Требования по защите данных поставщиками Microsoft

Применимость

Требования по защите данных («**DPR**») поставщиками Microsoft применяются к каждому поставщику Microsoft, который обрабатывает персональные или конфиденциальные данные Microsoft, с учетом осуществляемой этим поставщиком деятельности (например, предоставление услуг, лицензии на программное обеспечение, облачные службы) в рамках заключенного с Microsoft контракта (например, условия заказа на покупку, основное соглашение) («**осуществление деятельности**», «**осуществлять деятельность**» или «**осуществляемая деятельность**»).

- В случае конфликта между содержащимися здесь требованиями и договорными соглашениями между поставщиком и корпорацией Microsoft настоящие требования по защите данных имеют преимущественную силу, если только соответствующий поставщик не укажет в аттестационной форме требований по защите данных то положение в контракте, которое вступает в конфликт с соответствующим разделом требований по защите данных (в этом случае приоритет имеют условия этого контракта).
- В случае конфликта между содержащимися здесь требованиями и любыми юридическими или предписанными законом требованиями такие юридические или предписанные законом требования имеют преимущественную силу.
- Если поставщик Microsoft выступает в качестве контролера, в рамках этих требований по защите данных к деятельности поставщика, связанной с обработкой, применяются только требования из разделов К «Безопасность» и А «Управление».
- Если поставщик Microsoft обрабатывает только конфиденциальные данные Microsoft, но не персональные данные Microsoft, в рамках этих требований по защите данных к обработке конфиденциальных данных Microsoft этим поставщиком применяются только требования из разделов А «Управление», Д «Хранение» и К «Безопасность».

Международная передача данных

Без ограничения других обязательств поставщик обязуется не выполнять международную передачу персональных данных Microsoft без предварительного письменного согласия Microsoft, при этом поставщик в любом случае должен соответствовать требованиям по защите данных любых стандартных условий контракта, обязательных корпоративных правил или другой схемы, утвержденной органом защиты данных, советом Европы по защите данных (European Data Protection Board) или Европейской комиссией, принятых или утвержденных Microsoft, в том числе в рамочных соглашениях EU-U.S. и Swiss-U.S. Privacy Shield, а также в общем регламенте по защите данных ЕС. Поставщик соглашается уведомлять корпорацию Microsoft о ситуациях, в которых он осознает свою неспособность дальше выполнять обязательства по обеспечению прежнего уровня защиты, соответствующего принципам Privacy Shield. Поставщик должен также убедиться, что все сторонние обработчики данных (как указано в Условии 1 (d) стандартных условий контрактов 2010, опубликованных в Приложении к решению Европейской комиссии (European Commission Decision) C(2010)593) также соответствуют требованиям.

Основные определения

Ниже указано значение некоторых терминов, используемых в этих требованиях по защите данных. Список примеров, следующий за словами «включая», «такие как», «например» и аналогичными, следует воспринимать как включаемые «без ограничений» или «помимо прочего», если только не присутствуют такие слова, как «только» или «исключительно».

«**Законодательство**» — это все применимые законы, правила, акты, указы, решения, приказы, нормативные постановления, предписания, положения, резолюции и требования любого правительственного органа (федерального, государственного, местного или международного), обладающего соответствующей юрисдикцией. «**Противозаконный**» — это любое нарушение законодательства.

«**Контролер**» — это физическое или юридическое лицо, орган власти, государственное учреждение или любая другая организация, которые самостоятельно или совместно с другими лицами определяют задачи и средства обработки персональных данных. Когда задачи и средства обработки определяются законодательством Европейского союза («**ЕС**») или стран-участников, эти законы могут указывать самого контролера (или критерии для его назначения).

«**Конфиденциальные данные Microsoft**» — это любые сведения, раскрытие которых вследствие нарушения конфиденциальности или целостности может привести к существенному ущербу для репутации или финансового положения корпорации Microsoft. Сюда входят программные и аппаратные продукты Microsoft, внутренние бизнес-приложения, лицензионные ключи продуктов и техническая документация, связанная с продуктами и услугами Microsoft.

«**Нарушение безопасности данных**» — это брешь в системе безопасности, ведущая к случайному или противозаконному удалению, утере, изменению, несанкционированному раскрытию передаваемых, хранимых и иным образом обрабатываемых персональных или конфиденциальных данных Microsoft, а также доступу к ним.

«**Обработка**» — это одна операция или несколько, выполняемые с любыми персональными или конфиденциальными данными Microsoft с применением средств автоматизации или без них, такие как сбор, запись, упорядочение, структурирование, хранение, адаптация или изменение, извлечение, консультирование, использование, раскрытие путем передачи, распространение или иное предоставление для доступа, согласование или комбинирование, ограничение, удаление или уничтожение. Термины «обрабатывать» и «обработанный» будут иметь соответствующие значения.

«**Обработчик**» — это физическое или юридическое лицо, орган власти, государственное учреждение или любая другая организация, которые обрабатывают персональные данные от имени контролера.

«**Персональные данные Microsoft**» — это любые персональные данные, обрабатываемые Microsoft или от ее имени.

«**Персональные данные**» — это любая информация, связанная с идентифицированным или идентифицируемым физическим лицом («**субъект данных**»). Идентифицируемым является физическое лицо, которое можно прямо или косвенно идентифицировать, в частности, по ссылке на некоторый идентификатор, такой как имя, идентификационный номер, данные о расположении, индикатор в сети либо один связанный с этим физическим лицом фактор физического, психологического, генетического, интеллектуального, экономического, культурного или социального характера или несколько других.

«**Право субъекта данных**» — это право субъекта данных на удаление, редактирование, экспорт, ограничение персональных данных Microsoft этого субъекта данных, доступ к ним, а также возражение против их обработки, если это требуется законодательством.

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел А. Управление		
1	Каждое применимое соглашение между корпорацией Microsoft и поставщиком (например, основное соглашение, техническое задание, заказы на покупку и иные заказы) содержит соответствующие положения о защите конфиденциальных и персональных данных в отношении конфиденциальных и персональных данных Microsoft. Для компаний, выступающих в роли обработчиков, такое соглашение должно включать в себя объект и длительность обработки, характер обработки и ее назначение, тип персональных данных Microsoft и категории субъектов данных, а также обязательства и права корпорации Microsoft.	Поставщик должен заключить соответствующий контракт с Microsoft. Для обработчиков описания обработки должны быть указаны в применимом соглашении (*например*, техническом задании, заказах на покупку). Примечание. Компании, использующие оперативные заказы на закупку, могут добавить необходимое описание процедур обработки на более позднем этапе процесса закупок.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
2	Назначить ответственным и подотчетным в отношении соблюдения требований по защите данных определенного сотрудника или группу внутри организации.	Назначение ответственного лица или группы для обеспечения соответствия требованиям по защите данных поставщиком Microsoft. Документ, описывающий полномочия и подотчетность этого лица или этой группы, в котором отражены их функции по обеспечению безопасности и (или) конфиденциальности.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
3	Разработать, согласовать и проводить ежегодное обучение по вопросам конфиденциальности и безопасности для сотрудников, которые получат доступ к персональным или конфиденциальным данным Microsoft. Если у вашей организации нет готовых материалов, можно использовать эту раскадровку и адаптировать ее под особенности своей организации.	Имеются годовые записи о посещении. Учебные материалы содержат описание принципов обеспечения конфиденциальности и безопасности.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел A. Управление (продолжение)		
4	Обрабатывать персональные данные Microsoft исключительно в соответствии с задокументированными инструкциями Microsoft, включая те из них, которые касаются передачи персональных данных в третью страну или международную организацию, если только того не требует законодательство. В этом случае обработчик (поставщик) должен уведомить контролера (Microsoft) о таком юридическом требовании до обработки, если только законодательство в интересах государства не запрещает передачу такой информации.	Документальные доказательства инструкций, обозначенных в контракте (например, техническом задании или заказе на покупку) либо зафиксированных в электронной системе, используемой для осуществления деятельности.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел Б. Примечание		
5	Поставщик должен использовать заявление о конфиденциальности корпорации Microsoft при сборе персональных данных от ее имени. Уведомление о конфиденциальности должно быть понятно и доступно субъектам данных, чтобы помочь им принять решение о передаче персональных данных поставщику. Примечание. Если ваша организация является контролером деятельности по обработке, вам нужно опубликовать собственное уведомление о конфиденциальности. *Чтобы получить доступ к соответствующим уведомлениям Microsoft, обратитесь по адресу SSPAHelp@microsoft.com.*	Поставщик использует fwdlink на актуальное опубликованное заявление о конфиденциальности корпорации Microsoft. Заявление о конфиденциальности публикуется в любом контексте, где будет осуществляться сбор персональных данных пользователя. При необходимости доступна автономная версия, предоставляемая перед сбором данных. Все автономные заявления о конфиденциальности соответствуют актуальной опубликованной версии и датированы соответствующим образом. К службам для сотрудников Microsoft применяется уведомление о защите данных Microsoft.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
6	При сборе персональных данных Microsoft с помощью обычного или записанного голосового звонка поставщики должны быть готовы обсудить методы сбора, обработки, использования и хранения применимых данных с субъектами данных.	Сценарий для голосовых записей содержит описание того, как осуществляется обработка персональных данных Microsoft, включая: ▪ сбор; ▪ использование; ▪ хранение.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел B. Выбор и согласие		
7	В случаях когда поставщик прибегает к согласию на обработку и связанным с ним юридическим основаниям, он должен получить и документально оформить согласие субъекта данных на все процедуры обработки (включая новые и обновленные) перед сбором его персональных данных.	Поставщик может продемонстрировать, как субъект данных предоставляет согласие на процедуру обработки и что такое согласие охватывает все процедуры обработки поставщика в отношении персональных данных субъекта данных. Поставщик может продемонстрировать, как субъект данных отзывает согласие на процедуру обработки. Поставщик может продемонстрировать, как учитываются предпочтения перед запуском новой процедуры обработки. Поставщик отслеживает эффективность учета предпочтений, чтобы обеспечить сроки реагирования на смену предпочтений, удовлетворяющие наиболее жестким требованиям применимого местного законодательства. Примечание. Доказательством могут служить снимки экрана, описывающие взаимодействие с пользователем, экспериментирование со службой или возможность просмотра технической документации.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел B. Выбор и согласие (продолжение)		
8	Файлы cookie — это небольшие текстовые файлы, которые сохраняются на устройствах веб-сайтами и (или) приложениями и содержат сведения, используемые для распознавания субъекта данных или устройства. Поставщики, создающие и контролирующие веб-сайты и (или) приложения Microsoft, должны выводить субъектам данных понятное уведомление об использовании файлов cookie с возможностью включения или отключения этой функции. Поставщики, создающие и контролирующие веб-сайты и (или) приложения Microsoft, должны следить за тем, чтобы использование файлов cookie соответствовало задачам, изложенным в заявлении о конфиденциальности корпорации Microsoft, и требованиям местного законодательства, например правилам, установленным ЕС.	Следует задокументировать назначение каждого из файлов cookie, указав в нем тип применяемого файла. ▪ Сохраняемые файлы cookie не должны использоваться, если достаточно файлов cookie сеанса. ▪ При использовании сохраняемых файлов cookie их срок действия не должен превышать 2 лет с момента обращения пользователя к сайту. Для пользователей из ЕС срок действия сохраняемого файла cookie не должен превышать 13 месяцев. Нужно подтвердить соответствие применимому законодательству ЕС, включая: ▪ использование соглашения о метках из раздела «Конфиденциальность и файлы cookie» заявления о конфиденциальности; ▪ получение подтверждения согласия пользователя перед использованием файлов cookie для «неосновных» целей, таких как реклама.	*<Соответствует>* *<Не соответствует>* *<Неприменимо>* *<Юридическая коллизия>* *<Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел Г. Сбор		
9	Поставщик должен отслеживать сбор персональных и (или) конфиденциальных данных Microsoft, чтобы гарантировать, что собираемая информация необходима для осуществления деятельности.	Поставщик может предоставить документацию, показывающую, что собираемые персональные и (или) конфиденциальные данные Microsoft необходимы для осуществления деятельности.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
10	Если поставщик собирает персональные данные третьих лиц от имени Microsoft, он должен подтвердить, что политика и практика защиты данных третьих лиц соответствуют контракту с Microsoft и требованиям по защите данных.	Поставщик может документально подтвердить проведение надлежащей проверки принятой третьими лицами практики и политики в области защиты данных.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
11	Перед сбором персональных данных Microsoft с помощью установки или использования исполняемого программного обеспечения на устройстве субъекта данных нужно документально оформить необходимость сбора таких данных в действующем контракте поставщика с Microsoft.	Соглашение с Microsoft, касающееся использования исполняемого программного обеспечения на устройстве субъекта данных, указано в действующем контракте.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
12	Перед сбором конфиденциальных персональных данных Microsoft (данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, принадлежность к профсоюзу, генетические данные, биометрические данные, данные о состоянии здоровья, сексуальной жизни или сексуальной ориентации) нужно документально оформить необходимость сбора таких персональных данных в действующем контракте поставщика с Microsoft.	Необходимость сбора конфиденциальных персональных данных Microsoft указана в действующем контракте с Microsoft.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел Д. Хранение		
13	Убедиться, что персональные и конфиденциальные данные Microsoft хранятся не дольше, чем это необходимо для осуществления деятельности, за исключением случаев, когда хранение персональных и (или) конфиденциальных данных Microsoft требуется законодательством.	Поставщик соблюдает документально оформленную политику хранения данных или требования к хранению данных, указанные Microsoft в контракте (например, техническом задании или заказе на покупку).	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
14	По единоличному усмотрению Microsoft персональные и конфиденциальные данные Microsoft, которыми владеет поставщик или которые находятся под его контролем, должны возвращаться в Microsoft или уничтожаться по завершении осуществляемой деятельности либо по запросу Microsoft. В приложениях должны быть предусмотрены процедуры, обеспечивающие надежное уничтожение данных, удаляемых как самими пользователями, так и по триггерам, таким как возраст данных. При возникновении необходимости в уничтожении персональных или конфиденциальных данных Microsoft поставщик должен сжечь, растереть в порошок или измельчить физические активы с персональными и (или) конфиденциальными данными Microsoft таким образом, чтобы эти данные невозможно было прочесть или восстановить.	Учет дальнейшего распоряжения персональными и конфиденциальными данными Microsoft (например, возврат данных в Microsoft для их уничтожения). Если уничтожение запрошено или затребовано корпорацией Microsoft, нужно предоставить акт об уничтожении, подписанный сотрудником поставщика.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел E. Субъекты данных		
	Субъекты данных имеют право на использование, удаление, правку, экспорт, ограничение своих персональных данных, а также могут запретить их обработку («**права субъекта данных**»). Если субъект данных желает реализовать свои права согласно действующему законодательству в отношении своих персональных данных Microsoft, он должен сделать следующее:		
15	Настолько, насколько это возможно, оказать корпорации Microsoft содействие в виде подходящих технических и организационных мероприятий, чтобы выполнить свои обязательства по реагированию на запросы субъектов данных, стремящихся реализовать свои права субъекта данных.	Предусмотрены процессы и процедуры, способствующие реализации прав субъектов данных.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
16	Реагировать на все запросы, связанные с правами субъектов данных, без необоснованной задержки.	Поставщик периодически проверяет свою способность по оказанию поддержки в отношении прав субъектов данных.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
17	При отсутствии иных указаний со стороны корпорации Microsoft поставщик направит всех обращающихся к нему субъектов данных непосредственно в Microsoft для осуществления их прав. Поставщик сообщит субъектам данных о тех шагах, которые им потребуется выполнить для получения доступа или иного осуществления прав в отношении их персональных данных Microsoft. *Для получения содействия по данному требованию обратитесь по адресу SSPAHelp@microsoft.com.*	Поставщик сообщает о действиях, необходимых для получения доступа к персональным данным, а также о доступных методах их обновления.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
18	Подтвердить личность субъекта данных при прямом взаимодействии с ним.	Поставщик задокументировал методику, используемую для идентификации субъектов данных Microsoft.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел E. Субъекты данных (продолжение)		
	После проверки подлинности субъекта данных поставщик должен осуществить следующее.		
19	Определить, владеет или управляет ли он персональными данными Microsoft о таком субъекте данных.	Поставщик имеет необходимые процедуры для установки текущего местонахождения персональных данных.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
20	Приложить все обоснованные усилия, чтобы определить расположение персональных данных Microsoft, и сохранить необходимые записи, чтобы доказательно подтвердить проведение обоснованного поиска.	Поставщик ведет записи, демонстрирующие предпринятые меры для выполнения запросов, связанных с правами субъектов данных. Эта документация включает в себя: ▪ дату и время запроса; ▪ меры, предпринятые для реагирования на запрос; ▪ запись о том, когда была уведомлена корпорация Microsoft.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
21	Фиксировать дату и время запросов, связанных с правами субъектов данных, и действий, предпринятых поставщиком в ответ на такие запросы. Предоставлять записи запросов субъектов данных в корпорацию Microsoft по требованию.	Поставщик ведет учет запросов доступа к персональным данным и документирует все внесенные в персональные данные изменения.	
	После проверки подлинности субъекта данных и проверки наличия у поставщика запрошенных персональных данных Microsoft поставщик должен:		
22	Для запросов на получение копии персональных данных предоставить персональные данные Microsoft субъекту данных в подходящей печатной, электронной или устной форме.	Поставщик предоставляет персональные данные субъекту данных в формате, понятном и удобном для самого субъекта данных и для поставщика.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел E. Субъекты данных (продолжение)		
23	Если запрос отклонен, по указанию Microsoft предоставить субъекту данных письменное объяснение в соответствии с любыми актуальными инструкциями, ранее предоставленными корпорацией Microsoft. *Для получения содействия по данному требованию обратитесь по адресу SSPAHelp@microsoft.com.*	Документируйте экземпляры с отклоненными запросами и храните доказательства рассмотрения и утверждения корпорацией Microsoft.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
24	Поставщик должен предпринять обоснованные предосторожности, чтобы гарантировать, что персональные данные Microsoft, выданные субъекту данных, не могут быть использованы для идентификации другого лица.	Поставщик должен документально подтвердить, что приняты необходимые меры, предотвращающие идентификацию одного лица на основании информации, выданной другому лицу (например, не допускается фотокопирование всей страницы документа, где персональные данные запрашивающего субъекта данных занимают только одну строчку).	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
25	Если субъект данных и поставщик не согласны относительно полноты и точности персональных данных Microsoft, поставщик должен передать вопрос в Microsoft и при необходимости сотрудничать с Microsoft для устранения разногласий. *Для получения содействия по данному требованию обратитесь по адресу SSPAHelp@microsoft.com.*	Поставщик документально оформляет случаи разногласия и передает вопрос на рассмотрение Microsoft.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел Ж. Раскрытие информации третьим лицам		
	Если поставщик намеревается привлечь субподрядчика для обработки персональных или конфиденциальных данных Microsoft, он обязан сделать следующее.		
26	Получить предварительное письменное согласие Microsoft перед оформлением субподряда либо добавлением или заменой субподрядчиков. *Для получения содействия по данному требованию обратитесь по адресу SSPAHelp@microsoft.com.*	Подтверждение того, что персональные данные Microsoft обрабатываются только организациями, известными корпорации Microsoft, к чему обязывает соответствующий контракт (например, техническое задание, дополнение, заказ на покупку), или внесенными в базу данных SSPA.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
27	Документировать характер и объем персональных и конфиденциальных данных, обработанных субподрядчиками, и следить за тем, чтобы собранная информация требовалась для осуществления деятельности.	Поставщик ведет необходимую документацию относительно раскрытия или передачи субподрядчикам персональных и конфиденциальных данных Microsoft.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
28	Убедиться, что субподрядчик использует персональные данные Microsoft в соответствии с указанными контактными предпочтениями субъекта данных.	Демонстрация того, как предпочтение субъекта данных учитывается субподрядчиками. Предоставление вспомогательной документации, включающей в себя сроки учета смены предпочтений субподрядчиком.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
29	Ограничить обработку персональных данных Microsoft субподрядчиком, за исключением случаев, когда это необходимо для выполнения контракта поставщика с Microsoft.	Поставщик может предоставить документацию, показывающую, что предоставляемые субподрядчику персональные данные Microsoft необходимы для осуществления деятельности.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел Ж. Раскрытие информации третьим лицам (продолжение)		
30	Просматривать сообщения, указывающие на несанкционированную или незаконную обработку персональных данных Microsoft.	Поставщик может продемонстрировать системы и процедуры для рассмотрения жалоб о несанкционированном использовании или раскрытии персональных данных Microsoft субподрядчиком.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
31	Незамедлительно уведомить Microsoft при получении сведений о том, что субподрядчик обработал персональные или конфиденциальные данные в любых целях, не связанных с осуществлением деятельности.	Поставщик предоставил инструкции и средства, позволяющие субподрядчику сообщить о неправильном использовании данных Microsoft.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
32	Незамедлительно предпринимать действия по устранению фактического или возможного ущерба, вызванного несанкционированной или незаконной обработкой персональных и конфиденциальных данных Microsoft субподрядчиком.	Поставщик может продемонстрировать наличие плана и процессов на случай неправильного использования персональных и конфиденциальных данных Microsoft субподрядчиком.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
	Раздел З. Качество		
33	Поставщик должен обеспечить целостность всех персональных данных Microsoft, чтобы гарантировать их точность, полноту и актуальность при обработке в указанных целях.	Поставщик может продемонстрировать наличие процедур для проверки персональных данных Microsoft при их сборе, создании и изменении. Поставщик может продемонстрировать наличие процедур мониторинга и выборки для непрерывной проверки точности и внесения корректив по мере необходимости.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел И. Мониторинг и принудительное применение		
34	Поставщик располагает планом реагирования на инциденты, предписывающим поставщику без необоснованных задержек уведомлять Microsoft о получении сведений о нарушении безопасности данных или уязвимости, связанных с обработкой персональных или конфиденциальных данных поставщиком. *Чтобы сообщить об инциденте, обратитесь по адресу SSPAHelp@microsoft.com.*	Поставщик располагает планом реагирования на инциденты, предусматривающим уведомление клиентов (Microsoft) способом, описанным в этом разделе.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
35	Не делать заявлений для прессы или любых других публичных заявлений, связанных с нарушением безопасности данных, затрагивающим персональные или конфиденциальные данные Microsoft, не получив согласия Microsoft, за исключением случаев, когда это требуется законодательством.	Поставщик соглашается следовать этому требованию при возникновении описанной ситуации.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
36	Реализовать план по исправлению и отслеживать устранение нарушений безопасности данных и уязвимостей, связанных с персональными или конфиденциальными данными Microsoft, чтобы обеспечить выполнение соответствующих корректирующих действий в надлежащее время.	Поставщик располагает задокументированными процедурами по реагированию на нарушение безопасности данных.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
37	Организовать формальную процедуру связи для ответов на все сообщения о защите данных, включающие персональные данные Microsoft.	Поставщик располагает средствами для приема жалоб, связанных с персональными данными Microsoft, и задокументированной процедурой рассмотрения жалоб.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность		
	Поставщик должен разработать, согласовать и реализовать программу информационной безопасности, включающую в себя политики и процедуры для защиты и обеспечения безопасности персональных и конфиденциальных данных Microsoft в соответствии с надлежащей отраслевой практикой и требованиями действующего законодательства. Программа обеспечения безопасности поставщика должна соответствовать стандартам, указанным в требованиях 38–56 ниже.	Программа может включать большее число мер предосторожностей, чем перечислено в соответствующих пунктах, когда это требуется в соответствии с регулятивными программами (например, акт о передаче и защите данных учреждений здравоохранения HIPAA, закон Грэмма-Лича-Блайли (GLBA)) или предусмотрено контрактными требованиями. Допустимый отчет SOC 2 или сертификация ISO 27001 по безопасности являются приемлемыми заменителями раздела К. Чтобы воспользоваться такой заменой, обратитесь по адресу SSPAHelp@microsoft.com. Примечание. Вам потребуется предоставить документацию, описывающую область действия этих сертификаций/отчетов.	
38	Ежегодно проводить оценку безопасности сети, которая включает в себя следующее: ▪ обзор основных изменений в среде, таких как новый системный компонент, топология сети, правила брандмауэра и т. п.; ▪ поиск уязвимостей; ▪ ведение журналов изменений.	Поставщик располагает документацией по оценкам сети, журналам изменений и результатам проверок. Требуемые журналы изменений должны отслеживать изменения, предоставлять информацию о причине изменения, а также включать имя и должность назначенного утверждающего.	*<Соответствует>* *<Не соответствует>* *<Неприменимо>* *<Юридическая коллизия>* *<Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
39	Поставщик должен определить, согласовать и реализовать политику мобильных устройств, которая обеспечивает защиту и ограничение использования персональных или конфиденциальных данных Microsoft, к которым обращается или с которыми работает пользователь мобильного устройства.	Поставщик демонстрирует использование совместимой политики мобильных устройств в тех случаях, где для обработки персональных или конфиденциальных данных Microsoft требуется мобильное устройство.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
40	Нужно учесть все активы, используемые для осуществления деятельности, и все они должны иметь идентифицированного владельца. Поставщик несет ответственность за инвентаризацию таких информационных активов, обеспечение их приемлемого и санкционированного использования, а также за обеспечение достаточного уровня их защиты на протяжении всего жизненного цикла.	Инвентаризация активов устройств, используемых для осуществления деятельности. Инвентаризация этих активов должна включать в себя следующее: ▪ расположение устройства; ▪ классификацию данных по активам; ▪ запись о возврате активов при увольнении сотрудника или разрыве делового соглашения; ▪ запись об утилизации более не нужных носителей данных.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
41	Разработать и реализовать процедуры управления доступом для предотвращения несанкционированного доступа к любым персональным или конфиденциальным данным Microsoft, находящимся в распоряжении поставщика.	Поставщик демонстрирует внедрение плана по управлению правами доступа, который включает в себя следующее: ▪ процедуры управления доступом; ▪ процедуры идентификации; ▪ процедуры блокировки после неудачных попыток; ▪ сброс пароля с подходящим интервалом, но не больше 90 дней; ▪ надежные параметры для выбора учетных данных проверки подлинности; ▪ отключение учетных записей пользователей при увольнении в течение 48 часов. Поставщик демонстрирует, что он организовал процедуру для контроля доступа пользователей к персональным или конфиденциальным данным Microsoft с соблюдением принципа предоставления минимальных прав. Эта процедура включает в себя следующее: ▪ четко определенные роли пользователей; ▪ процедуры для контроля и утверждения прав доступа к ролям; ▪ проверка того, что у пользователей с ролями, которым предоставляется доступ к данным Microsoft, имеется задокументированное обоснование для использования соответствующей роли или группы.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
42	Разработать и реализовать процедуры управления исправлениями, в которых приоритет отдается обновлениям безопасности для систем, используемых для обработки персональных и конфиденциальных данных Microsoft. Эти процедуры включают в себя следующее: ▪ определенный подход на основе рисков для назначения приоритета обновлениям безопасности; ▪ возможность использования и применения экстренных обновлений; ▪ возможность применения для операционной системы и серверного программного обеспечения, например сервера приложений или программного обеспечения базы данных; ▪ документирование уменьшения риска, обеспечиваемого обновлением, и отслеживание возможных исключений; ▪ требования по прекращению использования программного обеспечения, которое больше не поддерживается организацией-разработчиком.	Поставщик может продемонстрировать внедренную процедуру управления обновлениями, которая соответствует этому требованию и охватывает по крайней мере следующее. ▪ Назначение уровней серьезности для информированной расстановки приоритетов. (Определения серьезности документируются.) ▪ Задокументированная процедура для применения экстренных обновлений. ▪ Контроль за прекращением использования операционных систем, которые больше не поддерживаются организацией-разработчиком. ▪ Записи управления обновлениями, отслеживающие утверждения и исключения.	*<Соответствует>* *<Не соответствует>* *<Неприменимо>* *<Юридическая коллизия>* *<Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
43	Устанавливать антивирусное и антивредоносное программное обеспечение для оборудования, подключенного к сети, которое используется для обработки персональных и конфиденциальных данных Microsoft, включая серверы, рабочие и тестовые настольные компьютеры, для защиты от приложений с потенциально опасными вирусами и вредоносным программным обеспечением. Обновлять определения антивредоносной программы на ежедневной основе или согласно рекомендациям поставщика решений по защите от вирусов и вредоносных программ. Примечание. Это касается всех операционных систем, включая Linux.	Имеются записи, показывающие использование программного обеспечения для защиты от вирусов и вредоносных программ. Примечание. Это требование касается всех операционных систем.	*<Соответствует>* *<Не соответствует>* *<Неприменимо>* *<Юридическая коллизия>* *<Контрактный конфликт>*
44	Поставщики, разрабатывающие программное обеспечение для Microsoft, в процессе создания должны реализовывать принципы встроенной безопасности.	Документы поставщика с техническими спецификациями должны включать пункты по проверке безопасности в рамках циклов разработки.	*<Соответствует>* *<Не соответствует>* *<Неприменимо>* *<Юридическая коллизия>* *<Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
45	Применять программу защиты от потери данных («**DLP**»). Данные должны быть должным образом классифицированы, маркированы и защищены, а поставщик должен отслеживать используемые информационные системы, где обрабатываются персональные или конфиденциальные данные Microsoft, на предмет атак, потерь и другой несанкционированной активности. Программа DLP, как минимум: ▪ требует использовать соответствующие отраслевым стандартам системы обнаружения атак («**IDS**») для узлов, сетей и облаков, если вы храните персональные или конфиденциальные данные Microsoft; ▪ требует внедрять усовершенствованные системы обнаружения атак («**IPS**»), настроенные для отслеживания и активного предотвращения потери данных; ▪ требует проанализировать систему в случае образования бреши, чтобы устранить все остаточные уязвимости; ▪ требует документировать необходимые процедуры по контролю средств, отслеживающих нарушения в системе; ▪ формирует процесс реагирования на инциденты и управления ими, который применяется при обнаружении нарушения безопасности данных.	Задокументированные системы IDS/IPS, развернутые вместе с процедурами прямого реагирования при обнаружении уязвимости или нарушения безопасности данных.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
46	Незамедлительно сообщать старшему руководству и корпорации Microsoft о результатах расследования в рамках реагирования на инциденты. *Чтобы проинформировать Microsoft, обратитесь по адресу SSPAHelp@microsoft.com.*	Поставщик должен располагать необходимыми системами и процедурами для передачи корпорации Microsoft результатов расследований в рамках реагирования на инциденты.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
47	Системные администраторы, рабочий персонал, руководство и третьи лица должны ежегодно проходить обучение по безопасности.	Организуйте учебную программу по вопросам безопасности, включающую в себя следующее: ▪ ежегодное обучение по вопросам реагирования на инциденты; ▪ смоделированные мероприятия и автоматические механизмы, улучшающие реагирование на инциденты в кризисных ситуациях. Распространение информации о предотвращении инцидентов, например о рисках, связанных со скачиванием вредоносного программного обеспечения.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
48	Поставщик должен убедиться, что процессы планирования резервного копирования защищают персональные и конфиденциальные данные Microsoft от несанкционированного использования, доступа, раскрытия, изменения и уничтожения.	Поставщик может продемонстрировать задокументированные процедуры реагирования и восстановления, подробно описав, как именно организация будет реагировать на происшествие и обеспечивать необходимый уровень информационной безопасности, описанный в указаниях руководства по непрерывной защите информации. Поставщик может продемонстрировать, что он разработал и внедрил процедуры периодического резервного копирования, безопасного хранения и эффективного восстановления критически важных данных.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
49	Разработать и протестировать планы непрерывности бизнес-процессов и аварийного восстановления.	План аварийного восстановления должен включать в себя все следующие элементы. ▪ Обозначенные критерии для определения того, является ли система критически важной для функционирования бизнеса поставщика. ▪ Основанный на определенных критериях список критически важных систем, для которых потребуется восстановление в случае аварии. ▪ Заданная процедура аварийного восстановления для каждой критически важной системы, позволяющая не знакомому с системой инженеру восстановить приложение в течение 72 часов. ▪ Проверка и повторное рассмотрение планов аварийного восстановления на предмет выполнимости целей восстановления не реже одного раз в год.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
50	Выполнить проверку подлинности лица перед тем, как предоставлять ему доступ к персональным или конфиденциальным данным Microsoft.	Убедитесь, что все идентификаторы пользователей уникальны и каждый из них имеет метод проверки подлинности, соответствующий отраслевому стандарту, например Azure Active Directory. При доступе с повышенными правами (административного или другого типа) должна запрашиваться двухфакторная проверка подлинности, например с использованием смарт-карты или телефона.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
51	Поставщик должен защитить персональные и конфиденциальные данные Microsoft во время их передачи через сеть с помощью шифрования на базе **TLS** или **IPsec**. Эти методы описаны в стандартах NIST 800-52 и NIST 800-57. Кроме того, можно использовать эквивалентный отраслевой стандарт. Поставщик должен отказаться от передачи любых персональных или конфиденциальных данных Microsoft по нешифрованным каналам.	Требуется разработать и реализовать процедуру по передаче, развертыванию и замене TLS или других сертификатов.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
52	Все устройства поставщика (ноутбуки, рабочие станции и т. д.), которые будут осуществлять доступ к персональным или конфиденциальным данным Microsoft или обрабатывать их, должны использовать дисковое шифрование.	Все устройства, используемые для обработки персональных или конфиденциальных данных Microsoft, должны быть зашифрованы с помощью Bitlocker или другого аналогичного отраслевого решения для шифрования дисков.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
53	Должны быть предусмотрены системы и процедуры (использующие актуальные отраслевые стандарты, например, описанные в стандарте NIST 800-111) для шифрования любых неактивных (хранимых) персональных и (или) конфиденциальных данных Microsoft, включая все следующие данные: ▪ учетные данные (например, имена пользователей и пароли); ▪ данные о платежных средствах (например, кредитных картах и номерах банковских счетов); ▪ персональные данные, связанные с иммиграцией; ▪ медицинские данные (например, номера медицинских записей или биометрические маркеры или идентификаторы, такие как ДНК, отпечатки пальцев, сетчатка и радужная оболочка глаза, тембр голоса, особенности лица и замеры рук, используемые для проверки подлинности); ▪ идентификационные данные, выданные государственными органами (например, номер социального страхования или водительских прав); ▪ данные, принадлежащие клиентам Microsoft (например, Sharepoint, документы Office 365, клиенты OneDrive); ▪ материалы, касающиеся необъявленных продуктов Microsoft; ▪ дата рождения; ▪ сведения о профиле ребенка; ▪ географические данные в реальном времени; ▪ физический домашний (не рабочий) адрес; ▪ домашние (не рабочие) номера телефона; ▪ вероисповедание; ▪ политические убеждения; ▪ сексуальные предпочтения и ориентация; ▪ ответы на контрольные вопросы (например, двухфакторная проверка подлинности, сброс пароля); ○ девичья фамилия матери.	Обеспечьте шифрование персональных и конфиденциальных данных Microsoft, указанных в этом пункте, на этапе хранения.	*<Соответствует>* *<Не соответствует>* *<Неприменимо>* *<Юридическая коллизия>* *<Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
54	При обработке кредитных карт от имени Microsoft придерживаться действующих стандартов по обработке подобных данных, установленных эмитентом карт.	Подтвердите соответствие, ежегодно проходя сертификацию по стандарту безопасности данных в сфере платежных карт («**PCI-DSS**»). *Отправляйте сертификации PCI DSS в SSPA. По любым вопросом обращайтесь по адресу SSPAHelp@microsoft.com*.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*
55	Поставщик должен хранить физические активы Microsoft в среде с управлением доступом.	Поставщик должен располагать необходимыми системами и процедурами, призванными регулировать физический доступ к данным Microsoft, хранящимися в электронном виде в архивных и резервных копиях или в виде твердых копий. При перемещении и уничтожении физических носителей с данными Microsoft нужно следовать по цепи обеспечения сохранности.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*

№	Требования по защите данных поставщиками Microsoft	Доказательство соответствия	Ответ
	Раздел К. Безопасность (продолжение)		
56	Анонимизировать все персональные данные Microsoft, использующиеся в среде разработки или тестирования.	Персональные данные Microsoft не должны использоваться в ходе разработок или испытаний. Но если их использование необходимо, персональные данные должны быть анонимными для предотвращения идентификации субъектов данных или злоупотребления персональными данными. Примечание. Анонимизированные данные отличаются от псевдоанонимных. Анонимизированные данные не связаны ни с каким идентифицированным или идентифицируемым физическим лицом, когда субъект персональных данных более не может быть идентифицирован.	*<Соответствует> <Не соответствует> <Неприменимо> <Юридическая коллизия> <Контрактный конфликт>*