Требования по защите данных поставщиками Майкрософт

Применение

Требования по защите данных («**Требования**») поставщиками Майкрософт применяются к каждому поставщику Майкрософт, который обрабатывает Персональные или Конфиденциальные данные Майкрософт в процессе осуществления деятельности этим поставщиком (например, предоставление услуг, лицензии на программное обеспечение, облачные службы) в соответствии с условиями договора заключенного с Майкрософт (например поставка товаров, рамочный договор на предоставление услуг) («**Осуществление деятельности**», «**Осуществлять деятельность**» или «**Осуществляемая деятельность**»).

- При наличии противоречий между содержащимися здесь требованиями и договорными соглашениями между поставщиком и корпорацией Майкрософт настоящие Требования по защите данных имеют преимущественную силу, если только поставщик не укажет иное положение в контракте, которое заменяет применимое требование о защите данных (в таком случае, условия контракта имеют преимущество).
- В случае противоречия между содержащимися здесь требованиями и любыми юридическими или законодательными требованиями, такие юридические или законодательные требования имеют преимущественную силу.
- Если поставщик Майкрософт выступает в качестве Управляющего данными, к поставщику может быть применим сокращенный список требования с учетом этих Требований.
- Если поставщик Майкрософт обрабатывает только конфиденциальные данные Майкрософт, но не персональные данные Майкрософт, в рамках этих Требований к поставщику могут быть применимы сокращенные требования.

Международная передача данных

Не ограничивая другие свои обязательства поставщик обязуется не осуществлять какую-либо международную передачу Персональных данных Майкрософт без предварительного письменного согласия со стороны корпорации Майкрософт. Также в любых ситуациях обязан соблюдать Требования, включая Стандартные Договорные Положения, или, на усмотрение Майкрософт, другие соответствующие механизмы трансграничной передачи, утвержденные соответствующим органом по защите данных или Европейской комиссией, в зависимости от ситуации, принятые или согласованные Майкрософт. Преемственные стандартные договорные положения, принятые (i) Европейской комиссией или принятые Европейским органом по защите данных и одобренные Европейской комиссией, (ii) Соединенным Королевством в соответствии с Общим федеральным законом Великобритании о защите данных, (iii) Швейцарией в соответствии с Федеральным законом Швейцарии о защите данных или (iv) положения, регулирующие международную передачу персональных данных, официально принятые правительством в юрисдикции, отличной от Швейцарии, Соединенного Королевства и юрисдикций, входящих в Европейский Союз / Европейскую экономическую зону, должны быть включены и обязательны для Поставщика со дня их принятия. Поставщик также должен обеспечить, чтобы все участники процесса (как определено в стандартных договорных положениях) также соблюдали эти Требования.

Основные определения

Ниже приведено значение терминов, используемых в этих Требованиях. Когда в Требованиях идет перечисление примеров после слов «включая», «такие как», «например» и аналогичных слов, их следует трактовать со значением «без ограничений» или «помимо прочего», если отсутствуют уточняющие слова, такие как: «только» или «исключительно».

«Управляющий данными» (“Контроллер”) — означает организацию, которая определяет цели и средства обработки Персональных Данных. Понятие включает в себя предприятие, контроллера (как этот термин определен в этих Требованиях) и эквивалентные термины в законодательных актах о защите данных, в зависимости от контекста.

«Файлы cookie» — небольшие текстовые файлы, которые сохраняются на устройствах веб-сайтами и/или приложениями, и содержат информацию, используемую для распознавания Субъекта данных или устройства.

Нарушение безопасности данных означает (1) нарушение безопасности, повлекшее случайное или незаконное уничтожение, потерю, изменение, несанкционированное раскрытие или получение персональных или конфиденциальных данных Майкрософт, передаваемых, хранимых или иным способом обрабатываемых Поставщиком или его Субподрядчиками, либо (2) уязвимость системы безопасности, связанная с обработкой поставщиком Персональных или Конфиденциальных данных Майкрософт.

Субъект данных — это физическое лицо, которое возможно прямо или косвенно идентифицировать, в частности с помощью какого-либо идентификатора, такого как имя, идентификационный номер, данные о местоположении или онлайн идентификатор, либо с помощью одного или нескольких связанных с этим физическим лицом факторов физического, физиологического, генетического, интеллектуального, экономического, культурного или социального характера.

Право Субъекта Данных — это право субъекта данных на получение, удаление, редактирование и экспорт своих Персональных данных Майкрософт, ограничение к ним доступа и на возражение против их обработки, согласно требованиям законодательства.

Законодательство — это все применимые законы, правила, статуты, указы, решения, приказы, нормативные постановления, кодексы, предписания, резолюции и требования любого государственного органа (федерального, регионального, местного или международного), с соответствующей юрисдикцией.
Противозаконным называется любое нарушение законодательства.

Конфиденциальные данные Майкрософт — это любые сведения, раскрытие которых в следствии нарушения конфиденциальности или целостности может привести к существенному репутационному или финансовому ущербу для корпорации Майкрософт. К ним относятся программные и аппаратные продукты Майкрософт, внутренние бизнес-приложения, неопубликованные маркетинговые материалы, лицензионные ключи продуктов и техническая документация, связанная с продуктами и услугами Майкрософт.

Персональные данные Майкрософт — это любые персональные данные, обрабатываемые корпорацией Майкрософт или от ее имени.

Персональные данные — это любая информация, связанная с субъектом данных, и любая другая информация, которая подразумевается под понятиями «персональные данные» или «личные данные» согласно законодательства.

Обработка — это любая операция или набор операций, которые выполняются по отношению к любым Персональными или Конфиденциальными данными Майкрософт с возможным применением средств автоматизации, в том числе сбор, запись, упорядочение, структурирование, хранение, адаптация или изменение, получение, анализ, использование, раскрытие путем передачи, распространение или иное предоставление доступа, согласование или комбинирование, ограничение доступа, удаление или уничтожение. Термины «обрабатывать» и «обработанный» будут иметь соответствующие значения.

Обработчик (Контроллер) — это физическое или юридическое лицо, орган власти, учреждение или любое другое лицо, которое обрабатывает персональные данные от имени управляющего данными.

Субподрядчик — это третье лицо, которому поставщик делегирует свои обязательства, которые определены договором, по которому поставщик осуществляет свою деятельность, в том числе аффилированные лица поставщика, не связанные прямыми договорными обязательствами с корпорацией Майкрософт.

Дополнительный обработчик данных (Саб-контроллер) — это третье лицо, привлекаемое корпорацией Майкрософт для осуществления деятельности, включающей обработку персональных данных Майкрософт, для которых сама корпорация Майкрософт является Обработчиком данных.

Ответ поставщика

Поставщики ежегодно подтверждают соответствие этим Требованиям с помощью онлайн службы, которая находится под управлением Майкрософт. Подробнее о том, как осуществляется управление соответствием, указано в Руководстве по программе SSPA.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел А. Управление	
1	Каждое соглашение между корпорацией Майкрософт и поставщиком (например, рамочный договор на предоставление услуг, описание работы, заказ на поставку и другие заказы) содержит соответствующие положения о защите Конфиденциальных и Персональных данных и безопасности Конфиденциальных и Персональных данных Майкрософт, включая запреты на продажу Персональных данных Майкрософт и их обработку, которые выходят за пределы прямых деловых отношений между Майкрософт и поставщиком. Для компаний, выступающих в роли обработчиков или дополнительных обработчиков данных в связи с осуществлением деятельности, связанной с персональными данными Майкрософт, соглашение должно включать в себя предмет и длительность обработки, характер и назначение обработки, тип Персональных данных Майкрософт и категории субъектов данных, а также обязательства и права Майкрософт.	Поставщик должен предоставить соответствующий контракт с Майкрософт. Для Обработчиков и дополнительных обработчиков данных необходимо включать описания обработки в применимое соглашение (*например*, описание работы, заказы на поставку). Примечание: компании, которые выполняют оперативные заказы на поставку, могут добавить необходимое описание процедур обработки на более позднем этапе процесса закупок.
2	Если Майкрософт подтверждает, что вы выполняете роль дополнительного обработчика данных, поставщик должен заключить с Майкрософт соответствующие соглашения о защите данных. Примечание: Майкрософт обозначит этот статус в вашем профиле, когда это применимо.	Стандартные договорные положения, Дополнение о данных заказчиков в режиме онлайн и (или) Дополнение об обработке данных поставщиков и партнеров профессиональных услуг.
3	Назначение ответственного и подотчетного сотрудника (или группы сотрудников) в компании, по соблюдению требований о защите данных.	Назначение роли ответственного лица или группы лиц для обеспечения соответствия Требованиям по защите данных поставщиком Майкрософт. Документ, описывающий полномочия и подотчетность этого лица или этой группы, в котором отражены их функции по обеспечению безопасности и (или) конфиденциальности.

№	Требования по защите данных оставщиками Майкрософт	Доказательство соответствия
	Раздел А. Управление (продолжение)	
4	Разработка, согласование и проведение ежегодного обучения по вопросам конфиденциальности и безопасности для сотрудников, у которых будет доступ к персональным данным, обрабатываемым поставщиком или к Конфиденциальным данным Майкрософт, в связи с осуществлением деятельности. Если у вашей компании нет готовых материалов, вы можете воспользоваться этим планом раскадровки и адаптировать его под особенности своей компании. Примечание: сотрудникам поставщика может потребоваться пройти дополнительное обучение, предоставляемое подразделениями Майкрософт.	Наличие ежегодных записей об участии в обучении, они должны предоставляться корпорации Майкрософт по запросу. Учебные материалы должны включать описание принципов обеспечения конфиденциальности и безопасности. Документирование соответствия требованиям по обучению будет включать подтверждение прохождения обучения, связанного с нормативными требованиями о конфиденциальности, обязательствами по обеспечению безопасности и соответствия применимым требованиям контракта и обязательствам.
5	Обработка Персональных данных Майкрософт должна осуществляться исключительно в соответствии с задокументированными инструкциями Майкрософт, включая сценарии передачи Персональных данных Майкрософт в третью страну или международную организацию, за исключением случаев, когда это требуется законодательством. В этих случаях Обработчик или дополнительный обработчик данных (поставщик) должен уведомить Контролера (Майкрософт) о таком юридическом требовании до обработки, если только законодательство в интересах государства не запрещает передачу такой информации.	Поставщик должен собирать и хранить все задокументированные инструкции Майкрософт (например, соглашение, описание работы или документацию по заказам) в электронном виде в месте, которое доступно сотрудникам поставщика и подрядчикам, участвующим в осуществлении деятельности.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел B. Уведомление	
6	Поставщик должен использовать форму Заявления о конфиденциальности корпорации Майкрософт при сборе Персональных данных от ее имени. Уведомление о конфиденциальности должно быть понятным и доступным субъектам данных, чтобы помочь им принять решение о передаче Персональных данных поставщику. Примечание: если ваша компания является Контроллером по обработке, вам нужно опубликовать собственное уведомление о конфиденциальности.	Поставщик использует актуальное Заявление о конфиденциальности корпорации Майкрософт, актуальная версия которого находится по ссылке fwdlink Заявление о конфиденциальности публикуется в любом контексте, где будет осуществляться сбор Персональных данных пользователя. Доступна оффлайн версия Заявления, которая предоставляется перед сбором данных и может быть использована при необходимости. Все оффлайн заявления о конфиденциальности должны соответствовать актуальной опубликованной версии и датированы соответствующим образом. Службами Майкрософт применяется для сотрудников уведомление о конфиденциальности данных Майкрософт.
7	При сборе Персональных данных Майкрософт с помощью обычного или записанного голосового звонка поставщики должны быть готовы обсудить методы сбора, обработки, использования и хранения применимых данных с Субъектами данных.	Предоставление расшифровки голосовых записей, включающую сведения о том, как осуществляется Обработка Персональных данных Майкрософт, включая: ▪ сбор, ▪ использование, ▪ хранение.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел C. Возможность выбора и согласие	
8	Если применимо: поставщик должен получить и зарегистрировать согласие Субъекта данных на все его действия по Обработке (включая любые новые и обновленные действия по Обработке) до начала сбора Персональных данных этого Субъекта данных. Поставщик отслеживает эффективность учета предпочтений, чтобы обеспечить сроки реагирования на изменения предпочтений, которые соответствуют более жестким требованиям применимого местного законодательства.	Поставщик должен быть способным продемонстрировать, согласие Субъекта на процедуру Обработки данных и что такое согласие охватывает все процессы Обработки поставщиком 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. Примечание: доказательством могут служить снимки экрана, описывающие взаимодействие с пользователем, экспериментирование со службой или возможность просмотра технической документации.
9	Поставщики, которые создают и контролируют веб-сайты и (или) приложения Майкрософт, должны предоставлять Субъектам данных понятное уведомление об использовании файлов cookie с возможностью включения или отключения этой функции в соответствии с заявлениями о конфиденциальности корпорации Майкрософт, и требованиями местного законодательства. Если бизнес-подразделением, с которым заключен контракт, не запрошено иное, поставщики должны использовать Стандартный баннер, разработанный 1ES, для отображения вариантов выбора. Это требование применяется, когда сайты предназначены для пользователей в странах Европейского союза/Европейской экономической зоны и других регионах с действующим законодательством о конфиденциальности и везде, где используется Положение о конфиденциальности Майкрософт. Примечание: бизнес-спонсорам Майкрософт необходимо зарегистрировать веб-сайты Майкрософт на внутреннем веб-портале по обеспечению соответствия (http://aka.ms/wcp), для каталогизации и управления списком файлов cookie.	Следует задокументировать назначение и тип каждого из применяемых файлов cookie. ▪ Постоянные файлы cookie не должны использоваться, если достаточно сессионных файлов cookie. ▪ При использовании постоянных файлов cookie их срок действия не должен превышать 13 месяцев с момента посещения сайта пользователем. Нужно подтвердить соответствие применимому законодательству ЕС, включая: ▪ использование условного обозначения «Конфиденциальность и файлы cookie» для заявления о конфиденциальности, ▪ получение подтверждения согласия пользователя перед использованием файлов cookie для таких целей, как реклама, и ▪ обеспечение истечения срока действия согласия или повторного запроса согласия не реже чем каждые 6 месяцев.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел D. Сбор	
10	Поставщик должен отслеживать сбор Персональных и (или) Конфиденциальных данных Майкрософт для гарантии того, что собираемая информация необходима для осуществления деятельности.	Поставщик может представить документацию, подтверждающую, что собираемые Персональные и (или) Конфиденциальные данные Майкрософт необходимы для осуществления деятельности. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
11	Перед сбором данных несовершеннолетних (в соответствии с действующим законодательством) Поставщик должен получить согласие в соответствии с местным законодательством о защите персональных данных.	Поставщик может предоставить документацию, подтверждающую согласие родителей/опекунов. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
	Раздел E. Хранение	
12	Персональные и Конфиденциальные данные Майкрософт не должны храниться дольше, чем это необходимо для осуществления деятельности, за исключением случаев, когда хранение Персональных и (или) Конфиденциальных данных Майкрософт требуется законодательством.	Поставщик должен соблюдать утвержденные политики хранения данных или требования к хранению данных, которые указаны корпорацией Майкрософт в контракте (например, в описании работы, в заказе на поставку). Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
13	По единоличному усмотрению Майкрософт Персональные и Конфиденциальные данные Майкрософт, которыми владеет поставщик или которые находятся под его контролем, должны быть возвращены в Майкрософт или быть уничтоженными по завершению осуществляемой деятельности либо по запросу Майкрософт. В приложениях должны быть предусмотрены процедуры, обеспечивающие надежное уничтожение данных, удаляемых как самими пользователями, так и по сигнализирующим факторам, таких как срок хранения данных. При необходимости уничтожения Персональных или Конфиденциальных данных Майкрософт поставщик должен сжечь, измельчить или уничтожить физические активы с Персональными и (или) Конфиденциальными данными Майкрософт таким образом, чтобы эти данные невозможно было прочесть или восстановить.	Необходимо вести учет утилизации Персональных и Конфиденциальных данных Майкрософт (в том числе, возврат данных в Майкрософт для их уничтожения). Если уничтожение запрошено или затребовано корпорацией Майкрософт, нужно предоставить акт об уничтожении, подписанный сотрудником поставщика.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел F. Субъекты данных	
	Субъекты данных имеют определенные права в соответствии с законодательством, включая права на доступ к своим Персональным данным, их удаление, изменение, экспорт, а также на ограничение доступа к Персональным данным и запрет на обработку Персональных данных («**Права субъектов данных**»). Для реализации своих прав в соответствии с законодательством в отношении Персональных данных Майкрософт Субъект данных должен разрешить Майкрософт выполнять следующие действия или должен самостоятельно выполнять следующие действия от имени Майкрософт:	
14	Содействовать Майкрософт с помощью подходящих технических и организационных мер, если это возможно, для того, чтобы выполнить свои обязательства по реагированию на запросы Субъектов данных, которые стремятся реализовать свои права, без неоправданной задержки. При отсутствии иных указаний со стороны корпорации Майкрософт поставщик направит всех обращающихся к нему Субъектов данных непосредственно в Майкрософт для осуществления их прав.	Поставщик должен хранить доказательства по документированию процессов и процедур для поддержки реализации прав Субъектов данных. Поставщик должен хранить задокументированное свидетельство тестирования. Такие доказательства должны предоставляться по запросу Майкрософт.
15	Если поставщик отвечает на запросы Субъекта данных напрямую или предоставляет веб-механизм для самообслуживания, поставщик должен обеспечить процессы и процедуры, необходимые для идентификации Субъекта данных, выполняющего запрос.	Поставщик обязан документировать методику, используемую для идентификации Субъектов данных Майкрософт. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
16	При получении от Майкрософт запроса на поиск Персональных данных Майкрософт о Субъекте данных, к которому невозможно обратиться с помощью веб-механизма самообслуживания, поставщик должен предпринять обоснованные усилия для поиска запрошенных Персональных данных и должен сохранить достаточные записи для подтверждения обоснованных приложенных усилий при поиске данных.	Поставщик обязан хранить документальные доказательства процедур, позволяющих установить хранение Персональных данных Майкрософт, и обязан предоставить соответствующие документы по запросу Майкрософт. Поставщик обязан вести записи, демонстрирующие предпринятые меры для выполнения запросов, связанных с правами субъектов данных. Эта документация включает в себя: ▪ дату и время запроса, ▪ действия, предпринятые в ответ на запрос, и запись с датой и временем предоставления информации Майкрософт. Поставщик должен предоставить подтверждение ведения документации по запросу Майкрософт.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел F. Субъекты данных (продолжение)	
17	Поставщик должен сообщать Субъектам данных о тех шагах, которые им потребуется выполнить для получения доступа или иного осуществления прав в отношении их Персональных данных Майкрософт.	Поставщик должен хранить документальные доказательства коммуникаций и процедур, связанных с доступом к Персональным данным Майкрософт. Поставщик должен хранить документальные доказательства и обязан представить их по запросу Майкрософт.
18	Фиксировать дату и время запросов, связанных с правами Субъектов данных, и действий, предпринятых поставщиком в ответ на такие запросы. Если запрос субъекта данных отклонен, поставщик по указанию Майкрософт должен предоставить Субъекту данных письменное обоснование. Предоставлять записи запросов Субъектов данных в корпорацию Майкрософт по требованию.	Поставщик должен вести учет запросов доступа к Персональным данным и документировать все изменения, вносимые в Персональные данные Майкрософт. Поставщик обязан документировать случаи отклонения запросов, сохранять доказательства их рассмотрения и утверждения корпорацией Майкрософт. Поставщик обязан предоставить подтверждение учета запросов доступа и отказов в предоставлении таких доступов к Персональным данным Майкрософт.
19	Поставщик должен предоставить Майкрософт или получить копию запрашиваемых Персональных данных Майкрософт для Субъекта данных, прошедшего проверку подлинности, в соответствующем печатном, электронном или устном формате.	Поставщик должен предоставлять Персональные данные Майкрософт Субъекту данных в формате, понятном и удобном для самого Субъекта и для поставщика.
20	Поставщик должен предпринять обоснованные меры предосторожности для гарантии того, что Персональные данные Майкрософт, предоставленные корпорации Майкрософт или Субъекту данных, прошедшему проверку подлинности, не могут быть использованы для идентификации другого лица.	Поставщик должен обеспечить документальное подтверждение мер предосторожности, чтобы не допустить идентификацию Субъекта данных с нарушением условий соглашения. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
21	Если Субъект данных считает, что его Персональные данные Майкрософт не являются полными и точными, поставщик должен передать вопрос в Майкрософт и при необходимости оказывать содействие Майкрософт для устранения разногласий.	Поставщик должен документально оформлять случаи разногласий и передавать вопрос на рассмотрение Майкрософт. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел G. Субподрядчики	
	Если поставщик намеревается привлечь Субподрядчика для обработки Персональных или Конфиденциальных данных Майкрософт, он обязан сделать следующее:	
22	Уведомить Майкрософт прежде чем оформить субподрядные услуги либо внести изменения касающиеся добавления или замены субподрядчиков. Примечание: подтвердите принятие этого обязательства, даже если сейчас вы не привлекаете Субподрядчиков, но можете привлечь их в будущем.	Необходимо подтвердить, что Персональные данные Майкрософт обрабатываются только компаниями, известными корпорации Майкрософт в соответствии с требованиями применимого контракта (например, описанием работы, приложением, заказом на поставку) или внесенными в базу данных программы SSPA. Поставщик может опубликовать свой список субподрядчиков онлайн либо включить их в список базы данных SSPA.
23	Документировать характер и объем Персональных и Конфиденциальных данных, обработанных Субподрядчиками, и следить за тем, чтобы собранная информация была необходима для осуществления деятельности.	Поставщик ведет необходимую документацию относительно Персональных и Конфиденциальных данных Майкрософт, раскрываемым или передаваемым Субподрядчикам. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
24	Если управляющим Персональными данными Майкрософт является сама корпорация Майкрософт, Субподрядчик должен использовать Персональные данные Майкрософт в соответствии с указанными контактными предпочтениями субъекта данных.	Необходимо продемонстрировать, как предпочтения Субъекта данных Майкрософт учитываются Субподрядчиками. Необходимо представить вспомогательную документацию (например, снимки экрана, соглашение об уровне услуг, техническое задание и т.д.), включающую в себя сроки учета изменений предпочтений Субподрядчика.
25	Ограничить обработку Персональных данных Майкрософт Субподрядчиком, за исключением случаев, когда это необходимо для выполнения контракта поставщика с Майкрософт.	Поставщик должен предоставить документацию, подтверждающую, что предоставляемые субподрядчику Персональные данные Майкрософт необходимы для осуществления деятельности. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел G. Субподрядчики (продолжение)	
26	Рассматривать жалобы на наличие признаков несанкционированной или незаконной обработки Персональных данных Майкрософт.	Поставщик должен предоставить наличие систем и процессов для рассмотрения жалоб, относительно несанкционированного использования или раскрытия Субподрядчиком Персональных данных Майкрософт. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
27	Незамедлительно уведомлять Майкрософт, в случае получения информации о том, что субподрядчик обрабатывает Персональные или Конфиденциальные данные Майкрософт в любых целях, не связанных с осуществлением деятельности.	Поставщик должен быть способным предоставить Субподрядчику инструкции и средства для информирования о несанкционированном использовании данных Майкрософт. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
28	Если поставщик собирает Персональные данные от третьих лиц по поручению Майкрософт, поставщик должен убедиться, что политика и практика защиты данных третьих лиц соответствуют договору поставщика с Майкрософт и этим Требованиям.	Поставщик может предоставить документацию о проведенной должным образом проверке в отношении политики и практики защиты данных третьей стороны. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
29	Незамедлительно предпринимать действия по устранению фактического или возможного ущерба, вызванного несанкционированной или незаконной обработкой Персональных и Конфиденциальных данных Майкрософт Субподрядчиком.	Поставщик должен обеспечить документальное подтверждение плана и процедуры, обязан предоставить документальное подтверждение по запросу Майкрософт.
	Раздел H. Качество	
30	Поставщик должен обеспечить целостность всех Персональных данных Майкрософт для того, чтобы гарантировать их точность, полноту и актуальность при обработке в указанных целях.	Поставщик должен продемонстрировать наличие процедур для проверки Персональных данных Майкрософт при их сборе, создании и изменении. Поставщик должен продемонстрировать наличие процедур мониторинга и выборки для непрерывной проверки точности и внесения корректив при необходимости. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел I. Мониторинг и принудительное исполнение	
31	Поставщик должен иметь план реагирования на инциденты, который предписывает ему без необоснованных задержек уведомлять Майкрософт о ставших известными нарушениях безопасности данных. Поставщик обязан по запросу или указанию Майкрософт сотрудничать с Майкрософт в любом расследовании, устранении рисков или последствий инцидента, в том числе предоставлять Майкрософт данные, информацию, доступ к персоналу поставщика или к оборудованию для проведения криминалистической проверки. Примечание: Ознакомьтесь с Руководством по программе SSPA о том, как уведомить Майкрософт об инциденте.	Поставщик должен иметь план реагирования на инциденты, предусматривающий уведомление клиентов (Майкрософт), как описано в этом разделе. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
32	Реализовать план устранения последствий и контролировать разрешение каждого инцидента с данными для обеспечения своевременного принятия соответствующих корректирующих мер.	Поставщик должен иметь задокументированными процедуры по реагированию на нарушение безопасности данных вплоть до устранения инцидента. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.
33	В случаях, когда Майкрософт является Управляющим Персональными данными корпорации Майкрософт, установить формальный процесс рассмотрения жалоб для реагирования на все жалобы по защите данных, относительно Персональных данных Майкрософт.	Поставщик располагает средствами для приема жалоб, касающихся Персональных данных Майкрософт, и имеет задокументированную процедуру рассмотрения таковых. Поставщик должен предоставить документальное подтверждение по запросу Майкрософт.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел J. 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 Майкрософт в соответствии с надлежащей отраслевой практикой и требованиями действующего законодательства. Программа обеспечения безопасности поставщика должна соответствовать стандартам, указанным в пунктах 34–50 ниже.	В качестве приемлемой замены для раздела J подойдет действующая сертификация ISO 27001. Для применения этой замены обратитесь к SSPA. Примечание: вам потребуется предоставить сертификацию.
34	Ежегодно проводить оценку безопасности сети, которая включает в себя следующее: ▪ проверку крупных изменений в среде, например новых системных компонентов, топологии сети и правил брандмауэра, ▪ поиск уязвимостей и ▪ ведение журналов изменений.	Поставщик располагает документацией по оценке 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.
35	Поставщик обязан сформулировать, распространить и внедрить политику о мобильных устройствах, которая обеспечивает защиту Персональных или Конфиденциальных данных Майкрософт, а также ограничивает использование и доступ к этим данным на мобильных устройствах.	Поставщик должен продемонстрировать использование соответствующей политики о мобильных устройствах в тех случаях, когда для обработки Персональных или Конфиденциальных данных Майкрософт требуется использовать мобильное устройство.
36	Все активы, используемые для поддержки производительности должны быть учтены и иметь определенного владельца. Поставщик несет ответственность за инвентаризацию таких информационных активов, обеспечение их приемлемого и санкционированного использования, а также за обеспечение надлежащего 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 носителей данных, которые больше не нужны.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел J. Безопасность (продолжение)	
37	Разработать и реализовать процедуры управления доступом для предотвращения несанкционированного доступа к любым Персональным или Конфиденциальным данным Майкрософт, 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, ▪ надежные параметры для выбора учетных данных проверки подлинности, ▪ отключение учетных записей пользователей при увольнении в течение 48 часов, ▪ надежные средства контроля паролей, обеспечивающие соблюдение длины и сложности пароля и предотвращающие его повторное использование. Поставщик демонстрирует наличие установленного процесса проверки доступа пользователей к Персональным или Конфиденциальным данным Майкрософт с соблюдением принципа предоставления минимальных прав. Эта процедура включает в себя следующее: ▪ четко определенные роли пользователей, ▪ процедуры для проверки и утверждения прав доступа к ролям, и ▪ проверка того, что у пользователей с ролями, которым предоставляется доступ к данным Майкрософт, имеется задокументированное обоснование принадлежности к соответствующей роли или группы.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел J. Безопасность (продолжение)	
38	Определить и внедрить процедуры управления исправлениями, которые определяют приоритетность исправлений безопасности для систем, используемых для обработки Персональных или Конфиденциальных данных Майкрософт. Эти процедуры включают: ▪ определенный подход по оценке рисков для определения приоритетности исправлений безопасности; ▪ возможность обработки и внедрения аварийных исправлений; ▪ применимость к программному обеспечению операционной системы и сервера, такому как сервер приложений и программное обеспечение баз данных, ▪ документировать риск, который устраняет исправление, и отслеживать любые исключения, и требования к выходу из эксплуатации программного обеспечения, которое больше не поддерживается компанией-автором.	Поставщик может продемонстрировать внедренную процедуру управления исправлениями, которая соответствует этим Требованиям и охватывает, как минимум, следующее: ▪ Присвоение степени серьезности для определения приоритетов. (Определения серьезности должны быть задокументированы). ▪ Предоставить задокументированную процедуру внедрения аварийных исправлений. ▪ Проследить, чтобы не использовались операционные системы, которые больше не поддерживаются компанией-автором. ▪ Запись управления исправлениями, которые отслеживают утверждения и исключения.
39	Установить антивирусное и антивредоносное программное обеспечение на оборудование, подключенное к сети, используемое для обработки Персональных и Конфиденциальных данных Майкрософт, включая серверы, производственные и учебные компьютеры для защиты от потенциально опасных вирусов и вредоносных программных приложений. Обновлять антивирусное программное обеспечение ежедневно или по указанию поставщика антивирусного/антивредоносного программного обеспечения. Примечание: это относится ко всем операционным системам, включая Linux.	Поставщик может предоставить записи, подтверждающие активное использование программного обеспечения для защиты от вирусов и вредоносных программ. Примечание: это требование относится ко всем операционным системам.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел J. Безопасность (продолжение)	
40	Поставщики, разрабатывающие программное обеспечение для Майкрософт, в процессе создания должны реализовывать принципы встроенной безопасности.	Документы поставщика с техническими спецификациями должны включать пункты по проверке безопасности в рамках циклов разработки.
41	Применять программу защиты от потери данных («**DLP**») для предотвращения атак, потерь и другой несанкционированной активности. Данные должны быть должным образом классифицированы, маркированы и защищены, а поставщик должен отслеживать используемые информационные системы, в которых обрабатываются Персональные или Конфиденциальные данные Майкрософт, на предмет атак, потерь и другой несанкционированной активности. Программа DLP как минимум: ▪ требует использование стандартных хостов, сети и облачных систем обнаружений атак («**IDS**»), если вы храните Персональные или Конфиденциальные данные Майкрософт, ▪ внедрение усовершенствованных систем обнаружения атак («**IPS**»), настроенных для отслеживания и активного предотвращения потери данных, ▪ в случае взлома системы требуется провести анализ системы, чтобы убедится, что все остаточные уязвимости устранены, ▪ документировать необходимые процедуры по контролю средств, отслеживающих нарушения в системе, ▪ формирует процесс реагирования на инциденты и управления ими; применяется при обнаружении нарушения безопасности данных, ▪ необходимо сообщать (всем сотрудникам и субподрядчикам поставщика, не имеющим отношения к деятельности поставщика) о несанкционированном скачивании и использовании Персональных или Конфиденциальных данных Майкрософт.	Должна быть задокументированная программа DLP с установленными процедурами по предотвращению вторжений, потери данных и других незаконных действий (и как минимум со всеми пунктами, указанными в этом разделе).

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел J. Безопасность (продолжение)	
42	Незамедлительно сообщать вышестоящему руководству и корпорации Майкрософт о результатах расследования в рамках реагирования на инциденты.	Поставщик должен располагать необходимыми системами и процедурами для передачи корпорации Майкрософт результатов расследований в рамках реагирования на инциденты.
43	Системные администраторы, административный персонал, руководство и третьи лица должны ежегодно проходить обучение по безопасности.	Организуйте учебную программу по вопросам безопасности, которая включает в себя следующее: ▪ ежегодное обучение по вопросам реагирования на инциденты и ▪ моделированные мероприятия, автоматические механизмы для эффективного реагирования на инциденты в кризисных ситуациях, ▪ распространение информации о предотвращении инцидентов, например о рисках, связанных со скачиванием вредоносного программного обеспечения.
44	Поставщик должен обеспечить процессы таким образом, чтобы планирование и резервное копирование защищали Персональные и Конфиденциальные данные Майкрософт от несанкционированного использования, доступа, раскрытия, изменения и уничтожения.	Поставщик может продемонстрировать задокументированные процедуры реагирования и восстановления с подробным описанием того, как компания будет управлять процессами в случае аварии, поддерживая информационную безопасность на должном уровне, в соответствии с утвержденными руководством целями обеспечения непрерывности информационной безопасности. Поставщик может продемонстрировать как определены и внедрены процедуры периодического резервного копирования, безопасного хранения и эффективного восстановления критически важных данных.
45	Разработать и протестировать планы непрерывности бизнес-процессов и аварийного восстановления.	План аварийного восстановления должен включать в себя следующее: ▪ Обозначенные критерии для определения того, является ли система критически важной для функционирования бизнеса поставщика. ▪ Перечисленные критические системы на основе определенных критериев, которые необходимо восстановить в случае аварии. ▪ Заданная процедура аварийного восстановления для каждой критически важной системы, позволяющая инженеру, который незнаком ранее с системой, восстановить приложение в течение 72 часов. ▪ Проверка и повторное рассмотрение планов аварийного восстановления на предмет выполнимости целей восстановления не реже одного раза в год.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел J. Безопасность (продолжение)	
46	Необходимо проверять подлинность физического лица, прежде чем предоставлять ему личный доступ к Персональным или Конфиденциальным данным Майкрософт, и ограничивать его доступ в соответствии с разрешенным для него набором действий, необходимым для осуществления Деятельности.	Нужно проверить, что все идентификаторы пользователей уникальны и каждый из них имеет метод проверки подлинности, соответствующий отраслевому стандарту, например Azure Active Directory. При доступе с расширенными правами (административного или иного типа) должна производиться двухфакторная проверка подлинности, например с использованием смарт-карты или телефона. Обязательное наличие задокументированной программы информационной безопасности, которая контролирует доступ всех сотрудников и субподрядчиков поставщика к Персональным или Конфиденциальным данным Майкрософт, в том числе, что он предоставляется исключительно в том объеме и на тот временной период, которые необходимы для осуществления деятельности.
47	Поставщик обязан обеспечить защиту всех данных, обрабатываемых в связи с осуществлением деятельности, во время их передачи по сетям, используя шифрование на базе протокола Transport Layer Security («**TLS**») или Internet Protocol Security («**IPsec**»). Эти методы описаны в требованиях NIST 800-52 и NIST 800-57. Допустимо использовать эквивалентный отраслевой стандарт. Поставщик должен отказаться от передачи любых Персональных или Конфиденциальных данных Майкрософт по незашифрованным каналам.	Требуется разработать и реализовать процедуру по передаче, развертыванию и замене TLS или других сертификатов.
48	Все устройства поставщика (ноутбуки, рабочие станции и т. д.), которые будут иметь доступ к Персональным или Конфиденциальным данным Майкрософт или обрабатывать их, должны использовать дисковое шифрование.	Все устройства, используемые для обработки Персональных или Конфиденциальных данных Майкрософт, должны быть зашифрованы с помощью Bitlocker или другого аналогичного отраслевого решения для шифрования дисков.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел J. Безопасность (продолжение)	
49	Должны быть предусмотрены системы и процедуры (при использовании актуальных отраслевых стандартов, например описанных в стандарте NIST 800-111) для шифрования любых неактивных (хранимых) Персональных и (или) Конфиденциальных данных Майкрософт, включая такие данные: ▪ учетные данные (например, имена пользователей и пароли), ▪ данные о платежных средствах (например, кредитные карты и номера банковских счетов), ▪ персональные данные, связанные с иммиграцией, ▪ медицинские данные (например, номера медицинских записей, 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 Майкрософт (например, клиентам SharePoint, пользователям документов O365, клиентам OneDrive), ▪ материалы, которые относятся к продуктам Майкрософт, которые не были официально анонсированы, ▪ дата рождения, ▪ сведения о ребенке, ▪ 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, для двухфакторной проверки подлинности или сброса пароля), ▪ девичья фамилия матери.	Обеспечьте шифрование Персональных и Конфиденциальных данных Майкрософт, указанных в этой последовательности, на этапе хранения.
50	Аноминизировать все Персональные данные Майкрософт, которые используются в среде разработки или тестирования.	Персональные данные Майкрософт не должны использоваться в ходе разработок или тестирования. Но если их использование необходимо, Персональные данные должны быть анонимными для предотвращения идентификации Субъектов данных или злоупотребления Персональными данными.

№	Требования по защите данных поставщиками Майкрософт	Доказательство соответствия
	Раздел J. Безопасность (продолжение)	
		Примечание: Анонимизированные данные отличаются от псевдо анонимных. Анонимизированные данные не связаны с идентифицированным или идентифицируемым физическим лицом, если Субъект Персональных данных не может быть идентифицирован.

Основные определения

Уполномоченный представитель — лицо, которому предоставлено право подписи от имени компании на соответствующем уровне. Это лицо должно обладать необходимыми знаниями в области конфиденциальности и безопасности или проконсультироваться с экспертом в данной области перед отправкой ответа на действие программы SSPA. Кроме того, добавляя свое имя к форме SSPA, представитель подтверждает, что прочитал и понял эти Требования.

EUDPR — Постановление (ЕС) 2018/1725 Европейского парламента и Европейского совета от 23 октября 2018 г. о защите физических лиц в отношении обработки персональных данных учреждениями, органами, кабинетами и агентствами Европейского союза, свободной передачи таких данных, отменяющее Постановление (ЕС) 45/2001 и Решение 1247/2002/EC0.

Фрилансер — лицо, которое выполняет задачи или предоставляет услуги по запросу, используя цифровые платформы или другими способами.

GDPR — Постановление (ЕС) 2016/679 Европейского парламента и Европейского совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и свободной передачи таких данных, отменяющее Директиву 95/46/ЕС (Общий регламент о защите данных).

Требования к защите конфиденциальности данных — это GDPR, EUDPR, местные законы о защите данных ЕС/ЕЭЗ, Закон штата Калифорния о защите конфиденциальности потребителей, параграф 1798.100 и др. Гражданского кодекса штата Калифорния (далее «CCPA»), Закон о защите данных Великобритании от 2018 года и любые связанные и последующие законы, нормативно-правовые акты и другие требования законодательства, действующие в Великобритании, а также любые применимые законы, нормативно-правовые акты и другие требования законодательства, связанные с (a) конфиденциальностью и защитой данных или (б) использованием, сбором, удержанием, хранением, защитой, раскрытием, передачей, уничтожением и другой обработкой любых Персональных данных.

Типовые положения ЕС и Стандартные договорные положения означают (i) стандартные положения о защите данных для передачи персональных данных обработчикам, созданным в третьих странах, которые не обеспечивают адекватный уровень защиты данных, как описано в статье 46 GDPR и утверждено решением Европейской комиссии (ЕС) 2021/914 от 4 июня 2021 года; (ii) любые последующие стандартные договорные положения, принятые (a) Европейской комиссией, (b) Европейским органом по надзору за защитой данных и утвержденные Европейской комиссией, (c) Соединенным Королевством в соответствии с Общим федеральным законом Великобритании о

защите данных, (d) Швейцарией в соответствии с Федеральным законом Швейцарии о защите данных или (e) правительством юрисдикции, отличной от Швейцарии, Соединенного Королевства и юрисдикций, входящих в Европейский союз / Европейскую экономическую зону, где эти положения регулируют международную передачу персональных данных, должны быть включены и обязательны для поставщика со дня их принятия.

Хостинг веб-сайтов — это онлайн служба, которая создает и (или) поддерживает веб-сайты от имени корпорации Майкрософт в домене Microsoft, т.е. поставщик предоставляет все материалы и услуги, необходимые для создания и поддержки сайта, и делает его доступным в интернете. “Провайдер услуг хостинга веб-сайтов" или "веб-хост" — это поставщик, который предоставляет инструменты и услуги, необходимые для просмотра веб-сайта или веб-страницы в интернете, например, файлы cookie или веб-маячки для рекламы.