количеством персонала могут подпадать под это требование. Например, если такая компания обрабатывает «особо важные» личные данные: о расе, этнической принадлежности, политических взглядах человека и т.д.

Регламент не устанавливает каких-либо форм ведения отчетности кроме общего требования, что такая отчетность должна быть в письменной форме (или в форме электронного документа). Содержание отчетности зависит от того, распоряжается ли компания собранными данными (контролер данных) или просто выполняет их сбор и обработку по заказу третьей стороны (оператор данных). Так, контролер обязан в такой отчетности отразить цели сбора персональных данных, категории лиц, в отношении которых собирается информация, реципиентов персональных данных из третьих стран, которым эти данные будут предоставлены, принимаемые меры по защите данных. Операторы в свою очередь раскрывают в отчетности применяемые ими методы обработки данных, меры защиты и т.д.

Помимо этого, и контролеры, и операторы персональных данных обязаны раскрыть в своих документах случаи передачи данных в любую страну, не являющуюся участником ЕС.

3. Назначение постоянного представителя в ЕС. Это требование применимо только к тем компаниям, которые на постоянной основе обрабатывают данные физических лиц из ЕС либо работают с «особо важными» личными данными (о расе, этнической принадлежности, политических взглядах и т.д.). Постоянный представитель в ЕС должен выступать от имени компании перед государственными органами по всем

вопросам исполнения требований Регламента. Он также обязан в случае необходимости работать с индивидуальными запросами граждан ЕС, чьи данные обрабатываются.

Фото с сайта everplans.com

Помимо этих требований, Регламент установил и ряд иных обязательных условий:

Необходимость получения согласия в отношении каждой конкретной цели обработки персональных данных

Право пользователя в любой момент отозвать свое согласие на обработку данных

Необходимость письменного одобрения родителями согласия на обработку персональных данных их детей

Извещение государственных органов ЕС о взломах информационных систем и хищении персональных данных не позднее 72 часов с момента, когда о них стало известно

Право пользователя потребовать полного удаления его персональных данных и т.д.

Риски

Регламент устанавливает достаточно высокие штрафы в отношении компаний, нарушивших его требования.

В частности, за некоторые нарушения размер штрафа может достигать 20 миллионов евро или 4% глобального оборота компании (в зависимости от того, что больше).

Однако, пока существует правовая неопределенность относительно того, как будет проходить исполнение решений о взыскании указанных штрафов в третьих странах, не входящих в ЕС.

Таким образом, вступление в силу Регламента может повлечь возникновение для ряда компаний, расположенных в том числе и на территории СНГ, обязательств по защите персональных данных физических лиц из ЕС, игнорирование которых может вылиться в большие штрафы.