Local Knowledge
for Global Business

www.gratanet.com

Общий регламент ЕС по защите данных (GDPR): территориальное действие

Общий регламент по защите данных (General Data Protection Regulation), принятый Европейским парламентом 17 декабря 2015 г. (далее - «Регламент» или «GDPR») вступил в силу с 25 мая 2018 г.

Статья 3 Регламента устанавливает два основных критерия его действия по территории: «критерий учреждения» и «критерий направленности».

Регламент действует в отношении организаций, имеющих в ЕС «учреждения» (англ. establishment), где персональные данные обрабатываются «в контексте деятельности» такого учреждения, независимо от того, на территории ЕС или нет фактически происходит обработка данных. Учреждение подразумевает эффективное и реальное осуществление деятельности посредством «стабильной организации», независимо от их юридической формы - будь то через филиал или дочернее предприятие.[1]

Требования Регламента применяются также к организациям, не учрежденным в ЕС, если они обрабатывают персональные данные субъектов персональных данных (физических лиц) находящихся в ЕС в связи с:

1) предложением им товаров или услуг (без требования оплаты); для предложения товаров и услуг Интернет-сайт должен быть не просто доступен в ЕС, но должно быть очевидно, что организация «предвидит», что ее деятельность будет направлена на субъектов персональных данных в ЕС;

2) мониторингом поведения таких субъектов персональных данных в ЕС, то есть отслеживанием отдельных пользователей в Интернете для создания профилей, в том числе, когда это используется для принятия решений для анализа/прогнозирования личных предпочтений, поведения и отношения.

На практике, вместе с тем, возникает множество вопросов в связи с применимостью требований Регламента в отношении обработки персональных данных организациями как находящимися на территории ЕС, так и вне ее.

16 ноября 2018 г. Европейский совет по защите данных (EDPB) принял Руководящие принципы 3/2018 по территориальному действию GDPR (Статья 3).

В документе даны разъяснения относительно действия Регламента по территории при различных сценариях, которые могут возникнуть в зависимости от вида деятельности по обработке персональных данных, организации, осуществляющей эти виды обработки, или местонахождения таких организаций. В Руководящих принципах вместе с тем подчеркивается важность для контроллеров и операторов персональных данных, особенно тех, кто предлагает товары и услуги на международном уровне, проводить тщательный анализ конкретно их деятельности по обработке персональных данных с тем, чтобы определить, подпадает ли такая обработка под требования Регламента.

1. Критерий учреждения

EDPB рекомендует трехэтапный подход для определения того, попадает ли обработка персональных данных под действие Регламента в соответствии со статьей 3 (1).

a) «Учреждение в ЕС»

Сначала необходимо определить лицо, которое является контроллером или оператором для целей обработки.

«Контролер» для целей Регламента означает физическое или юридическое лицо, орган государственной власти, агентство или иное учреждение, которое самостоятельно или совместно с другими определяет цели и средства обработки персональных данных.

«Оператор» означает физическое или юридическое лицо орган государственной власти, агентство или иное учреждение, которое обрабатывает персональные данные от имени контролера.

Для того, чтобы определить, имеет ли организация, находящаяся за пределами ЕС, учреждение в государстве-члене ЕС, как степень стабильности организации, так и фактическое осуществление деятельности в этом государстве-члене должны быть рассмотрены в свете специфики соответствующей экономической деятельности и предоставления услуг.

Особенно это касается предприятий, предлагающих услуги исключительно через Интернет, для которых порог для «стабильной организации» может фактически быть довольно низким, в результате чего в некоторых случаях присутствие одного сотрудника или агента организации, не учрежденной в государстве-члене ЕС, может быть достаточным для создания «стабильной организации», если этот сотрудник или агент действует с достаточной степенью стабильности.

Например, компания по производству автомобилей со штаб-квартирой в США имеет свой филиал и офис, расположенный в Брюсселе, контролирующий все ее операции в Европе, включая маркетинг и рекламу. Бельгийский филиал можно считать стабильной организацией, которая осуществляет реальную и эффективную деятельность в свете характера экономической деятельности данной компании - производителя автомобилей.

b) Обработка персональных данных "в контексте деятельности" учреждения

EDPB полагает, что для целей статьи 3 (1) Регламента значение «обработки в контексте деятельности учреждения контроллера или оператора» следует понимать в свете соответствующих прецедентов. С одной стороны, с целью достижения цели обеспечения эффективной и полной защиты прав субъектов персональных данных, значение «в контексте деятельности учреждения» не может быть интерпретировано ограничительно. С другой стороны, существование учреждения в значении Регламента не следует толковать слишком широко, чтобы сделать вывод о том, что существование любого присутствия в ЕС с даже самыми отдаленными связями с деятельностью по обработке персональных данных организацией, не учрежденной в государстве - члене ЕС, будет достаточно, чтобы считать такую обработку подпадающей под требования Регламента.

i. Связь между контроллером данных или оператором вне ЕС и учреждением в ЕС

Если анализ в каждом конкретном случае будет свидетельствовать о том, что существует неразрывная связь между деятельностью учреждения в ЕС и обработкой персональных данных, осуществляемой контроллером, не учрежденным ЕС, законодательство ЕС будет применяться к такой обработке, независимо от того, играет ли учреждение такого контролера в ЕС роль в обработке данных.

ii. Получение дохода в ЕС

Получение дохода в ЕС местным учреждением в той мере, в какой такая деятельность может считаться «неразрывно связанной» с обработкой персональных данных, происходящей вне ЕС и отдельных лиц в ЕС, может свидетельствовать об обработке контроллером, учрежденным в ЕС, или оператором, осуществляемой «в контексте деятельности учреждения ЕС», и быть достаточным основанием для применения законодательства ЕС к такой

обработке.

В качестве примера приводится ситуация, когда компания в сфере электронной торговли, базирующаяся в Китае, управляющая Интернет-сайтом, через который обрабатываются персональные данные исключительно в Китае, создала европейский офис в Берлине, чтобы вести коммерческие и маркетинговые кампании на рынках ЕС.

В этом случае можно считать, что деятельность европейского офиса компании в Берлине неразрывно связана с обработкой персональных данных, осуществляемой Интернет-сайтом в Китае, поскольку коммерческая разведка и маркетинговая кампания на рынках ЕС явно служат для того, чтобы сделать услуги в сфере электронной торговли предлагаемые данным Интернет-сайтом, приносящими прибыль. Обработка персональных данных китайской компанией может рассматриваться поэтому как осуществляемая в контексте деятельности учреждения в ЕС и, следовательно, подпадает под действие положений Регламента в соответствии с его статьей 3 (1).

c) Применение GDPR к учреждению контроллера или оператора в ЕС, независимо от того, осуществляется ли обработка в ЕС

Присутствие через учреждение контроллера данных или оператора в ЕС и то обстоятельство, что обработка персональных данных происходит в контексте деятельности этого учреждения, влекут применение Регламента к соответствующим процессам обработки. Поэтому в данном случае конкретное место обработки не имеет значения для определения того, подпадает ли обработка, осуществляемая в контексте деятельности в ЕС, под действие Регламента.

Например, фармацевтическая компания со штаб-квартирой в Стокгольме перенесла всю деятельность по обработке персональных данных в отношении клинических исследований в свой филиал в Сингапуре. Согласно структуре компании, филиал не является самостоятельным юридическим лицом, а штаб-квартира в Стокгольме определяет цель и средства обработки данных, осуществляемой от ее имени филиалом в Сингапуре.

В этом случае, несмотря на то, что обработка данных происходит в Сингапуре, такая обработка выполняется в контексте деятельности фармацевтической компании в Стокгольме, то есть контроллера данных, учрежденного в ЕС. Таким образом, положения GDPR применяются к такой обработке в соответствии со статьей 3 (1).

При этом, поскольку текст статьи 3 (1) не ограничивает применение Регламента к обработке персональных данных лиц, которые находятся в ЕС, EDPB считает, что любая обработка персональных данных в контексте деятельности учреждения контроллера или оператора в ЕС, независимо от местонахождения или гражданства субъекта данных, персональные данные которого обрабатываются, подпадает под действие Регламента.

d) Применение критерия учреждения к контроллеру и оператору

По мнению EDPB, оператора в ЕС не следует рассматривать как учреждение контроллера данных по смыслу статьи 3 (1) Регламента исключительно в силу его статуса оператора. Наличие взаимоотношений в связи с обработкой персональных данных между контроллером и оператором не обязательно влечет применение Регламента в отношении их обоих, если один из этих двух субъектов не учрежден в ЕС.

i. Обработка контроллером в ЕС с использованием оператора, не подпадающего под действие GDPR

Если контроллер, подпадающий под действие GDPR, предпочитает использовать оператора, расположенного за пределами ЕС, не подпадающего под действие GDPR, контролеру необходимо обеспечить в соответствии с договором или иным юридически обязывающим документом, чтобы оператор обрабатывал персональные данные в соответствии с GDPR.

ii. Обработка в контексте деятельности учреждения оператора в ЕС

EDPB подчеркивает, что важно рассматривать вопрос деятельности учреждения контроллера и оператора по отдельности.

Первый вопрос заключается в том, имеет ли сам контроллер учреждение в ЕС и обрабатывает ли персональные данные в контексте деятельности этого учреждения. Предполагая, что контроллер не считается обрабатывающим персональные данные в контексте своего собственного учреждения в ЕС, такой контроллер не будет нести обязанности контролера в силу статьи 3 (1) Регламента (хотя он все-таки может подпадать под статью 3 (2)). При прочих равных условиях, учреждение оператора в ЕС не будет считаться учреждением в отношении контроллера.

Отдельный вопрос возникает в том случае, обрабатывает ли оператор данные в контексте своего учреждения в ЕС. Если это так, то оператор будет нести обязанности оператора согласно Регламенту. Однако это не приводит к тому, что контроллер, не учрежденный в ЕС, также будет нести обязанности контроллера согласно GDPR. То есть «не-ЕС» контроллер не будет подпадать под действие GDPR просто потому, что он решает использовать оператора в ЕС. Вместе с тем, требования GDPR, прямо применимые к операторам, в данном случае будут действовать в отношении оператора учрежденного в ЕС, обрабатывающего персональные данные.

Кроме того, поскольку такая обработка будет осуществляться в контексте деятельности учреждения оператора в ЕС, EDPB напоминает, что оператор должен обеспечить, чтобы обработка им персональных данных была законной применительно к другим обязанностям по законодательству ЕС или национальному законодательству соответствующего государства-члена.

2. Критерий направленности

EDPB обращает внимание, что контроллеры и операторы должны учитывать также другие применимые нормативные правовые акты, включая отраслевое законодательство ЕС и государств-членов и национальные законы. Несколько положений Регламента позволяют государствам-членам вводить дополнительные условия и определять конкретные рамки защиты персональных данных на национальном уровне в определенных областях или в отношении конкретных ситуаций обработки.

При оценке условий для применения критерия направленности EDPB рекомендует применять двухэтапный подход, чтобы сначала определить, связана ли обработка с персональными данными субъектов, находящихся в ЕС, и, во-вторых, относится ли такая обработка к предложению товаров или услуг или к мониторингу поведения субъектов данных в ЕС.

a) Субъекты персональных данных в ЕС

Поскольку в статье 3 (2) речь идет о «персональных данных субъектов данных, находящихся в Союзе», применение критерия направленности не ограничивается гражданством, местом жительства или другим типом юридического статуса субъекта данных, чьи персональные данные обрабатываются. П. 14 преамбулы подтверждает это толкование: «защита, предоставляемая настоящим Регламентом, должна применяться к физическим лицам, независимо от их гражданства или места жительства, в отношении обработки их персональных данных».

EDPB считает, что соответствие требованию о том, чтобы субъект данных находился в ЕС, необходимо оценить в тот момент, когда соответствующая направленная на него деятельность имеет место, то есть в момент предложения товаров или услуг или в момент, когда осуществляется мониторинг, независимо от продолжительности предлагаемого предложения или мониторинга.

Такая ситуация может иметь место, например, когда стартап, учрежденный в США, без какого-либо присутствия или создания бизнеса в ЕС, предоставляет мобильное приложение для составления карт для туристов. Приложение обрабатывает персональные данные относительно местоположения клиентов, использующих приложение (субъектов данных), после того, как они начнут использовать его в городе, который они посещают, чтобы предлагать целевую рекламу достопримечательностей, ресторанов, баров и отелей. Приложение доступно для туристов, когда они посещают Нью-Йорк, Сан-Франциско, Торонто, Лондон, Париж и Рим. Таким образом, поскольку американский стартап через приложение для составления карт города предлагает услуги отдельным лицам в ЕС, обработка персональных данных таких субъектов, расположенных в ЕС, в связи с предложением им услуги, подпадает под действие Регламента в соответствии со статьей 3 (2).

Кроме того, как отмечает EDPB, обработка персональных данных граждан или жителей ЕС, которая осуществляется в третьей стране, не влечет применения Регламента, пока такая обработка не связана с конкретным предложением, направленным на отдельных лиц в ЕС или мониторингом их поведения в ЕС.

Например, у банка в Тайване есть клиенты, которые проживают в Тайване, но имеют гражданство Германии. Банк ведет деятельность только в Тайване; его деятельность не направлена на рынок ЕС. Обработка банком персональных данных своих немецких клиентов не подпадает под действие Регламента.

b) Предложение товаров или услуг независимо от оплаты субъектами персональным данных в ЕС

В статье 3 (2) (a) Регламента указывается, что критерий направленности, касающийся предложения товаров или услуг, применяется независимо от того, требуется ли оплата субъектом персональных данных. Таким образом, будет ли деятельность контроллера или оператора, не учрежденного в ЕС считаться предложением товара или услуги, не зависит от того, произведена ли оплата в обмен на предоставленные товары или услуги.

В п.23 преамбулы Регламента указывается, что «в то время как простая доступность Интернет сайта контроллера, оператора или посредника в Союзе, адреса электронной почты или других контактных данных или использования языка, обычно используемого в третьей стране, где учрежден контроллер, недостаточны для установления такого намерения (предлагать услуги субъектам персональных данных в ЕС), такие факторы, как использование языка или валюты, обычно используемой в одном или нескольких государствах-членах ЕС, с возможностью заказывать товары и услуги на этом другом языке или упоминание клиентов или пользователей, которые находятся в ЕС, могут свидетельствовать о том, что контроллер предусматривает предложение товаров или услуг субъектам персональных данных в Союзе».

Деятельность по обработке, которая «связана» с деятельностью, влекущей применение статьи 3 (2) Регламента, также подпадает под территориальное действие Регламента. EDPB считает, что должна быть связь между обработкой и предложением товара или услуги, прямая либо косвенная.

EDPB также полагает, это судебные решения по делам Pammer v Reederei Karl Schlüter GmbH & Co и Hotel Alpenhof v Heller (дела C-585/08 и C-144/09) 23 могут оказаться полезными при рассмотрении вопроса о том, являются ли товары или услуги предлагаемыми субъекту персональных данных в ЕС.

Вместе с тем, необходимо учитывать, что, как следует из п. 23 преамбулы Регламента, что простая доступность Интернет сайта контроллера, оператора или посредника в ЕС, упоминание на Интернет сайте его электронной почты или географического адреса или его номера телефона без международного кода, сами по себе не дают достаточных доказательств для демонстрации намерения контроллера или оператора предлагать товары или услуги субъекту данных, находящемуся в ЕС.

Одним из частных случаев, когда деятельность по обработке персональных данных граждан ЕС не подпадает под

действие Регламента, является обработка в целях управления человеческими ресурсами, включая выплату заработной платы, компанией, учрежденной в третьей стране.

Например, частная компания, находящаяся в Монако, обрабатывает персональные данные своих сотрудников для целей выплаты заработной платы. Большое количество сотрудников компании - жители Франции и Италии. В этом случае, хотя обработка, осуществляемая компанией, относится к субъектам персональных данных во Франции и Италии, это не происходит в контексте предложения им товаров или услуг.

c) Мониторинг поведения субъектов персональных данных

Для применения Регламента в соответствии с его статьей 3 (2) (b), мониторинг поведения должен, прежде всего, относиться к субъекту персональных данных в ЕС, и в качестве кумулятивного критерия поведение, которое мониторится, должно иметь место на территории ЕС.

Характер деятельности по обработке, которую можно рассматривать как мониторинг поведения, уточняется в п. 24 преамбулы Регламента: «для определения того, можно ли рассматривать деятельность по обработке как мониторинг поведения субъектов персональных данных, должно быть установлено, отслеживаются ли физические лица в Интернете, включая возможное последующее использование таких способов обработки персональных данных, как профилирование физического лица, особенно для принятия решений относительно его или ее или для анализа или прогнозирования его или ее личных предпочтений, поведения и отношения».

Хотя п. 24 преамбулы относится исключительно к мониторингу поведения посредством отслеживания человека в Интернете, EDPB считает, что отслеживание через другие виды сетей связи или технологии, включающее обработку персональных данных также должны приниматься во внимание при определении того, является ли такая обработка мониторингом поведения, например, через портативные и другие смарт устройства.

В то же время, по мнению EDPB, не любой сбор или анализ онлайн персональных данных отдельных лиц в ЕС автоматически считается «мониторингом». Необходимо рассматривать цель контроллера при обработке персональных данных и, в частности, любой последующий поведенческий анализ или методы профилирования, связанные с этими данными. EDPB учитывает п. 24 преамбулы, согласно которому для определения того, является ли обработка мониторингом поведения субъекта данных, ключевое значение имеет отслеживание физических лиц в Интернете, включая потенциальное последующее использование методов профилирования.

Контроллер данных или оператор считаются осуществляющими мониторинг поведения субъектов персональных данных, находящихся в ЕС, в силу статьи 3 (2) (b) Регламента, при проведении широкого круга мероприятий, в частности:

- поведенческой рекламы;

- деятельности по географической локализации, в том числе для маркетинговых целей;

- онлайн-отслеживания с использованием файлов cookie или других методов отслеживания, таких как отпечатки пальцев;

- персонализированных услуг по анализу состояния здоровья и питания;

- видеонаблюдения;

- исследования рынка и других поведенческих исследований на основе индивидуальных профилей;

- мониторинга или регулярной отчетности о состоянии здоровья человека

В качестве примера приводится ситуация, когда маркетинговая компания, учрежденная в США, консультирует французский торговый центр, основываясь на анализе движений клиентов по всему центру, собранных посредством их отслеживания посредством Wi-Fi.

Анализ движений клиентов внутри центра путем отслеживания посредством Wi-Fi будет означать мониторинг поведения людей. В этом случае поведение субъектов данных имеет место в ЕС, так как торговый центр находится во Франции. Таким образом, маркетинговая компания, как контролер данных, обязана соблюдать требования Регламента в отношении обработки этих данных для этой цели в соответствии со статьей 3 (2) (b) и согласно статье 27 должна назначить представителя в ЕС.

---

[1] Определение «учреждения» в Регламенте, таким образом, соответствует определению, которое было дано Судом Европейского Союза («Суд ЕС») в деле Weltimmo в 2015 году V NAIH (C-230/14). Организация может быть «учреждена», когда она осуществляет «любую реальную и эффективную деятельность - даже минимальную» через «стабильные договоренности» в ЕС. Присутствия одного представителя может быть достаточно. Так, компания Weltimmo была признана имеющей «учреждение» в Венгрии в результате использования веб-сайта на венгерском языке, на котором рекламировалась недвижимость в Венгрии (это означало, что он считался «главным образом или полностью направленным на данное государство), использования местного агента (который отвечал за взыскание долгов и выступал в качестве представителя в административных и судебных разбирательствах), а также использования почтового адреса и банковского счета для деловых целей - несмотря на то, что Weltimmo была зарегистрирована в Словакии.

Скачать

Контакты для дополнительной информации:

Яна Дианова

Директор Департамента корпоративного и коммерческого права GRATA International (Москва)

T.: +7 (495) 660 11 84

E.: Ydianova@gratanet.com

Специализации

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И КОНФИДЕНЦИАЛЬНОСТЬ

Отрасли

ТЕХНОЛОГИИ, МЕДИА И ТЕЛЕКОММУНИКАЦИИ

Ключевые контакты

Яна Дианова

Советник

Москва, Россия

+7 495 660 1184

+7 906 734 6817

ydianova@gratanet.com