«DS-GVO. Защита персональных данных коснется всех компаний»

Интервью с адвокатом Р. Пусепом (Roman Pusep)

Буквально за несколько дней до сдачи номера в печать состоялась встреча с адвокатом Романом Пусепом, партнером адвокатского бюро WERNER RI г. Кёльн.

Адвокат Р. Пусеп является специалистом в области права информационных технологий, имеет более 10 лет практического опыта организации защиты данных для немецких предприятий и представляет интересы клиентов при спорах в различных государственных органах и судах.

Пользуясь возможностью, редакция журнала «Партнёр» взяла интервью у господина Пусепа о планируемых изменениях в европейском законодательстве о защите персональных данных, вводимых с 25 мая 2018 года.

В тексте использованы аббревиатуры законодательных актов:

DS-GVO *(EU-Datenschutz-Grundverordnung) – Положение о защите данных ЕС*

BDSG *(Bundesdatenschutzgesetz) – Федеральный закон о защите данных.*

В скобках приведены уточнения и пояснения редакции.

RA Roman Pusep
Fachanwalt für IT-Recht
WERNER Rechtsanwälte Informatiker
Oppenheimstraße 16, 50668 Köln
Tel.: 0221 97314373
E-Mail: roman.pusep@werner-ri.de
https://www.werner-ri.de

Господин Пусеп, кого коснутся ожидаемые с 25 мая изменения в законодательстве о защите персональных данных? Читателей интересует, в первую очередь, затронут ли нововведения представителей малого и среднего бизнеса?

Адвокат Р. Пусеп

Будет затронут практически весь бизнес, размер компании не важен. Единственное, что имеет значение – это обработка персональных данных на предприятиях.

Какие именно данные являются персональными (*личными*), было подробно изложено в мартовском номере журнала (*03 / 2018*), с перечнем прав можно ознакомиться в ст. 4 № 1 и 13-15 DS-GVO.

На сегодняшний день практически невозможно управлять бизнесом без обработки личной информации клиентов. Я посмотрел, например, каталог фирм на вашем сайте (*портал www.partner-inform.de*). Предприятия практически всех отраслей – туристические агентства, авиакомпании, розничные торговцы, салоны красоты, гостиницы, страховые компании, бухгалтеры и т.д. – имеют дело с персональными данными, такими как: имя, фамилия, адрес, дата рождения, банковские реквизиты. Некоторые компании, например, врачи и фармацевты, кроме «стандартного» набора обрабатывают данные повышенного уровня риска (ст. 4 № 13-15 DS-GVO, ст. 9 DS-GVO), такие как данные медицинского страхования, диагнозы и прочее.

Повсеместно компании работают и с данными их сотрудников, которые необходимо обрабатывать из-за многочисленных юридических и контрактных требований. Любая современная компания обрабатывает данные. Поэтому защита данных играет определенную роль в любом бизнесе.

Найти компанию, в которой полностью исключена обработка личной информации, невозможно. Теоретически это могла бы быть фирма, которая:

принимает только наличные платежи;

не ведет видеонаблюдение;

не хранит списки клиентов (например, для предварительных заказов);

никаким образом не поддерживает с клиентами связь (например, письмом, факсом или электронной почтой);

и, в конце концов, у которой в штате нет ни одного наемного сотрудника.

Исключение составляют только одномандатные предприятия, у которых в штате нет ни одного наемного сотрудника.

К вопросу о том, какие предприниматели особенно затронуты. Это, прежде всего, те компании, которые до сих пор не были обеспокоены защитой данных (по требованям BDSG). Они должны приложить максимум усилий и действовать очень быстро, ведь размер возможных штрафов и иных последствий напрямую зависит от степени нарушения законодательства о защите данных.

Расскажите, пожалуйста, какие первоочередные действия должно предпринять руководство компаний для организации надлежащего уровня безопасности по защите и использованию собранной личной информации о клиентах и сотрудниках?

1. Обезопасить видимый «снаружи» открытый фланг предприятия. Обязательно проверить и ввести поправки в IMPRESSUM и DATENSCHUTZHINWEISE на вебсайте, который видят все: конкуренты и проверяющие органы. Далее можно заниматься «внутренними» темами предприятия:

2. Проверить, должен ли быть назначен сотрудник по защите данных (ст. 37-39 DS-GVO).

3. Подготовить процедурный каталог (ст. 30 DS-GVO). Рекомендую предварительно проанализировать все процессы обработки и, если необходимо, упорядочить их.

4. При необходимости провести оценку воздействия защиты данных (ст. 35 DS-GVO).

5. Документировать все действия, связанные с организацией защиты персональных данных, чтобы по требованию проверяющих органов доказать такие действия.

Вы упомянули сотрудника предприятия по защите данных. Поясните читателям, когда наличие в штате предприятия сотрудника по защите информации обязательно?

Требуется ли сотрудник по защите данных или нет, следует рассматривать в каждом отдельном случае. Основные требования, регулирующие данный вопрос, изложены в ст. 37-39 DS-GVO и в будущем §38 BDSG-neu. Помимо «мягких» (*косвенных*) факторов, которые многим не сразу понятны, есть также четкие и ясные требования: согласно §38 BDSG-neu, компании должны назначить сотрудника по защите данных, если не менее 10 человек участвуют в автоматизированной обработке персональных данных. Это во многом корреспондирует с актуальной правовой позицией в §4f BDSG (*действующий Федеральный закон о защите данных*).

Кроме того, юридическое сообщество считает, что в любом случае назначать сотрудника по защите данных обязаны: юристы, врачи, лабораторные операторы и фармацевты, поскольку они обрабатывают личные данные, которые имеют повышенное значение для их защиты. Также есть много других факторов и предпосылок, которые в рамках нашей беседы невозможно обрисовать.

Обращаю внимание читателей, что сотрудник по защите данных должен обладать знаниями и квалификацией в соответствии со статьей 37 (5) DS-GVO. Поэтому назначить любого сотрудника не получится, по крайней мере, без предварительного обучения.

Сотрудник по защите данных должен обладать знаниями и квалификацией. Любого сотрудника назначать нельзя!

Кроме назначения сотрудника по защите данных, нужно ли проводить дополнительный инструктаж персонала компании?

Сотрудники предприятий должны уделять особое внимание принципам защиты данных согласно ст. 5 DS-GVO. Работодатель должен, в соответствии с действующим законом, обязать сотрудников «соблюдать секретность данных» в соответствии с § 5 BDSG. Обычно это делается в письменной или иной другой форме, которую можно предъявить для доказательства. В DS-GVO не существует сопоставимого регулирования. В будущем, возможно, станет актуальным положение ст. 29 DS-GVO, в соответствии с которым «лица, подпадающие под контроль и имеющие доступ к персональным данным», могут обрабатывать персональные данные «исключительно по указанию ответственного лица». Форму этой инструкции законодатель не регулирует, но желательно ее оформить также в письменном виде. Эта статья систематически включается в раздел DS-GVO по обработке персональных данных для ответственного лица по его заказу, так что эта статья не прямо действует на отношения между работодателем и сотрудником. Юридическая дискуссия по этому вопросу еще не завершена.

В DS-GVO один из разделов посвящен Процессору, кто это?

«Processor» – это английский термин для лица, обрабатывающего персональные данные по заказу компании (ответственного лица), например, налоговый консультант при подготовке учета заработной платы.

Спасибо, что прояснили требования к ответственным лицам. Хотелось бы выяснить, какие новые требования предъявляются к внутренней документации предприятия. На какие документы следует обратить особое внимание?

Прежде всего, важны следующие документы или документация:

1. Каталог обработки: это описание всех процессов, в ходе которых обрабатываются персональные данные.

2. Концепция удаления: предприниматель должен подумать о том, какие персональные данные из его процессов (они описаны в каталоге обработки) удаляются и в соответствии с какими критериями. Например, временной критерий – через 10 лет.

3. Информация о защите данных: DS-GVO представляет собой обширные информационные обязательства, особенно в ст. 13 и 14 DS-GVO. Затронутые стороны, клиенты и сотрудники, должны быть проинформированы о том, что происходит с их личными данными.

4. Согласие: если обработка данных происходит на основе согласия, то оно должно быть задокументировано. Тем не менее, согласие действует только касательно той обработки персональных данных, которую ответственное лицо описало дла получения согласия, т.е. согласиться можно только на те меры обработки, которые были оглашены, так что это тоже подлежит документированию.

Каким образом следует организовать процессы обработки информации?

Предприятие должно организовать процессы обработки данных так, чтобы они соответствовали принципам защиты данных (ст. 5 DS-GVO), то есть законность, прозрачность, целевое назначение, минимизация данных, правильность, ограничение хранения, целостность и конфиденциальность, подотчетность.

Вы упоминали Процессора. Многие компании передают данные на аутсорсинг, например, для ведения бухгалтерского учета. Как обезопасить себя при передаче данных сторонним исполнителям?

При аутсорсинге (обработка заказа в соответствии со ст. 28 DS-GVO) важно выбрать надежного обработчика данных и обязательно документировать как критерии этого выбора, так и сами договорные взаимоотношения (контракт). Кроме того, контракт на оформление заказа (услуги) должен соответствовать требованиям законодательства.

Например, в случае учета заработной платы это означает, что вам необходимо сначала получить от налогового консультанта сведения о технико-организационных мерах. Их следует рассматривать и анализировать в соответствии с требованиями DS-GVO.

Следующий шаг – это проверка реализации действенности таких мер. Поэтому на практике налоговый консультант должен будет пройти аудит, в котором безопасность процесса обработки будет подтверждена. Тогда договор может быть заключен. Наше бюро (*WERNER RI*) рекомендует клиентам проводить регулярные проверки Процессора в течение всего периода договорных отношений; но делать это не всегда стоит и не всегда разрешено самому предприятию – для этого есть специалисты. Кроме указанных действий, работодатель обязан также сообщить сотрудникам, что учет заработной платы будет выполнен назначенным бухгалтером.

Многие предприятия ведут активные бизнес-процессы в интернете. На что следует обратить внимание при ведении бизнеса онлайн?

В случае бизнес-деятельности в интер-

нете очень важно, чтобы на веб-сайте присутствовала политика конфиденциальности. Это первое, на что смотрит контролирующий орган, а также и конкуренты, желающие вам «насолить». Пользователь должен быть проинформирован о том, какие персональные данные собираются, когда, как, с какой целью и как долго обрабатываются.

Есть много особенностей, которые следует учитывать при активных онлайн действиях. Например, анализ с помощью Cookies-файлов; использование инструментов анализа, таких как GoogleAnalytics или Matomo (ранее Piwik); интеграция социальных сетей, Facebook, XiNG, Twitter или других кнопок; интеграция карт Google или шрифтов Google.

Если предприятие использует *Newsletter* (новостную рассылку), то также требуется соблюдение определенной процедуры, так называемой Double-Opt-In. Другая юридическо-техническая тема затрагивает использование пикселей, так называемых Zählpixel.

Раз уж Вы засыпали читателей техническими терминами, то следующий вопрос, какое техническое обеспечение требуется согласно законодательству?

Технически, DS-GVO предусматривает внедрение и использование различных программ и техники. Предприниматель должен проанализировать риски обработки данных и рассмотреть, какие меры применять в соответствии со ст. 32 DS-GVO. Например, это может быть псевдоминимизация, шифрование, быстрое восстановление (например, резервные и параллельные системы). Всё индивидуально и зависит от бизнес-процессов фирмы.

А если техника подвела? Что делать в случае потери данных?

Согласно ст. 33 DS-GVO, ответственное лицо обязано сообщить органу по защите данных о потере данных в течение 72 часов (3 дня) после того, как инцидент станет известен в компании. Минимальное содержание уведомления также регламентируется указанной нормой. Кроме того, при определенных условиях соответствующее лицо или все затронутые лица также должны быть уведомлены, в соответствии со ст. 34 DS-GVO. Наконец, согласно ст. 32 DS-GVO, необходимо инициировать процедуру исправления происшествия и создания более безопасных процессов, чтобы инцидент больше не мог повториться.

Какова ответственность за нарушения, за что и на какую сумму могут наказать предприятие?

Согласно ст. 83 (4) DS-GVO, предусмотрен штраф в размере до 10 млн евро или до 2% годового оборота (в зависимости от того, что больше), в частности за нарушение норм следующих статей:

– ст. 8 DS-GVO (условия для согласия ребенка в отношении услуг информационного общества);

– ст. 11 DS-GVO (обработка, для которой идентификация субъекта данных не требуется);

– ст. 30 DS-GVO (перечень видов деятельности по переработке – перечень процедур);

– ст. 33 DS-GVO (уведомление о нарушениях защиты персональных данных надзорному органу);

– ст. с 37 до 39 DS-GVO (ответственный за защиту данных).

В соответствии со ст. 83 (5) DS-GVO, предусмотрен штраф в размере до 20 млн евро или до 4% годового оборота (в зависимости от того, что больше), в частности за нарушение:

– ст. 5, 6, 7 и 9 DS-GVO (согласие);

– ст. с 12 до 22 DS-GVO (права субъектов данных, включая уведомления о конфиденциальности);

– ст. с 44 до 49 DS-GVO (передача данных в третьи страны).

А кто контролирует соблюдение законодательства об охране данных? Кого можно ждать в гости?

Государственный орган защиты данных. Он может применять различные меры в соответствии со ст. 58 DS-GVO. Например, запросить информацию, провести аудит, посетить бизнес-помещения для расследования обработки данных. Несоблюдение указаний государственного органа защиты данных, согласно ст. 83 (6) DS-GVO, также может привести к штрафу в размере до 20 миллионов евро или до 4% годового оборота (в зависимости от того, что больше).

Большие штрафы предусмотрены за нарушение правил передачи информации в третьи страны. О чем должны знать предприниматели из третьих стран (не ЕС), занимающиеся бизнесом в Германии, или немецкие бизнесмены, у которых, например, сервер расположен в третьих странах?

Обработка данных в третьих странах – очень сложная тема, так что приведу лишь несколько требований законодательства.

Согласно ст. 45 DS-GVO, данные могут быть переданы странам, для которых ЕС принял соответствующее решение, например, для передачи в США – применяется EU-US Privacy Shield.

Согласно ст. 46 DS-GVO, данные могут быть переданы, например, при соблюдении стандартного положения о защите данных (ранее: стандартные договорные положения) или если у обеих сторон проведена сертификация в соответствии со ст. 42 DS-GVO.

До сих пор еще нет аккредитованных компаний, которые могут проводить сертификационные проверки.

Согласно ст. 47 DS-GVO, компании из одной группы (концерн) могут передавать личные данные друг другу, если они имеют обязательные внутренние правила защиты данных (ранее обязательные корпоративные правила). Однако они должны быть одобрены властями.

С какими самыми распространенными ошибками предпринимателей Вы сталкиваетесь?

Каждый случай настолько различен, что я не могу привести или назвать список наиболее частых ошибок при организации деятельности по защите конфиденциальности.

Каков типичный перечень затрат? Для каких предприятий эти затраты особенно велики?

Стоимость внедрения вряд ли может быть оценена. Это зависит от многих очень разных факторов. Например, в зависимости от того, работает ли сегодня компания в соответствии с BDSG; сколько процессов существует в отношении персональных данных; есть ли сотрудник по защите данных; какой основной вид деятельности и т.д.

От лица наших читателей хотелось бы поблагодарить Вас, господин Пусеп, за интервью.

Пожалуйста. В случае возникновения дополнительных вопросов относительно организации защиты персональных данных на немецких предприятиях я с удовольствием отвечу на них при следующей встрече! ■■■

Беседу вёл Юрий Джуваго

Уважаемые читатели!
Уважаемые предприниматели!

Нам важно Ваше мнение! Вопросы по проблеме защиты данных просим задавать любым удобным для вас способом:

- на интернет-портале в разделе «Вопросы и ответы» http://www.partner-inform.de/faq/zashhita-dannyh-i-bezopasnost/73/
- на электронную почту i.dzhuvago@partner-inform.de
- в письменном виде на адрес редакции.

Ответы специалистов будут опубликованы на интернет-портале и в следующих номерах журнала.