# Отдел закупок Майкрософт

## Руководство по Программе обеспечения защиты и конфиденциальности данных для поставщиков (SSPA)

Версия 8

Июнь 2022

# Введение

Microsoft Corporation (далее — «корпорация Майкрософт» или «Майкрософт») считает право на соблюдение конфиденциальности основополагающим. Мы видим свою миссию в том, чтобы помогать людям и организациям по всему миру достигать большего, и ежедневно делаем все, чтобы завоевать и укрепить доверие наших клиентов.

Эффективное обеспечение конфиденциальности и безопасности имеет критически важное значение для нашей деятельности, выполнения обязательств перед клиентами и соблюдения законодательных требований ряда стран. Стандарты, устанавливаемые политиками обеспечения конфиденциальности и безопасности Майкрософт, отражают наши корпоративные ценности и распространяются на поставщиков (таких как ваша компания), которые обрабатывают данные Майкрософт от нашего имени.

Корпоративная программа Майкрософт по обеспечению безопасности и конфиденциальности для поставщиков (Supplier Security and Privacy Assurance, далее — **SSPA**) дает нашим поставщикам базовые указания по обработке данных в виде Требований к защите данных поставщиками Майкрософт (Microsoft Supplier Data Protection Requirements, далее — **DPR**), которые можно просмотреть в SSPA на странице Microsoft.com/Procurement. Обратите внимание, что для поставщиков могут устанавливаться дополнительные требования на уровне организации. Эти требования вырабатываются и коммуницируются за пределами SSPA группой Майкрософт, ответственной за взаимодействие с поставщиком.

Основные условия SSPA определены в DPR. Дополнительные сведения о программе см. в разделе FAQ (Вопросы и ответы) на этой странице. Вы также можете обратиться к нашей международной команде специалистов по электронной почте: SSPAHelp@microsoft.com.

## Обзор программы SSPA

SSPA — это программа, совместно организованная следующими подразделениями корпорации Майкрософт: отделом закупок (Microsoft Procurement), внешних корпоративных и юридических связей (Corporate External and Legal Affairs) и отдела корпоративной безопасности (Corporate Security). Ее цель — обеспечить соблюдение требований к конфиденциальности и безопасности данных нашими поставщиками.

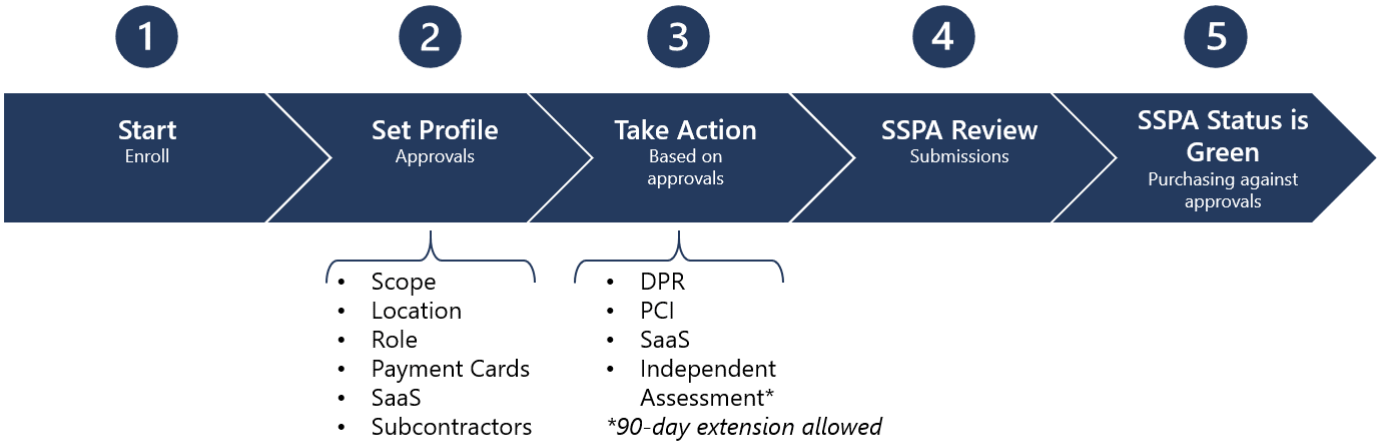
Программа SSPA действует по всему миру для всех поставщиков, которые обрабатывают персональные или конфиденциальные данные Майкрософт в связи с осуществляемой ими деятельностью (например, предоставлением услуг, лицензий на программное обеспечение, облачных служб) в рамках заключенного с Майкрософт контракта (например, условия заказа на поставку, основное соглашение) (далее — **осуществлять деятельность**, **осуществление деятельности** или **осуществляемая деятельность**).

SSPA позволяет поставщику выбирать профили обработки данных в соответствии с товарами и (или) услугами, предоставляемыми поставщиком в рамках осуществления деятельности согласно условиям контракта. Выбранные профили определят требования по обеспечению соответствия для Майкрософт.

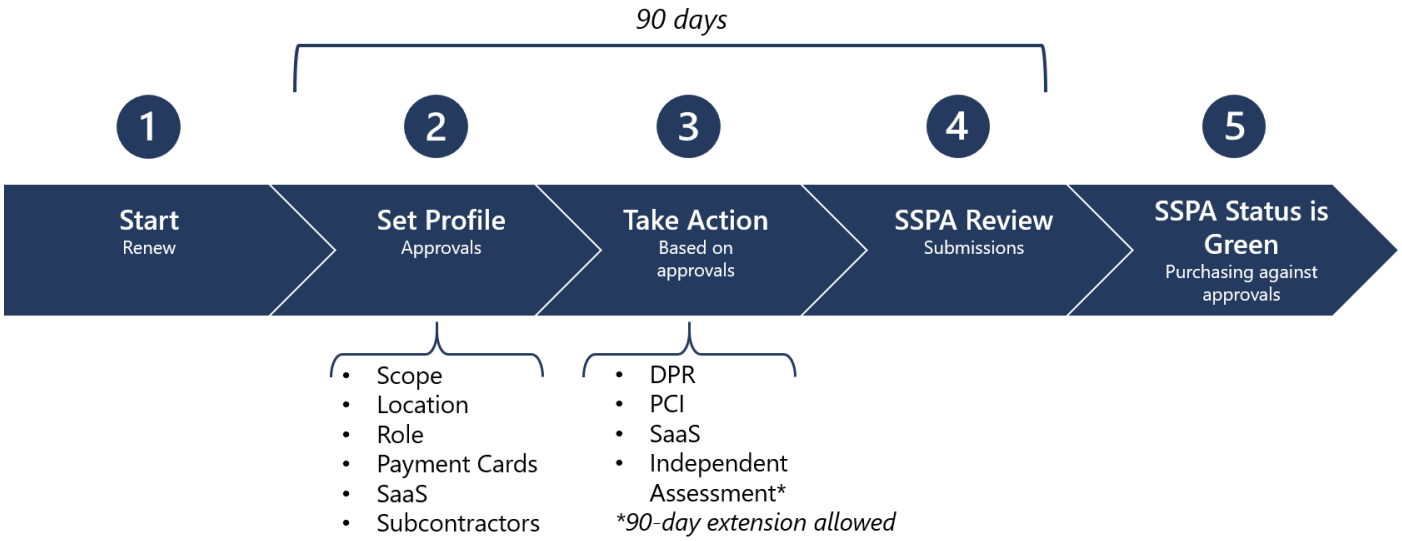
**Все поставщики, зарегистрированные в программе, обязаны ежегодно проходить самостоятельную аттестацию на соответствие DPR**. Ваш профиль обработки данных определяет, будут ли применены полные требования DPR или только их часть. К поставщикам, обрабатывающим данные, которые по мнению Майкрософт представляют более высокий риск, могут предъявляться дополнительные требования, например прохождение независимой проверки соответствия требованиям. Поставщикам, которые входят в утвержденный список Дополнительных обработчиков данных корпорации Майкрософт, будет предложено пройти независимую проверку на соответствие требованиям.

**Важно:** по результатам действий, выполняемых в ходе проверки, определяется статус SSPA: «Зеленый» (соответствует требованиям) или «Красный» (не соответствует требованиям). Средства закупок Майкрософт проверяют наличие «Зеленого» статуса в рамках программы SSPA (для каждого поставщика, в отношении которого действуют эти требования) и только после этого разрешают последующее взаимодействие.

## Схема процесса SSPA: регистрация нового поставщика



## Схема процесса SSPA: ежегодное продление для поставщика




# Область действия программы SSPA

Чтобы определить, обрабатываете ли вы как поставщик персональные и (или) конфиденциальные данные Майкрософт, обратитесь к списку примеров в таблицах ниже. Учтите, что эти примеры и список не являются исчерпывающими.

**Примечание:** учитывая конфиденциальность обрабатываемых данных, представитель Майкрософт может запросить регистрацию, выходящую за рамки этого списка.

## Персональные данные по типам данных

**Примеры (список не является исчерпывающим)**

| Конфиденциальные данные |
|---|
| Данные, относящиеся к детям |
| Генетические данные, биометрические данные или данные о состоянии здоровья |
| Расовое или этническое происхождение |
| Политические, религиозные или философские взгляды, мнения и предпочтения |
| Членство в профсоюзах |
| Половая жизнь или сексуальная ориентация физического лица |
| Иммиграционный статус (виза, разрешение на работу и др.) |

| |
|---|
| Государственные идентификационные данные (паспорт, водительские права, виза, номер в системе социального страхования, другие национальные идентификационные номера) |
| Точные сведения о местонахождении пользователя (в радиусе 300 м) |
| Данные личных банковских счетов |
| Номер и срок действия кредитной карты |
| **Материалы клиента** |
| Документы, фотографии, видеоролики, музыка и т. д. |
| Оценки и (или) отзывы по продуктам и услугам |
| Ответы на опросы |
| История просмотра веб-страниц, интересы и избранные страницы |
| Высказывания в рукописной, печатной и устной форме (голосовая/аудиосвязь, чаты и общение с ботами) |
| Учетные данные (пароли, подсказки для пароля, имя пользователя, биометрические данные для идентификации) |
| Данные клиента, связанные с обращением в службу поддержки |
| **Собираемые и генерируемые данные** |
| Неточные данные о местоположении |
| IP-адрес |
| Параметры и персональные настройки устройств |
| Данные об использовании служб на веб-сайтах, отслеживание посещений веб-страниц |
| Данные социальных сетей и отношения между их пользователями |
| Данные об активности с подключенных устройств, таких как фитнес-трекеры |
| Контактные данные такие как имя, адрес, номер телефона, адрес электронной почты, дата рождения, зависимые лица и контакты для экстренной связи |
| Данные по оценке мошенничества и рисков, проверка прошлых данных |
| Сведения о страховании, пенсиях и льготах |
| Резюме соискателей, заметки в ходе собеседований, отзывы |
| Metadata and telemetry |
| **Банковские данные** |
| Данные платежных средств |
| Номер и срок действия кредитной карты |
| Сведения о банковских переводах |
| Номер банковского счета |

| |
|---|
| Заявки на кредит и кредитная линия |
| Налоговые документы и идентификационные номера |
| Инвестиционные данные и данные о расходах |
| Данные о корпоративных картах |
| Обезличенная информация о конечном пользователе (EUPI)<br>(Удостоверения, созданные Майкрософт для идентификации пользователей продуктов и служб Майкрософт) |
| Глобальный уникальный идентификатор (GUID) |
| Номер карты или уникальный идентификатор (PUID) |
| Хешированные данные, позволяющие установить личность конечного пользователя (EUII) |
| Идентификаторы сеансов |
| Идентификаторы устройств |
| Диагностические данные |
| Регистрационные данные журналов |
| Online Customer Data |
| Microsoft online enterprise customer (example: Azure tenant, M365 tenant…) |
| Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …) |
| Microsoft enterprise customer (on premises customer) |
| Support data (example: Customer originates a ticket) |
| Account data (example: billing data, e-commerce) |
| Survey/Event Registration/Training |

# Конфиденциальные данные Майкрософт по классам данных

## Примеры (список не является исчерпывающим):

| Строго конфиденциальные данные |
|---|
| Информация, связанная с разработкой, тестированием или изготовлением продуктов Майкрософт или компонентов продуктов Майкрософт<br>*Программное обеспечение, веб-службы, службы или оборудование Майкрософт, продаваемое по любым коммерческим каналам, считается* ***продуктом Майкрософт****.* |
| Маркетинговая информация об устройствах Майкрософт до их выпуска на рынок |
| Необъявленные корпоративные финансовые данные Майкрософт, регулируемые правилами SEC |

| Конфиденциальные данные |
| --- |
| Лицензионные ключи на продукты Майкрософт, распространяемые любым методом от имени корпорации Майкрософт |
| Информация, связанная с разработкой или тестированием внутренних бизнес-приложений Майкрософт (LOB) |
| Предрелизные маркетинговые материалы по программному обеспечению и службам Майкрософт, например Office, SQL, Azure и др. |
| Письменная, проектная, электронная или печатная документация для любых служб или продуктов Майкрософт, таких как устройства (руководства по процессам и процедурам, данные о конфигурации и др.). |

**Важно:** представитель Майкрософт может потребовать включить в область действия программы другие данные, не указанные в этом списке.

# Профиль обработки данных

Поставщики Майкрософт полностью контролируют свой профиль обработки данных SSPA.

Это позволяет поставщикам самим решать, на какие типы взаимодействия им требуется право для осуществления деятельности. Делайте выбор с особой тщательностью и учитывайте те мероприятия по обеспечению соответствия, которые потребуется выполнить для получения утверждения. **См. раздел «Требования к обеспечению соответствия» ниже и Приложение А**.

Рабочие группы Майкрософт смогут регистрировать взаимодействие с поставщиками только в том случае, если деятельность по обработке данных последних соответствует утверждениям, полученным поставщиком.

Поставщики могут изменять свой профиль обработки данных в любое время в течение года, **если им не назначено открытых задач**. При внесении изменения будет назначено соответствующее действие, которое нужно выполнить для получения утверждений. Пока новые назначенные требования не выполнены, будут действовать существующие полученные ранее утверждения.

Если новые задачи не будут выполнены в течение разрешенного периода в 90 дней, статус поставщика в программе SSPA изменится на «Красный» (не соответствует требованиям) и его учетная запись может быть деактивирована в системах расчета с поставщиками Майкрософт.

| Утверждения для обработки данных | |
| --- | --- |
| 1 | Область обработки данных<br>▪ Конфиденциальные |

| | |
|---|---|
| | ▪ Персональные и конфиденциальные данные |
| 2 | Место обработки данных<br>▪ В корпорации Майкрософт или у клиента<br>▪ У поставщика |
| 3 | Роль обработки данных<br>▪ Управляющий данными (независимый или совместный)<br>▪ Обработчик данных<br>▪ Дополнительный обработчик данных (назначен корцией Майкрософт) |
| 4 | Обработка платежных карт<br>▪ Да<br>▪ Неприменимо |
| 5 | Программное обеспечение как услуга<br>▪ Да<br>▪ Неприменимо |
| 6 | Использование субподрядчиков<br>▪ Да<br>▪ Неприменимо |

# Что учитывается при утверждении

## Область обработки данных

Конфиденциальные данные

Выберите это утверждение, если осуществляемая деятельность поставщика будет включать только обработку конфиденциальных данных Майкрософт.

При выборе этого варианта утверждения вы не сможете получить право на обработку персональных данных.

Персональные и конфиденциальные данные

Выберите это утверждение, если осуществляемая деятельность поставщика будет включать обработку персональных и конфиденциальных данных Майкрософт.

_____

## Место обработки

В корпорации Майкрософт или у клиента

Выберите это утверждение, если осуществляемая деятельность поставщика включает обработку поставщиком данных в сетевой среде Майкрософт, в которой персонал использует учетные данные доступа *@microsoft.com*, или в среде клиента Майкрософт.

Не выбирайте этот вариант в следующих случаях.

- Поставщик работает с назначенным офшорным центром Майкрософт.
- Поставщик предоставляет ресурсы корпорации Майкрософт, и эти ресурсы периодически используются как в сети Майкрософт, так и за ее пределами. Обработка данных за пределами сети рассматривается как обработка данных у поставщика.

У поставщика
Если условие «в корпорации Майкрософт или у клиента» (как описано выше) не применяется, выберите этот вариант

_____

## Роль обработки данных

**Управляющий данными** (распространяется на независимых и совместных управляющих)

Выберите это утверждение, если **все** аспекты осуществляемой деятельности поставщика соответствуют определению роли обработки данных управляющего (см. DPR).

При выборе этого варианта утверждения вы не сможете получить право на обработку персональных данных с назначением роли «обработчик данных». Если поставщик одновременно является обработчиком данных и управляющим данными по отношению к Майкрософт, выберите роль «Обработчик данных», а не «Управляющий данными».

### Обработчик данных

Это самая распространенная роль поставщика, обрабатывающего данные от имени Майкрософт. Ознакомьтесь с определением роли «Обработчик данных» в DPR.

### Дополнительный обработчик данных

Дополнительный обработчик данных — это третье лицо, привлекаемое корпорацией Майкрософт для осуществления деятельности, включающей обработку персональных данных Майкрософт, для которых сама корпорация Майкрософт является Обработчиком данных. Поставщики не могут самостоятельно идентифицировать себя в качестве Дополнительного обработчика данных в Майкрософт, поскольку это требует предварительного одобрения внутренними группами по защите конфиденциальности. Поставщики могут являться лишь Дополнительными обработчиками данных, при условии, что Майкрософт является Обработчиком данных, а поставщик обрабатывает типы персональных данных, которые соответствуют требованиям корпорации. Дополнительные обработчики данных могут иметь дополнительные требования к контракту и соответствию требованиям, включая Дополнение о защите данных и независимую оценку (см. ниже).

## Обработка платежных карт

Выберите это утверждение, если любая часть данных, обрабатываемых поставщиком, включает данные для обработки кредитных или любых других платежных карт от имени Майкрософт.

Этот вариант утверждения позволяет поставщику осуществлять деятельность, связанную с обработкой платежных карт.

_____

## Программное обеспечение

Отдел закупок Майкрософт направляет покупателей на процесс приема всех покупок программного обеспечения, который включает различные проверки, в том числе проверку SSPA, чтобы решить, входит ли поставщик, предоставляющий программное обеспечение, в сферу управления SSPA. (Покупатели Майкрософт могут ознакомиться с шагами, описанными на внутренней странице ProcureWeb Software and Cloud Service для получения более подробной информации). Если требуется SSPA, поставщикам также может потребоваться выбрать профиль "Программное обеспечение как услуга" (SaaS). Для поставщиков, зарегистрированных в SSPA, это можно сделать при заполнении профиля обработки данных на портале соответствия поставщиков Майкрософт (Microsoft Supplier Compliance Portal).

Для целей соответствия требованиям SSPA следует рассматривать SaaS в широком смысле, включая также платформу как услугу (PaaS) и инфраструктуру как услугу (IaaS). (Чтобы узнать больше о SaaS, ознакомьтесь с этим пояснением).

## Программное обеспечение как услуга (SaaS)

Программное обеспечение как услуга (SaaS) позволяет пользователям подключаться к облачным приложениям и использовать их через Интернет.

Майкрософт определяет **Программное обеспечение как услугу (SaaS)** как программное обеспечение на основе общего кода, используемое в модели “один ко многим" на основании оплаты за использование или подписки в зависимости от показателей использования. Поставщик облачных услуг разрабатывает и обслуживает облачное программное обеспечение, обеспечивает автоматическое обновление программного обеспечения и предоставляет программное обеспечение своим клиентам через Интернет по принципу "один ко многим" с оплатой по факту использования. Такой метод предоставления программного обеспечения и лицензирования позволяет не покупать и устанавливать программное обеспечение на каждом отдельном компьютере, а получать доступ к нему через Интернет по подписке.

**Примечание**: Большинству поставщиков SaaS необходимо добавить одобрение субподрядчика на портале соответствия поставщиков Майкрософт (Microsoft Supplier Compliance Portal), если персональные или конфиденциальные данные Майкрософт размещаются на платформе третьей стороны.

## Использование субподрядчиков

Выберите это утверждение, если поставщик использует субподрядчиков для осуществления деятельности. Ознакомьтесь с определениями в DPR.

Это также касается Фрилансеров (см. DPR)

# Требования к обеспечению соответствия

## Требования на основе утверждений профиля

Утверждения, выбранные поставщиком в профиле обработки данных, помогают SSPA оценить уровень риска взаимодействия Майкрософт с поставщиком с точки зрения обработки данных. Требования для обеспечения соответствия SSPA различаются в зависимости от утверждений в профилях поставщика. В этом разделе приводится объяснение для различных требований SSPA.

Также существуют сочетания параметров профиля, которые могут повысить или снизить объем требований для соответствия. Эти сочетания указаны в Приложении A, и именно эти требования будет необходимо выполнить на портале соответствия поставщиков при завершении заполнения профиля. Вы всегда можете проверить, как ваш сценарий соответствует этой схеме, попросив специалистов по программе SSPA рассмотреть вашу ситуацию.

**Действие:** найдите свой профиль утверждения в Приложении A и просмотрите соответствующие требования к обеспечению соответствия, а также варианты независимой проверки соответствия, если они применяются.

**Важно:** если вы выбираете варианты «Программное обеспечение как услуга» (SaaS), «Субподрядчики», «Хостинг веб-сайтов» или «Платежные карты» в своем профиле, вам потребуется пройти дополнительную проверку соответствия требованиям.

## Самостоятельная аттестация на соответствие DPR

Все поставщики, зарегистрированные в программе SSPA, обязаны провести самостоятельную аттестацию на соответствие DPR в течение 90 дней с момента получения запроса. Этот запрос будет отправляться ежегодно, но может отправляться и чаще в случае изменения профиля обработки данных в течение года.  Если ваша компания не предоставит необходимые данные в течение 90 дней, ей будет присвоен «Красный» статус в рамках программы SSPA, свидетельствующий о несоответствии требованиям последней. Новые заказы на поставку в вашей области не будут обрабатываться, пока компания не получит «Зеленый» статус в рамках программы SSPA, свидетельствующий о соответствии ее требованиям.

Регистрируемые впервые поставщики перед началом деятельности должны выполнить необходимые требования согласно выбранным вариантам утверждения и получить «Зеленый» статус SSPA (соответствие требованиям).

**Важно:** специалисты программы SSPA не имеют полномочий на продление сроков для этой задачи.

Уполномоченные представители, которые будут проходить самостоятельную аттестацию, должны получить достаточную информацию от экспертов в соответствующих областях, чтобы

уверенно дать ответ на каждое требование. Кроме того, указывая свое имя в форме SSPA, они подтверждают прочтение и понимание требований по защите данных. Поставщики могут в любое время добавить в веб-инструмент других контактных лиц, которые помогут им выполнить требования.

Уполномоченный представитель (см. определение в DPR) обязан:

1. Определить применимые требования;
2. Предоставить ответ на каждое применимое требование;
3. Подписать и отправить свидетельство об аттестации на портале соответствия поставщиков Майкрософт (Supplier Compliance Portal).

## Применимость

Поставщики должны дать ответ на все применимые требования DPR, предъявленные в соответствии с профилем обработки данных. Некоторые из этих требований могут не применяться к товарам или услугам, которые поставщик предоставляет корпорации Майкрософт. Такие требования могут быть помечены как «неприменимые» с подробным комментарием, который будет проверен специалистами программы SSPA.

Специалисты проверяют все выбранные варианты «неприменимо», «конфликт с местным законодательством» и «контрактный конфликт» для предъявленных требований в свидетельстве о соответствии DPR. Специалисты программы SSPA могут попросить уточнить какие-то из выбранных вариантов. Конфликты с местным законодательством и контрактные конфликты принимаются только при предоставлении справочных материалов, подтверждающих факт конфликта.

## Требования к независимой аттестации

Утверждения для обработки данных, которые приводят к появлению этого требования, описаны в разделе «Требования для вариантов утверждения» в Приложении A.

У поставщиков есть возможность изменить утверждения путем обновления своего профиля обработки данных. Однако, если поставщик является Дополнительным обработчиком данных, он не может изменить это разрешение и будет обязан ежегодно проводить независимую оценку.

Чтобы пройти утверждение, для которого требуется независимая проверка соответствия требованиям, поставщику необходимо выбрать независимого аудитора, который выполнит проверку на соответствие DPR. Аудитор должен подготовить письмо с заключением о соответствии требованиям для корпорации Майкрософт. Заключение должно быть безусловно положительным. Необходимо разрешить и устранить все проблемы, связанные с несоответствием требованиям, а затем отправить письмо на портале соответствия поставщиков Майкрософт для последующей оценки специалистами программы SSPA. Аудиторы могут

загрузить шаблон утвержденного консультативного письма, который прилагается к PDF-файлу "Предпочтительные аудиторы", доступному здесь.

**В Приложении А** приведены допустимые альтернативные варианты сертификации, если вы решили не использовать независимого аудитора для проверки соответствия требованиям DPR (в тех случаях, когда это применимо, например, для поставщиков SaaS, хостинга веб-сайтов или поставщиков с субподрядчиками). Стандарты ISO 27701 (конфиденциальность) и ISO 27001 (безопасность) основаны на обеспечении четкого соответствия требованиям по защите данных (DPR).

Если поставщик является поставщиком медицинских услуг в США или попадающей под их юрисдикцию организацией, мы примем отчет HITRUST для обеспечения конфиденциальности и безопасности.

SSPA может провести независимую оценку вручную, если обстоятельства, выходящие за рамки стандартных определений, требуют дополнительной проверки. В качестве примера можно привести запрос от отдела конфиденциальности или безопасности; проверку устранения последствий инцидентов с данными; или требование автоматического выполнения прав субъектов данных.

**Инструкции по выполнению этого требования:**

1. Аттестация выполняется аудитором, имеющим достаточный уровень технической подготовки и знаний предметной области для вынесения компетентной оценки по соответствию.
2. Аудиторы должны быть членами Международной федерации бухгалтеров (International Federation of Accountants, IFAC) или Американского института дипломированных общественных бухгалтеров (American Institute of Certified Public Accountants, AICPA) либо должны иметь сертификаты других организаций подобного типа по обеспечению безопасности и конфиденциальности, таких как Международная ассоциация специалистов в области защиты информации (International Association of Privacy Professionals, IAPP) или Ассоциация аудита и контроля информационных систем (Information Systems Audit and Control Association, (ISACA).
3. Аудитор должен использовать актуальную версию DPR, где указаны все нужные свидетельства для проверки каждого требования. **Поставщикам нужно будет предоставить аудитору свои последние утвержденные ответы по аттестации на соответствие требованиям DPR.**
4. Если поставщик зарегистрировался недавно, аудитор проверит структуру средств контроля обработки. Во всех остальных случаях аудитор проверит эффективность этих средств.
5. Аттестация распространяется только на персональные или конфиденциальные данные Майкрософт, обрабатываемые поставщиком в связи с осуществляемой им деятельностью.
6. Область деятельности ограничена всеми действиями по обработке данных, выполняемыми под номером учётной записи поставщика,

получившего запрос. Если поставщик хочет провести аттестацию множества учетных записей поставщиков за раз, то **в заключении об аттестации необходимо указать список учетных записей поставщиков, включенных в аттестацию, и соответствующие адреса**.

7. В заключении об аттестации, отправляемом специалистам SSPA, не должно быть никаких положений, согласно которым поставщик не может выполнить требования по защите данных в том виде, в котором они записаны. Проблемы с выполнением этих требований должны быть устранены перед отправкой заключения.

Для программы SSPA существует список предпочтительных аудиторов, который доступен на этой странице. Эти организации хорошо знакомы с процедурой проведения аттестации SSPA. Поставщики должны оплатить эту аттестацию. Ее стоимость зависит от объема и области обработки данных.

# Требование к сертификации PCI DSS

Стандарт безопасности данных индустрии платежных карт (PCI DSS) — это платформа для разработки надежного механизма защиты данных платежных карт, который включает предотвращение, обнаружение и устранение последствий нарушений безопасности. Платформа была разработана самоуправляемой отраслевой организацией «Совет по стандартам безопасности данных индустрии платежных карт». Цель требований PCI DSS — найти уязвимости в технологиях и процессах, которые подвергают риску безопасность обрабатываемых данных владельцев карт.

Корпорация Майкрософт обязана соблюдать требования этих стандартов. Мы требуем подтверждения соблюдения этих стандартов у всех поставщиков, которые обрабатывают данные платежных карт от имени Майкрософт. За дополнительными сведениями о требованиях, устанавливаемых организацией PCI, обратитесь в Совет по стандартам безопасности данных индустрии платежных карт.

В зависимости от объема обрабатываемых транзакций проверка соответствия должна будет проводиться независимым аудитором либо поставщиком самостоятельно с заполнением формы самостоятельной аттестации.

Различные бренды платежных карт обычно устанавливают ограничения для разных типов аттестации.

- Уровень 1: предоставьте сертификат PCI DSS стороннего аудитора.
- Уровень 2 или 3: предоставьте анкету по самостоятельной аттестации на соответствие PCI DSS, подписанную должностным лицом поставщика.

Отправьте применимый сертификат, соответствующий требованиям PCI.

# Требование для программного обеспечения как услуги (SaaS)

Поставщики, которые подпадают под определения SaaS и отображаются в профиле обработки данных, могут быть обязаны предоставить действующую сертификацию ISO 27001, если это предусмотрено условиями договора облачных услуг Майкрософт (Microsoft Cloud Service Agreement).

Специалисты SSPA проведут проверку на соответствие вашей заявки контрактным обязательствам.

Обратите внимание, что SSPA больше не требуется сертификация сторонних центров обработки данных — мы ожидаем, что сертификация программного обеспечения в соответствии с ISO 27001 будет предоставлена Майкрософт и указана в вашем контракте с Майкрософт.

# Использование субподрядчиков

Корпорация Майкрософт считает использование субподрядчиков фактором высокого риска.

Поставщики, использующие субподрядчиков, которые будут обрабатывать персональные данные и (или) конфиденциальные данные Майкрософт, должны уведомить об этих субподрядчиках. Кроме того, поставщик должен сообщить страны, в которых персональные данные будут обрабатываться каждым субподрядчиком.

# Нарушения при обработке данных

Если поставщику становится известно о нарушении конфиденциальности или безопасности данных, поставщик обязан уведомить корпорацию Майкрософт об этом в соответствии с требованиями, которые указаны DPR.

В случае нарушения обработки данных, вы обязаны сообщить об этом используя SupplierWeb или посредством электронного письма, отправив его на адрес SuppIR@microsoft.com.

Обязательно включите в сообщение следующую информацию:

- Дата нарушения конфиденциальности или безопасности данных:
- Название поставщика:
- Номер поставщика:
- Оповещаемые контактные лица Майкрософт:
- Связанный номер заказа на поставку, если применимо/доступно:
- Сводное описание нарушения при обработке данных:

# Приложение A

## Требования на основе утверждений профиля

| # | Профиль | Требования к обеспечению соответствия | Варианты независимой проверки соответствия |
|---|---|---|---|
| 1 | **Область**: персональные и конфиденциальные данные<br>**Расположение обработки:** в корпорации Майкрософт или у клиента<br>**Роль обработки:** обработчик данных или управляющий данными<br>**Класс данных:** конфиденциальные **или** строго конфиденциальные<br>**Платежные карты:** неприменимо<br>**SaaS:** неприменимо<br>**Использование субподрядчиков:** неприменимо<br>**Хостинг веб-сайтов:** неприменимо | Самостоятельная аттестация на соответствие DPR | |
| 2 | **Область**: конфиденциальные данные<br>**Место обработки:** у поставщика<br>**Роль обработки:** неприменимо<br>**Класс данных:** конфиденциально<br>**Платежные карты:** неприменимо<br>**SaaS:** неприменимо<br>**Использование субподрядчиков:** неприменимо<br>**Хостинг веб-сайтов:** неприменимо | Самостоятельная аттестация на соответствие DPR | |

| # | Профиль | Требования к обеспечению соответствия | Варианты независимой проверки соответствия |
|---|---|---|---|
| 3 | **Область**: конфиденциальные данные<br>**Место обработки:** у поставщика<br>**Роль обработки:** обработчик данных<br>**Класс данных:** строго конфиденциально<br>**Платежные карты:** неприменимо<br>**SaaS:** неприменимо<br>**Использование субподрядчиков:** неприменимо<br>**Хостинг веб-сайтов:** неприменимо | Самостоятельная аттестация на соответствие DPR<br>**и**<br>независимая проверка соответствия требованиям | Варианты независимой проверки соответствия:<br>1. Независимая аттестация на соответствие DPR<br>**или**<br>2. Сертификация ISO 27001 |
| 4 | **Область:** персональные и конфиденциальные данные<br>**Место обработки:** у поставщика<br>**Роль обработки:** обработчик данных<br>**Класс данных:** строго конфиденциально<br>**Платежные карты:** неприменимо<br>**SaaS:** неприменимо<br>**Использование субподрядчиков:** неприменимо<br>**Хостинг веб-сайтов:** неприменимо | Самостоятельная аттестация на соответствие DPR<br>**и**<br>независимая проверка соответствия требованиям | Варианты независимой проверки соответствия:<br>1. Независимая аттестация на соответствие DPR,<br>2. Независимая аттестация в соответствии с секциями A-I требований DPR и ISO 27001,<br>**или**<br>3. Сертификация ISO 27701 **и** ISO 27001 |

| # | Профиль | Требования к обеспечению соответствия | Варианты независимой проверки соответствия |
|---|---|---|---|
| 5 | **Область**: персональные и конфиденциальные данные<br>**Место обработки:** у поставщика<br>**Роль обработки:** обработчик данных<br>**Класс данных:** конфиденциально<br>**Платежные карты:** неприменимо<br>**SaaS:** неприменимо<br>**Использование субподрядчиков:** неприменимо<br>**Хостинг веб-сайтов:** неприменимо | Самостоятельная аттестация на соответствие DPR | |
| 6 | **Область**: персональные и конфиденциальные данные<br>**Место обработки:** у поставщика<br>**Роль обработки:** управляющий данными<br>**Класс данных:** строго конфиденциальные или конфиденциальные<br>**Платежные карты:** неприменимо<br>**SaaS:** неприменимо<br>**Использование субподрядчиков:** неприменимо<br>**Хостинг веб-сайтов:** неприменимо | Самостоятельная аттестация на соответствие DPR | |

| # | Профиль | Требования к обеспечению соответствия | Варианты независимой проверки соответствия |
|---|---|---|---|
| 7 | **Область:** персональные и конфиденциальные данные<br><br>**Место обработки:** Любое<br><br>**Роль обработки:** Дополнительный обработчик данных (Эта роль определяется корпорацией Майкрософт - в профиле будет написано "Утверждение дополнительного обработчика данных: Да")<br><br>**Класс данных:** строго конфиденциальные или конфиденциальные<br>**Платежные карты:** неприменимо<br><br>**SaaS:** неприменимо<br><br>**Использование субподрядчиков:** неприменимо<br><br>**Хостинг веб-сайтов:** неприменимо | Самостоятельная аттестация на соответствие DPR **и** независимая проверка соответствия требованиям | Варианты независимой проверки соответствия:<br><br>1. Независимая аттестация на соответствие DPR,<br><br>2. Независимая аттестация в соответствии с секциями A-I требований DPR и ISO 27001,<br>**или**<br>3. Сертификация ISO 27701 **и** ISO 27001 |

| # | Профиль | Требования к обеспечению соответствия | Варианты независимой проверки соответствия: |
|---|---|---|---|
| Изменения при добавлении вариантов «Программное обеспечение как услуга», «Субподрядчики», «Хостинг веб- сайтов» | | | |
| 8 | **Область:** персональные и конфиденциальные данные<br>**Место обработки:** у поставщика<br>**Роль обработки:** обработчик данных<br>**Класс данных:** строго конфиденциальные или конфиденциальные<br>**Платежные карты:** неприменимо<br>**Субподрядчики:** да или<br>**SaaS:** Да или<br>**Хостинг веб-сайтов:** Да | Самостоятельная аттестация на соответствие DPR **и** независимая проверка соответствия требованиям | Варианты независимой проверки соответствия:<br>1. Независимая аттестация на соответствие DPR,<br>2. Независимая аттестация в соответствии с секциями A-I требований DPR и ISO 27001, **или**<br>3. Сертификация ISO 27701 **и** ISO 27001 |
| 9 | **Область:** персональные и конфиденциальные данные<br>**Место обработки:** у поставщика<br>**Роль обработки** управляющий данными<br>**Класс данных:** строго конфиденциальные или конфиденциальные<br>**Платежные карты:** неприменимо<br>**Субподрядчики:** Да или<br>**SaaS:** Да или<br>**Хостинг веб-сайтов:** Да | Самостоятельная аттестация на соответствие DPR | |

| # | Профиль | Требования к обеспечению соответствия | Варианты независимой проверки соответствия: |
|---|---|---|---|
| Дополнительная проверка соответствия для вариантов «Платежные карты» и «ПО как услуга» | | | |
| 10 | Любой из профилей выше и **«Платежные карты»** | Применимые требования выше **и** проверка соответствия для индустрии платежных карт | Сертификация PCI DSS |
| 11 | Любой из профилей выше и **SaaS** | Вышеуказанные требования **и** сертификация ISO 27001 с описанием функциональных служб в соответствии с требованиями контракта. | Сертификация ISO 27001 с описанием функций предоставляемых служб. |