ЮРИСТ & ЗАКОН
АНАЛИТИЧЕСКОЕ ИЗДАНИЕ

27.04.2018 – 10.05.2018, № 16

ГЛАВНАЯ СТАТЬЯ

Компетентное мнение

Законодательная борьба Евросоюза за защиту частной жизни своих сограждан

Вступление

Первая эйфория относительно возможностей компьютерных технологий прошла. Интересно заметить, что еще в 1985 г. философ и компьютерный теоретик Джеймс Моор выражал свою озабоченность опасностью незаметности компьютерной технологии. Он считал, что это будет та дверь, которая откроет доступ к скрытому контролю, компьютерному криминалу и нарушению частной жизни. Технология может быть запрограммирована таким образом, что пользователь даже не подозревает, что его данные изымают или за ним тайно подглядывают.

Моор предвидел будущее. На сегодняшний день ежедневное количество скандалов и пострадавших от нарушения частной жизни, слежки, мошенничества, обмана и компьютерного криминалитета выходит за все обозримые рамки. К сожалению, эта проблематика слишком медленно просачивалась в сознание пользователей, профессионалов и законодателей.

Виновники происходящего – это не только компании, рекламные агентства, маркетологи, страховые компании и правительства. Люди сами постоянно выносят друг друга на всеобщее обозрение, не спрашивая разрешения. Примером этому являются видеоролики с насмешками между подростками, мстительные порновидео бывших влюбленных и анонимные нападки в социальных сетях.

В этом месяце печальная попытка самоубийства на террасе, наполненной людьми в Нидерландском городе Розендаале, к всеобщему шоку общественности страны, привела к тому, что наблюдатели вместо того, чтобы помогать бедняге, лихорадочно схватили свои телефоны, чтобы захватить драматическую сцену на камеру и поделиться этим в соцсетях.

Главные этические ценности, на которых основано европейское мировоззрение, подвергаются сегодня постоянной атаке. Онлайн-революция приводит к тому, что не только личная жизнь, но и свобода, независимость, собственное достоинство и социальная справедливость расшатываются во все стороны

в европейском обществе. Из-за культуры страха действия все больше и больше людей регистрируются, что увеличивает конфликт между свободой и безопасностью.

Регламент ЕС о защите персональных данных

В контексте этой технологической, моральной и этической какофонии, которая без преувеличения приобретает хронические формы всеобщего психоза, последствия которых станут по-настоящему видны спустя годы, европейский законодатель предпринимает в этом году попытку защитить общество не только от самого себя, но и от нападок и атак профессиональных компаний и организаций, которые с каждым днем становятся все более изощренными в проникновении в частную жизнь европейских граждан.

В мае этого года в законодательстве Европейского Сообщества в области защиты персональных данных (далее – ПД) будут произведены самые большие изменения за последние два десятилетия. Действующие правила были сформулированы еще в 90-е годы прошлого века, и существующий ныне режим работы с обработкой информации перестал соответствовать действительности и поставленным целям.

Для защиты прав физических лиц в отношении их персональных данных на смену действующей Директиве по защите данных 95/46/ЕС придет новый законодательный акт – Общий Регламент ЕС по защите персональных данных. Регламент имеет целью не просто усилить защиту и расширить права всех граждан ЕС по обеспечению неприкосновенности их персональных данных, он также требует согласования законов о неприкосновенности данных на территории Европейского Сообщества и изменения подхода организаций во всем регионе к проблеме неприкосновенности данных.

Интересно заметить, что новый Регламент напрямую касается и украинских компаний, которые работают на европейских рынках. В данной статье будут рассмотрены главные положения вышеназванного Регламента, а также освещены важные изменения, произошедшие в европейском законодательстве в области защиты ПД.

Главные нововведения в Регламенте ЕС

Новое законодательное положение будет иметь важные последствия не только для физических лиц, но и для компаний, которые занимаются бизнесом в зоне ЕС.

Шесть наиболее важных новшеств Регламента будут состоять в следующем:

1. Более широкий перечень видов предпринимательской деятельности подпадает под действие Регламента. Также, если до нововведения под основополагающее определение "персональные данные" попадали только документы, содержащие имена, адреса и тому подобное, то сейчас это определение было расширено и данные, связанные с IP-адресами, MAC-адресами, cookie-файлы, сохраняющие сугубо индивидуальную информацию о пользователе сети и т. д., также попадут под Регламент.

2. Новый Регламент действует не только на компании, находящиеся в ЕС, но также на предприятия из стран, не входящих в ЕС, которые предлагают товары или услуги субъектам персональных данных в европейских странах или следят за поведением субъектов данных (при условии, что такое поведение имеет место в пределах ЕС). Иными словами, любая обработка персональных данных людей, находящихся в ЕС, будет попадать под нормы, установленные новым Регламентом. Это нововведение очень важно для украинских компаний, так как даже организации, у которых нет офиса или дочерней компании на территории ЕС, но которые поставляют свои услуги на европейский рынок, подвергнутся воздействию Регламента и таким образом любые действия, включающие в себя обработку

персональных данных, будут строго мониториться.

3. Регламент установил новые правила получения согласия на обработку персональных данных. Предыдущая Директива уже ввела правило, что согласие должно всегда быть получено, но теперь это согласие должно быть однозначным и подтвержденным. То есть "молчание, предварительно отмеченные поля галочкой или бездействие" не будут считаться легитимным согласием на обработку персональных данных.

4. ***Регламент вводит несколько основных принципов обработки персональных данных*** и требует от компаний продемонстрировать, как они следуют этим принципам.

1) Законность, справедливость и прозрачность

Принцип законности, справедливости и прозрачности требует не только получения согласия на обработку данных, но также осведомленности субъекта о типе обрабатываемых данных. Информация должна быть представлена ей/ему в прозрачной и доступной форме и изложена понятным и простым языком. В частности, чтобы достичь прозрачности, субъект должен получить информацию о личности контролера, цели сбора информации и также должен быть осведомлен о рисках, законах, защитных мерах и своих правах в отношении обработки данных.

2) Целевое ограничение

Персональные данные могут быть обработаны только для точно обозначенных и законных целей. Если же из первоначальной цели последует другая цель, то согласие должно быть дано для обоих. Однако за этим принципом кроется множество других аспектов. Например, чем больше субъектов обработки данных затронуто, тем точнее цель должна быть описана.

3) Минимизация данных

Личные данные должны соответствовать, иметь отношение и ограничиваться целями, для которых такие данные обрабатываются. Данное положение возвращает к целевому ограничению сбора и обработки персональных данных. Этот принцип должен привести к сокращению сбора данных до минимально возможного уровня.

4) Точность данных

Персональные данные должны быть точными и актуальными. Устаревшие и неточные данные необходимо исправлять или удалять.

5) Ограничение хранения

Персональные данные должны храниться ровно столько, сколько они необходимы для тех целей, для которых они были собраны. Если же хранение больше не требуется, то предприятия должны удалять эти данные. Регламент также уточняет, что компании должны проводить регулярные проверки с целью чистки устаревшей информации.

6) Целостность и конфиденциальность

Данный принцип затрагивает основу защиты частной жизни людей. В соответствии с данным принципом контролер должен удостовериться, что данные защищены от несанкционированной и незаконной обработки.

7) Седьмой принцип: отчетность

Принцип отчетности, установленный новым Регламентом, налагает на компании ответственность за соблюдение всех вышеупомянутых правил. Компании должны удостовериться, что они соблюдают все технические и организационные требования и уполномоченные организации имеют право потребовать от организаций все отчеты об обработке персональных данных.

Увеличение внимания к соблюдению требований, проистекающих из данного принципа, явилось одним из наиболее значимых и строгих изменений, которые вносит Регламент.

5. ***Регламент наделяет частных лиц рядом новых прав***, а также укрепляет некоторые права, уже существовавшие в рамках предыдущей Директивы, а именно:

1) Право на перемещение данных

Регламент вводит право частных лиц на получение, копирование и перенос их персональных данных в базы другого контролера и/или обработчиков данных. Это правило было внесено с целью защиты прав потребителя и влечет за собой значительные усилия со стороны организации-контролера, обрабатывающей эти данные.

2) Право возражения

Регламент позволяет частным лицам возражать определенным видам обработки их персональных данных: прямому маркетингу (прямое обращение к лицам через электронную почту или рекламные объявления на веб-сайтах), обработке с целью защиты законных интересов или выполнения какой-либо задачи в общественных интересах / реализации властных полномочий, а также обработке данных в исследовательских или статистических целях.

3) Право на удаление данных

Регламент позволяет частным лицам требовать уничтожения или удаления их персональных данных, если эти данные больше не нужны для тех целей, для которых они были собраны, объект обработки снял свое соглашение, объект обработки возражает или информация была незаконно обработана.

4) Право на ограничение обработки данных

Регламент гарантирует, что при наложении ограничения на обработку ПД компаниям разрешается хранить персональные данные, но им не разрешается их обрабатывать.

5) Право на получение ответа на запрос

Если частное лицо не знает о том, что его данные обрабатываются, и о том, как они обрабатываются, то оно не сможет осуществлять все остальные права. Таким образом, организация должна отвечать на любые запросы объекта обработки о собранных о нем данных.

6. В случае утечки персональных данных контролер данных обязан довести этот факт до сведения Комитета по защите персональных данных (регулятора) не позднее чем через 72 часа после того, как контролеру стало известно о такой утечке. Это правило может не соблюдаться только в случае, если это маловероятно, что права и свободы людей будут нарушены. Но также согласно Регламенту компании обязаны документировать факты утечки данных, даже если о таких утечках не сообщается в Комитет по защите персональных данных. Организации-контролеры ПД к тому же обязаны вести внутренний журнал учета случаев взлома данных.

Если же нарушение какой-либо статьи Регламента будет установлено, это может привести к штрафу в размере до 20000000 евро или до 4 % от мирового годового оборота компании.

Преимущества и недостатки нового закона

В основном Регламент повлияет положительно на развитие бизнеса, но также он может привнести определенные преграды. В данный момент 28 государств – членов ЕС имеют разные и противоречивые законы о защите персональных данных, что усложняет работу компаний. Благодаря появлению Регламента эти законы будут гармонизированы и ничем отличаться не будут. В то же время закон очень часто подвергается критике, так как множество правил кажутся слишком строгими и остается много места для интерпретации.

Заключение

Несмотря на то, что Моор и вправду предвидел будущее и интернет-технологии в наше время влекут за собой скрытый контроль, компьютерный криминал и нарушение частной жизни, европейский законодатель пытается защитить своих граждан от нарушения их прав. Новый Регламент – серьезная попытка Евросоюза на пути к обеспечению надежной защиты неприкосновенности, на сегодняшний день шаткой, частной жизни и персональных данных граждан ЕС и людей, находящихся в европейских странах.

Самым главным новшеством является не только тот факт, что действие Регламента распространяется на страны, не входящие в ЕС, но также ужесточенные правила по получению согласия на обработку персональных данных, 7 главных принципов обработки данных и увеличенные штрафы.

С первого взгляда новый Регламент может казаться слишком сложным и влекущим за собой слишком серьезные последствия, так как он также затрагивает украинские компании. Но, с другой стороны, самым большим преимуществом Регламента является потенциальное упорядочение разрозненных норм и правил. До сих пор компаниям приходилось учитывать правила по защите данных 28 различных государств – членов ЕС. Таким образом, чтобы закон и возможные штрафы никак не затронули украинские компании, очень важно спланировать детальную стратегию и пройти этапы подготовки внедрения политики практики соблюдения требований нового Регламента.

Максим Ходак,
адвокат
Адвокатской конторы Law & More (Нидерланды)