ROMAN PUSEP
Rechtsanwalt,
Fachanwalt für IT-Recht

Остался лишь месяц и европейское постановление о защите персональных данных (Datenschutz-Grundverordnung, DS-GVO) окончательно вступит в силу, а точнее, с 25 мая 2018 года. В связи с этим на нашем форуме увеличивается количество сообщений, вопросов и дискуссий по этому поводу. Например, наших абонентов (турбюро) всё чаще и чаще посещают представители ИТ-компаний, сообщают им о «законной необходимости» файервала и антивируса, и предлагают им свои услуги за техническое оборудование, его установку и ежемесячную поддержку. Стоимость составляет не редко более 3.000 евро плюс более 100 евро ежемесячно.

Этот конкретный вопрос мы задали адвокату Роману Пусепу (Roman Pusep), партнеру адвокатского бюро WERNER RI (Кёльн). Адвокат Роман Пусеп – сертифицированный специалист в области права информационных технологий, у него более 10-летний опыт в этой области и, в частности, по праву защиты личных данных.

Господин Пусеп ответил на этот вопрос так.

Reisebüros werden werden immer häufiger von IT-Dienstleistern angesprochen, um angeblich zwingend erforderliche Firewall- und Antiviren-Technologie (Software und Hardware) einzusetzen. Dies ist in den allermeisten Reisebüros tatsächlich zwingend erforderlich – wegen der DS-GVO, aber nicht nur.
Die neuen Regeln werden also die Technik professioneller und sicherer machen. Dennoch sollten die Unternemen vorsichtig sein und Angebote prüfen.

DS-GVO:

Техническое оснащение в турбюро обязательно станет профессиональнее и безопаснее

Ваши абоненты (турбюро) хотят непосредственно знать, как оценить «поведение» представителей ИТ-компаний. Действительно ли хотят эти компании предложить свои «по новому постановлению обязательные» услуги за адекватную цену или просто используют панику перед огромными штрафами (до 20 миллионов евро) и, попав в эту струю, навязать турбюро ненужные услуги или по намного завышенным ценам.

Ниже – во второй половине статьи – я отвечу на этот вопрос. Но для того чтобы мой ответ лучше понять и сделать индивидуальные выводы для каждого турбюро, необходимо сначала понять смысл, суть и рамки нового постановления. Это я попытаюсь объяснить в первой половине статьи.

1. СМЫСЛ, СУТЬ И РАМКИ НОВОГО ПОСТАНОВЛЕНИЯ

На данный момент почти все средства массовой информации занимаются вопросами DS-GVO, используя предисловием следующий лозунг: Европейское постановление было введено в основном по вине таких предприятий, как Google, Facebook и т.д., а представители малого и среднего бизнеса несут пошлину (отчасти очень дорогостоящую) при реализации новых правил. С моей точки зрения, это правильная оценка ситуации, но она не меняет закона. Поэтому не стоит тратить энергию, оплакивая новые правила, а заниматься их соблюдением.

DS-GVO введено для оптимальной, может даже максимальной, защиты личных данных физических лиц. И действительно, постановление было необходимо. Мы все, физические и юридические лица, на данный момент в основном слишком халатно относимся к своим и к чужим личным данным. У кого из нас нет смартфона, в который мы изо дня в день задаём массу своих и чужих данных, предоставляя их массе предприятий, которые используют их в своих целях.

В связи с этими рисками одно из нововведений DS-GVO – это информация о защите данных. **Обширные информационные обязательства** ответственных лиц находятся в основном в ст. 13 и 14 DS-GVO. Затронутые лица (клиенты, сотрудники, посетители веб-сайта и т.д.) должны быть проинформированы о том, что происходит с их личными данными. Информация касается всех видов обработки личных данных и охватывает, в частности:

● Контактные данные ответственного лица и его представителя.

● Контактные данные сотрудника по защите личных данных, если таков назначен.

● Цели обработки личных данных и статья DS-GVO, по которой эта обработка разрешена.

● При передаче личных данных третьим лицам – их категории (например, банк, страховка).

● При передаче личных данных за рубеж ЕС – уровень безопасности личных данных в стране получателя.

● Длительность сохранения личных данных у ответственного лица (например, когда они стираются на сервере).

● Право затронутого лица на получение полной информации по обработке его личных данных ответственным лицом.

● Право затронутого лица на внесение поправок в его личных данных у ответственного лица.

● Право затронутого лица на удаление его личных данных у ответственного лица.

● Право затронутого лица на перевод его личных данных от ответственного лица к другому ответственному лицу.

● Право затронутого лица на отказ от согласия будущей обработке данных ответственным лицом.

● Право затронутого лица на жалобу в органы защиты личных данных.

Перед тем, как выполнить свои информационные обязательства, возможно, ответственное лицо (в нашем случае турбюро) встанет перед вопросом: **что такое личные данные**, т.е. какие данные должны быть охвачены в информации затронутого лица (в нашем случае, например, клиента)? Этим вопросом занимается, например, ст. 4 № 1 DS-GVO и ст. 4 № 13 до 15 DS-GVO. В этой правовой области было и есть очень много проблем и нерешенных вопросов. Но одновременно DS-GVO в одном вопросе оказало юристам огромную услугу, упростив их деятельность. По ст. 4 № 1 DS-GVO, личные данные – это, в частности, все данные, которые относятся к затронутому лицу. В случае турбюро и его базы данных клиентов – это все данные клиента. К этим данным относятся имя, фамилия, дата рождения, место рождения, пол, данные сопровождающих (супруги, партнеры, дети, родители и т.д.), паспортные данные, место жительства, телефонные номера, электронная почта, банковские реквизиты, времена отпусков, цели отпусков, стоимость отпусков, заключенные страховки, особенности здоровья (например, заболевания, инвалидное кресло) и многое другое.

Потребуется ли в будущем **сотрудник по защите личных данных**? Ответить на этот вопрос помогут ст. 37 до 39 DS-GVO и будущий § 38 BDSG-neu. Такой сотрудник по новому постановлению (и, в общем, на данный момент по действующему BDSG), в принципе, обязателен всем тем предприятиям, которые обрабатывают личные данные и занимаются этим там 10 человек или более. Так что если в турбюро работают не менее 10 человек, то сотрудник по защите личных данных обязателен.

Однако если в турбюро работает менее 10 человек, то не факт, что защитник данных не обязателен. По выше названным новым правилам DS-GVO и BDSG-neu сотрудник по защите личных данных необходим во всех предприятиях, которые обширно обрабатывают личные данные особенного уровня риска. По ст. 9 DS-GVO к таким данным относятся генетические, биометрические и данные по здоровью, вероисповеданию, сексуальной жизни и ориентации. Об этих пунктах необходимо задуматься.

Однако, с моей точки зрения, этот вопрос можно относительно быстро решить, применив простую схему: если обработку таких личных данных в конкретном предприятии нужно долго искать или это происходит лишь в единичных случаях (например, если для каждого 100-го клиента нужна рампа для инвалидного кресла), то «обширная» обработка таких данных отсутствует и сотрудник по этой предпосылке не обязателен.

Для юридически не опытных может показаться и следующее правило в § 38 BDSG-neu «опасным», особенно для турбюро: сотрудник по защите личных данных обязателен во всех предприятиях, чьё делопроизводство заключается в передаче личных данных. По сути, все посредники (как турбюро или маклер) берут личные данные клиентов, чтобы сообщить их далее либо в отель, либо в авиакомпанию, либо туроператору на месте отдыха.

Но могу успокоить: с моей точки зрения, это правило к посредникам не относится. Оно касается только тех предприятий,

ОКОНЧАНИЕ НА СТР. 46

ОКОНЧАНИЕ. НАЧАЛО НА СТР. 44

ОКОНЧАНИЕ. НАЧАЛО НА СТР. 44

которые занимаются исключительно передачей личных данных, например, продавая эти данные.

Есть и другие факторы, по исполнению которых становится необходим сотрудник по защите личных данных. Но они в крайнем случае и только в виде исключения могут коснуться турбюро.

Хочу обратить внимание на то, что сотрудник по защите личных данных должен обладать знаниями и квалификацией (ст. 37 DS-GVO). Возможно, сотрудника нужно будет, или предварительно или непосредственно после назначения, обучить.

На этом я хотел бы закончить первую часть моей статьи. Конечно, есть еще множество тем, которые можно «обсудить» по поводу DS-GVO, например, обязательства по документации, особенные правила при передаче личных данных за рубеж ЕС (например, Office365), и, наконец, во всех статьях на эту тему упомянутые жесткие штрафы до 20 млн. евро. Однако все эти темы невозможно обрисовать в рамках введения в DS-GVO.

2. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОСНАЩЕНИЮ

Несомненно, DS-GVO ставит предпринимателей перед очень сложными задачами. Но постановление особенно охватит тех предпринимателей, которые до сих пор не заботились о защите данных по требованиям BDSG. Они должны будут приложить втрое или даже вчетверо больше персональных и финансовых усилий и действовать очень быстро, реализуя новое постановление.

Техническое обеспечение играет огромную роль в DS-GVO, ведь постановление в первую очередь действует для/при автоматизированной (т.е. компьютерной) обработке личных данных (ст. 2 DS-GVO).

Предприятие должно организовать процессы (особенно технические, а также и организационные) обработки личных данных в соответствии с принципами защиты личных данных (ст. 5 DS-GVO), то есть законность, прозрачность, целевое назначение, минимизация данных, правильность, ограничение хранения, целостность, конфиденциальность и подотчетность.

Технически DS-GVO предусматривает внедрение и использование различных программ и техники. Предприятия должны анализировать риски каждого процесса обработки личных данных, и принять в соответствии с уровнем конфиденциальности личных данных, в соответствии с подвержением их определенным рискам и в соответствии с финансовыми возможностями предприятия меры, чтобы избежать риска полностью или значительно его уменьшить. В соответствии со ст. 32 DS-GVO это может быть, например, псевдоминимизация, шифрование, быстрое восстановление (например, резервные и параллельные системы). Всё индивидуально и зависит от бизнес-процессов предприятия.

Прошу не уделять критерии «финансовых возможностей» особенно сильное значение. Этот параметр ни в коем случае не значит, что «бедное» предприятие не обязано предпринимать никаких мер технической безопасности.

При компьютерной обработке личных данных существует минимальный уровень защиты, который настолько само собой разумеющийся, что он как таковой не упомянут в законодательстве (но есть и другие технические источники, как, например, BSI-Grundschutz или ISO-правила). Приведу пример из нецифрового мира: предприятие, обрабатывающее личные данные, должно закрывать (по крайней мере на ночь) бюро на дверной замок и закрывать окна, а не на засов, оставляя форточку открытой. Эта обязанность касается и тех предприятий, у которых нет денег на замок или на починку сломавшегося окна. Переводим этот пример в цифровой мир: к минимальному уровню технической защиты относится, например, пароль. На сколько он должен быть сложный – дело каждого конкретного предприятия. Но ни в коем случае пароль не должен иметь менее чем 8 знаков, также в его состав должны входить буквы, цифры и другие знаки (например, $ или #).

Вот мы и подошли непосредственно к исходному вопросу читателей: использование файервала и антивируса. Эти две меры технического оборудования относятся к минимальному стандарту защиты личных данных на компьютерных системах предпринимателей. Без этих систем компьютерная обработка личных данных практически немыслима.

Возможно только одно исключение – если компьютер с базой данных клиентов турбюро находится на компьютере, не связанном с Интернетом. Более того, обязательно исключить также всякий другой путь «заражения», например, через интерфейс: USB-флешка, DVD-ROM, CD-ROM и т.д. Это исключение я считаю лишь теоретическим и практически немыслимым в турбюро.

Так что представители ИТ-компаний затронули, в принципе, очень важный и правильный вопрос. Однако не исключено, что их деловые предложения, тем не менее, не серьезны с финансовой стороны. Поэтому я рекомендую обратиться к нескольким ИТ-компаниям и сравнить их предложения, анализируя при этом не только цену, но и техническую сторону предложения.

В заключении я хочу обратить внимание читателей на то, что файервал и антивирус лишь два (сравнительно незначительных) аспекта технического оснащения. С технической точки зрения существует множество каналов для нападения. Всех их необходимо анализировать и, возможно, принять меры. ■