Bộ phận Mua hàng của Microsoft

Hướng dẫn Chương trình Đảm bảo Quyền riêng tư và Bảo mật cho Nhà cung cấp (SSPA)

Phiên bản 8

Tháng 6/2022

Giới thiệu

Tại Microsoft, chúng tôi tin rằng quyền riêng tư là một quyền cơ bản. Với sứ mệnh trao quyền cho mọi cá nhân và tổ chức trên hành tinh đạt được nhiều thành tựu hơn nữa, chúng tôi luôn nỗ lực giành được và duy trì sự tin tưởng của khách hàng mỗi ngày.

Các biện pháp thực hành về quyền riêng tư và bảo mật mạnh mẽ có ý nghĩa rất quan trọng đối với sứ mệnh của chúng tôi và là điều cần thiết để giành được sự tin tưởng của khách hàng và để tuân thủ yêu cầu pháp luật ở một số khu vực pháp lý. Các tiêu chuẩn được ghi nhận trong chính sách quyền riêng tư và bảo mật của Microsoft phản ánh các giá trị của chúng tôi với tư cách là một doanh nghiệp và những tiêu chuẩn này được mở rộng để áp dụng cho các nhà cung cấp (chẳng hạn như công ty của bạn) xử lý dữ liệu Microsoft thay mặt chúng tôi.

Chương trình Đảm bảo Quyền riêng tư và Bảo mật cho Nhà cung cấp ("**SSPA**") là chương trình công ty của Microsoft nhằm cung cấp các hướng dẫn xử lý dữ liệu cơ bản của Microsoft cho các nhà cung cấp, dưới dạng Yêu cầu bảo vệ dữ liệu dành cho Nhà cung cấp ("**DPR**") của Microsoft, có sẵn trong phần SSPA trên Microsoft.com/Procurement. Vui lòng lưu ý rằng các nhà cung cấp có thể phải đáp ứng các yêu cầu bổ sung ở cấp tổ chức được nhóm Microsoft chịu trách nhiệm về việc thuê tuyển nhà cung cấp quyết định và thông báo bên ngoài SSPA.

Các thuật ngữ SSPA chính được định nghĩa trong DPR. Để tìm hiểu thêm về chương trình, hãy đọc phần Câu hỏi thường gặp (FAQ) và liên hệ với nhóm toàn cầu của chúng tôi bằng cách gửi email đến SSPAHelp@microsoft.com.

Tổng quan Chương trình SSPA

SSPA là chương trình đối tác giữa bộ phận Mua hàng, Đối ngoại và Pháp chế của Microsoft, cũng như bộ phận An ninh Doanh nghiệp để đảm bảo các nhà cung cấp của chúng tôi tuân thủ các nguyên tắc về quyền riêng tư và bảo mật.

Phạm vi áp dụng SSPA bao gồm tất cả các nhà cung cấp toàn cầu tham gia xử lý Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft liên quan đến hoạt động của nhà cung cấp đó (ví dụ: cung cấp các dịch vụ, giấy phép phần mềm, dịch vụ đám mây) theo các điều khoản của hợp đồng với Microsoft (ví dụ: các điều khoản trong Đơn đặt hàng, thỏa thuận khung) ("**Thực hiện**","**Đang thực hiện**" hoặc "**Việc thực hiện**").

SSPA cho phép nhà cung cấp thực hiện các lựa chọn Hồ sơ xử lý dữ liệu phù hợp với hàng hóa và/hoặc dịch vụ mà bạn ký hợp đồng cung cấp. Các lựa chọn này sẽ kích hoạt các yêu cầu tương ứng để cung cấp yêu cầu đảm bảo tuân thủ cho Microsoft.

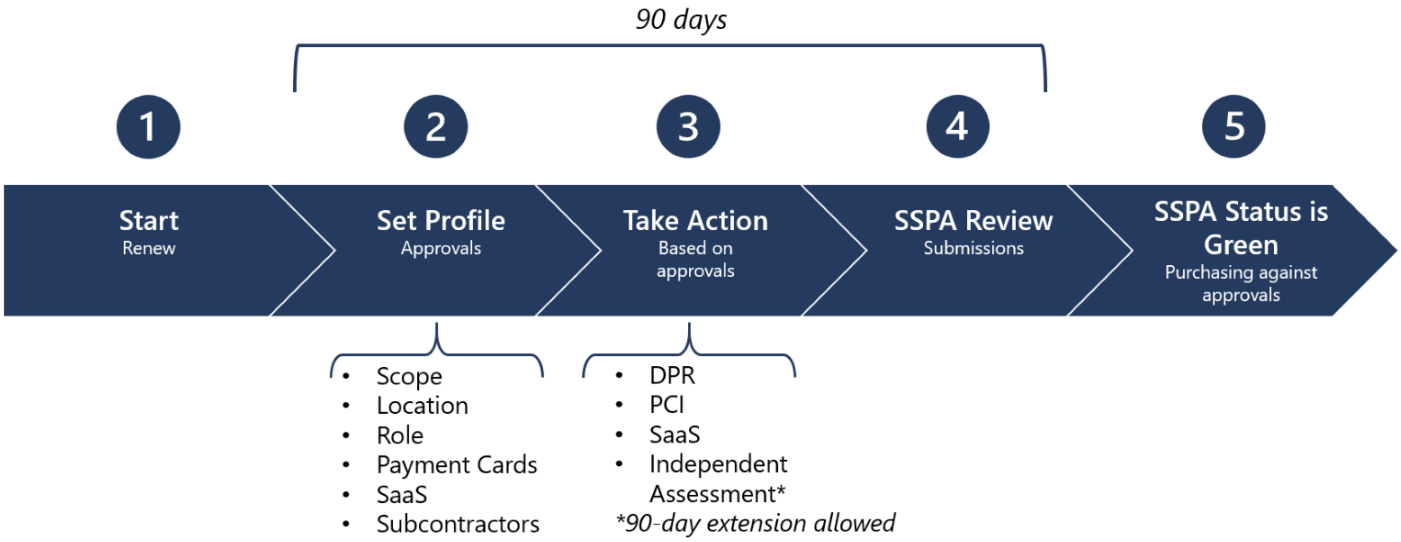
Tất cả các nhà cung cấp đã đăng ký sẽ hoàn thành tự chứng thực việc tuân thủ DPR hằng năm. Hồ sơ xử lý dữ liệu của bạn xác định xem có cần phát hành DPR đầy đủ hay là áp dụng một tập hợp con các yêu cầu. Các nhà cung cấp xử lý dữ liệu mà Microsoft cho là có rủi ro cao hơn cũng có thể cần đáp ứng các yêu cầu bổ sung, chẳng hạn như cung cấp xác minh độc lập về việc tuân thủ. Các nhà

cung cấp nằm trong danh sách Bên xử lý phụ của Microsoft đã liệt kê cũng sẽ được yêu cầu cung cấp xác minh độc lập về việc tuân thủ.

Quan trọng: Các hoạt động tuân thủ xác định trạng thái SSPA là Xanh (tuân thủ) hoặc Đỏ (không tuân thủ). Các công cụ mua hàng của Microsoft xác thực trạng thái SSPA là Xanh (cho từng nhà cung cấp trong phạm vi SSPA) trước khi cho phép tiếp tục quy trình thuê tuyển.

Sơ đồ Quy trình SSPA– Đăng ký Nhà cung cấp mới

Sơ đồ Quy trình SSPA – Gia hạn Nhà cung cấp hằng năm



Phạm vi áp dụng SSPA

Để giúp xác định xem bạn (nhà cung cấp) có xử lý Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft hay không, vui lòng xem danh sách các ví dụ trong bảng bên dưới. Hãy lưu ý rằng đây chỉ là ví dụ và không phải là một danh sách đầy đủ.
Lưu ý: Một đơn vị doanh nghiệp Microsoft có thể yêu cầu đăng ký theo các tiêu chí ngoài danh sách này và có xem xét tính chất bí mật của dữ liệu được xử lý.

Dữ liệu cá nhân theo Loại dữ liệu

Các ví dụ bao gồm nhưng không giới hạn ở:

Dữ liệu nhạy cảm
Dữ liệu liên quan đến trẻ em
Dữ liệu di truyền, Dữ liệu sinh trắc hoặc Dữ liệu y tế
Nguồn gốc chủng tộc hoặc sắc tộc
Niềm tin, quan điểm và đảng phái chính trị, tôn giáo hoặc triết học
Tư cách thành viên công đoàn
Đời sống tình dục hoặc khuynh hướng tính dục của một thể nhân
Tình trạng nhập cư (thị thực; giấy phép làm việc, v.v.)
Mã số định danh do Chính phủ cấp (hộ chiếu; bằng lái xe; thị thực; số an sinh xã hội; mã định danh quốc gia)
Dữ liệu vị trí người dùng chính xác (trong vòng 300 mét)
Số tài khoản ngân hàng cá nhân
Số thẻ tín dụng và ngày hết hạn
Dữ liệu nội dung của Khách hàng
Tài liệu, ảnh, video, nhạc, v.v.
Đánh giá và/hoặc xếp hạng được nhập vào một sản phẩm hoặc dịch vụ
Các câu trả lời khảo sát
Lịch sử duyệt web, sở thích và mục yêu thích
Viết, nhập và phát giọng nói (thoại/âm thanh và/hoặc trò chuyện/bot)
Dữ liệu thông tin xác thực (mật khẩu, gợi ý mật khẩu, tên người dùng, dữ liệu sinh trắc được sử dụng để nhận dạng)
Dữ liệu khách hàng liên kết với một trường hợp hỗ trợ

Dữ liệu thu thập được và tạo ra
Dữ liệu vị trí tương đối
Địa chỉ IP
Các tùy chọn và cá nhân hóa của thiết bị
Lịch sử sử dụng dịch vụ cho các trang web, theo dõi lần nhấp vào trang web
Dữ liệu mạng xã hội, mối quan hệ biểu đồ xã hội
Dữ liệu hoạt động từ các thiết bị được kết nối như vòng đeo tay thông minh
Dữ liệu liên hệ như họ tên, địa chỉ, số điện thoại, địa chỉ email, ngày sinh, người phụ thuộc và các liên hệ trong trường hợp khẩn cấp
Đánh giá gian lận và rủi ro, kiểm tra lý lịch
Chi tiết về bảo hiểm, lương hưu, quyền lợi
Sơ yếu lý lịch, ghi chép phỏng vấn/phản hồi cho ứng viên
Metadata and telemetry
Dữ liệu tài khoản
Dữ liệu công cụ thanh toán
Số thẻ tín dụng và ngày hết hạn
Thông tin định tuyến ngân hàng
Số tài khoản ngân hàng
Yêu cầu tín dụng hoặc hạn mức tín dụng
Chứng từ thuế và mã định danh
Dữ liệu đầu tư hoặc chi phí
Thẻ công ty
Thông tin biệt danh của Người dùng cuối (EUPI) (Mã định danh do Microsoft tạo để xác định người dùng các sản phẩm và dịch vụ của Microsoft)
Mã định danh duy nhất trên toàn cầu (GUID)
ID người dùng hoặc ID duy nhất theo hộ chiếu (PUID)
Thông tin nhận dạng người dùng cuối đã băm (EUII)
ID phiên truy cập
ID thiết bị
Dữ liệu chẩn đoán
Dữ liệu nhật ký

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

Dữ liệu mật của Microsoft theo Loại dữ liệu

Các ví dụ bao gồm nhưng không giới hạn ở:

Tuyệt mật
Thông tin về hoặc liên quan đến việc phát triển, thử nghiệm hoặc sản xuất Sản phẩm của Microsoft hoặc các thành phần của Sản phẩm Microsoft *Phần mềm, dịch vụ trực tuyến hoặc phần cứng của Microsoft được bán thương mại trên bất kỳ kênh nào đều được coi là "**Sản phẩm của Microsoft**"*
Thông tin tiếp thị trước khi ra mắt thiết bị của Microsoft
Dữ liệu tài chính doanh nghiệp không công khai của Microsoft tuân theo các quy tắc của SEC
Mật
Mã giấy phép sản phẩm của Microsoft được phân phối thay cho Microsoft qua bất kỳ phương thức nào
Thông tin về hoặc liên quan đến việc phát triển hoặc thử nghiệm các Lĩnh vực kinh doanh (LOB) nội bộ của Microsoft
Tài liệu tiếp thị trước khi ra mắt phần mềm và dịch vụ của Microsoft như Office, SQL, Azure, v.v.
Tài liệu ở dạng viết, thiết kế, điện tử hoặc in cho bất kỳ dịch vụ hoặc sản phẩm nào của Microsoft, chẳng hạn như thiết bị (hướng dẫn quy trình hoặc thủ tục, dữ liệu cấu hình, v.v.)

Quan trọng: Một đơn vị doanh nghiệp Microsoft có thể yêu cầu áp dụng cả những dữ liệu không có trong danh sách này.

Hồ sơ xử lý dữ liệu

Các nhà cung cấp của Microsoft có quyền kiểm soát Hồ sơ xử lý dữ liệu SSPA của họ.

Quyền này cho phép các nhà cung cấp quyết định những dịch vụ/sản phẩm thuê tuyển mà họ muốn đủ điều kiện cung cấp. Hãy đặc biệt lưu ý đến các lựa chọn và xem xét hoạt động tuân thủ cần phải hoàn thành để được phê duyệt. **Xem Phần "Yêu cầu đảm bảo" bên dưới và Phụ lục A.**

Các đơn vị kinh doanh của Microsoft sẽ chỉ có thể thuê tuyển các nhà cung cấp khi hoạt động xử lý dữ liệu khớp với các phê duyệt cấp cho nhà cung cấp đó.

Các nhà cung cấp sẽ có thể cập nhật Hồ sơ xử lý dữ liệu của họ bất kỳ lúc nào trong năm nếu **không có nhiệm vụ nào đang thực hiện**. Khi có thay đổi, hoạt động tương ứng sẽ được xác định và phải được hoàn thành trước khi các phê duyệt được cấp. Các phê duyệt hiện có, đã hoàn thành sẽ được áp dụng cho đến khi hoàn thành các yêu cầu mới đưa ra.

Nếu không hoàn thành các tác vụ mới đưa ra trong khung thời gian 90 ngày cho phép, trạng thái SSPA sẽ chuyển sang Đỏ (không tuân thủ) và tài khoản có nguy cơ bị vô hiệu hóa khỏi hệ thống Microsoft Accounts Payable.

Phê duyệt xử lý dữ liệu	
1	Phạm vi xử lý dữ liệu ▪ Mật ▪ Cá nhân, Mật
2	Địa điểm xử lý dữ liệu ▪ Tại địa điểm của Microsoft hoặc Khách hàng ▪ Tại địa điểm của Nhà cung cấp
3	Vai trò xử lý dữ liệu ▪ Bên quản lý (Bên quản lý độc lập hoặc Bên quản lý chung) ▪ Bên xử lý ▪ Bên xử lý phụ (Do Microsoft chỉ định)
4	Xử lý thẻ thanh toán ▪ Có ▪ Không áp dụng
5	Phần mềm dạng dịch vụ ▪ Có ▪ Không áp dụng
6	Sử dụng Nhà thầu phụ ▪ Có ▪ Không áp dụng

Những vấn đề cần lưu ý khi phê duyệt

Phạm vi xử lý dữ liệu

Mật

Chọn phê duyệt này nếu Việc thực hiện của nhà cung cấp sẽ chỉ liên quan đến việc xử lý Dữ liệu mật của Microsoft.

Nếu bạn chọn phê duyệt này, bạn sẽ không đủ điều kiện tham gia các hoạt động xử lý Dữ liệu cá nhân.

Cá nhân, Mật

Chọn phê duyệt này nếu Việc thực hiện của nhà cung cấp sẽ bao gồm xử lý Dữ liệu cá nhân và Dữ liệu mật của Microsoft.

Địa điểm xử lý

Tại địa điểm của Microsoft hoặc Khách hàng

Chọn phê duyệt này nếu Việc thực hiện của nhà cung cấp bao gồm Xử lý dữ liệu của nhà cung cấp trong môi trường mạng Microsoft nơi nhân viên sử dụng thông tin đăng nhập *@microsoft.com* hoặc trong môi trường khách của Microsoft.

Không chọn tùy chọn này trong những trường hợp sau:

- Nhà cung cấp quản lý một cơ sở ở nước ngoài (OF) do Microsoft chỉ định.
- Nhà cung cấp cung cấp các loại tài nguyên cho Microsoft và làm việc trên và bên ngoài mạng của Microsoft. Địa điểm xử lý ở ngoài mạng được coi là "tại địa điểm của nhà cung cấp".

Tại địa điểm của Nhà cung cấp
Nếu điều kiện "Tại địa điểm của Microsoft hoặc Khách hàng" (như mô tả ở trên) không áp dụng, hãy lựa chọn tùy chọn này.

Vai trò xử lý dữ liệu

Bên quản lý (bao gồm các bên quản lý chung và độc lập)

Chọn phê duyệt này nếu **tất cả** các khía cạnh trong Việc thực hiện của nhà cung cấp đáp ứng định nghĩa vai trò xử lý dữ liệu của Bên quản lý (xem DPR).

Nếu bạn chọn phê duyệt này, bạn sẽ không đủ điều kiện xử lý Dữ liệu cá nhân với chỉ định vai trò là "Bên xử lý". Nếu nhà cung cấp vừa là Bên xử lý vừa là Bên quản lý cho Microsoft, không chọn "Bên quản lý" và thay vào đó, hãy chọn Người xử lý.

Bên xử lý

Đây là vai trò xử lý phổ biến nhất của nhà cung cấp xử lý Dữ liệu thay cho Microsoft. Vui lòng xem lại định nghĩa về Bên xử lý trong DPR.

Bên xử lý phụ

Bên xử lý phụ có nghĩa là bên thứ ba mà Microsoft thuê tuyển để Thực hiện, trong đó Việc thực hiện bao gồm xử lý Dữ liệu cá nhân của Microsoft mà Microsoft là Bên xử lý. Các nhà cung cấp không thể tự xác định mình là Bên xử lý phụ tại địa điểm của Microsoft vì việc này cần có sự phê duyệt trước của các nhóm phụ trách Quyền riêng tư nội bộ. Nhà cung cấp chỉ có thể là Bên xử lý phụ khi Microsoft là Bên xử lý dữ liệu và nhà cung cấp xử lý các Loại dữ liệu cá nhân cho doanh nghiệp đủ điều kiện. Các bên xử lý phụ sẽ phải đáp ứng các yêu cầu về hợp đồng và tuân thủ bổ sung, bao gồm Phụ lục Bảo vệ dữ liệu và Đánh giá độc lập (xem bên dưới).

Xử lý thẻ thanh toán

Lựa chọn phê duyệt này nếu bất kỳ phần nào của dữ liệu do nhà cung cấp Xử lý bao gồm dữ liệu để hỗ trợ quá trình xử lý thẻ tín dụng hoặc thẻ thanh toán khác thay cho Microsoft.

Phê duyệt này cho phép một nhà cung cấp tham gia các hoạt động xử lý thẻ thanh toán.

_____

Phần mềm

Bộ phận Mua hàng của Microsoft định hướng Người mua thông qua một quy trình tiếp nhận cho mọi giao dịch mua phần mềm. Quy trình này bao gồm các bài kiểm tra khác nhau, trong đó có phân loại SSPA để quyết định xem nhà cung cấp của phần mềm đó có thuộc trong phạm vi quản lý theo SSPA hay không. (Người mua của Microsoft có thể tham khảo các bước được nêu trên trang Dịch vụ đám mây và Phần mềm ProcureWeb nội bộ để biết thêm chi tiết). Nếu bắt buộc phải áp dụng SSPA, các nhà cung cấp cũng có thể cần xác định tùy chọn cấu hình 'Phần mềm dạng dịch vụ' (SaaS) có áp dụng hay không. Đối với các nhà cung cấp đã đăng ký SSPA, mục này có thể được thực hiện khi hoàn thành Hồ sơ xử lý dữ liệu trong Cổng tuân thủ dành cho Nhà cung cấp của Microsoft.

Vì mục đích tuân thủ SSPA, hãy xem xét SaaS theo nghĩa rộng để bao gồm cả nền tảng dạng dịch vụ (PaaS) và cơ sở hạ tầng dạng dịch vụ (IaaS). (Để tìm hiểu thêm về SaaS, vui lòng xem phần giải thích này.)

Phần mềm dạng dịch vụ (SaaS)

Phần mềm dạng dịch vụ (SaaS) cho phép người dùng kết nối và sử dụng các ứng dụng trên đám mây qua Internet.

Microsoft định nghĩa **Phần mềm dạng dịch vụ (SaaS)** là phần mềm dựa trên mã chung được sử dụng trong mô hình một dịch vụ liên kết với nhiều thiết bị, trả phí khi sử dụng hoặc dưới dạng gói đăng ký dựa trên số liệu sử dụng. Nhà cung cấp dịch vụ đám mây phát triển và duy trì phần mềm trên đám mây, cung cấp các bản cập nhật phần mềm tự động và cung cấp phần mềm cho khách hàng thông qua internet trên cơ sở một dịch vụ liên kết với nhiều thiết bị và trả phí khi sử dụng. Phương thức phân phối và cấp phép phần mềm này cho phép người dùng truy cập phần mềm trực tuyến thông qua gói đăng ký thay vì mua và cài đặt trên từng máy tính riêng lẻ.

Lưu ý: Hầu hết các nhà cung cấp SaaS sẽ cần thêm phê duyệt Nhà thầu phụ trong Cổng tuân thủ dành cho Nhà cung cấp của Microsoft nếu Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft được lưu trữ trên nền tảng của bên thứ ba.

Sử dụng Nhà thầu phụ

Chọn phê duyệt này nếu nhà cung cấp sử dụng Nhà thầu phụ để Thực hiện (xem DPR để biết định nghĩa).

Phần này cũng bao gồm Người làm việc tự do (xem DPR).

Yêu cầu Đảm bảo

Yêu cầu dựa trên Phê duyệt hồ sơ

Các phê duyệt được chọn trong Hồ sơ xử lý dữ liệu của bạn hỗ trợ SSPA đánh giá mức độ rủi ro cho các mối quan hệ thuê tuyển của bạn với Microsoft. Các yêu cầu tuân thủ SSPA sẽ khác nhau tùy từng Hồ sơ xử lý dữ liệu và các phê duyệt liên quan. Phần này giải thích các yêu cầu SSPA khác nhau.

Ngoài ra còn có những lựa chọn kết hợp có thể tăng hoặc giảm yêu cầu tuân thủ. Các lựa chọn kết hợp được ghi lại trong Phụ lục A và đây là những tình huống bạn có thể dự kiến Cổng tuân thủ dành cho Nhà cung cấp của Microsoft sẽ thực thi sau khi bạn hoàn thành hồ sơ của mình. Bạn luôn có thể xác nhận tình huống của mình phù hợp với khung này như thế nào bằng cách yêu cầu nhóm SSPA đánh giá lại.

Hành động: Tìm hồ sơ phê duyệt của bạn trong Phụ lục A và xem xét các yêu cầu đảm bảo tương ứng và các tùy chọn Đảm bảo độc lập, nếu có.

Quan trọng: Nếu hồ sơ của bạn bao gồm Phần mềm dạng dịch vụ (SaaS), Nhà thầu phụ, dịch vụ lưu trữ trang web hoặc thẻ thanh toán thì sẽ yêu cầu đảm bảo bổ sung.

Tự chứng thực với DPR

Tất cả nhà cung cấp đã đăng ký SSPA phải hoàn thành bản tự chứng thực việc tuân thủ DPR trong vòng 90 ngày kể từ ngày nhận được yêu cầu. Yêu cầu này sẽ được đưa ra hằng năm nhưng cũng có thể thường xuyên hơn nếu Hồ sơ xử lý dữ liệu được cập nhật vào giữa năm. Tài khoản của nhà cung cấp sẽ chuyển sang trạng thái SSPA Đỏ (không tuân thủ) nếu vượt quá khoảng thời gian 90 ngày. Các đơn hàng mới trong phạm vi áp dụng sẽ không xử lý được cho đến khi trạng thái SSPA chuyển sang Xanh (tuân thủ).

Các nhà cung cấp mới đăng ký phải hoàn thành các yêu cầu đã đưa ra để đảm bảo trạng thái SSPA Xanh (tuân thủ) trước khi bắt đầu các hoạt động thuê tuyển.

Quan trọng: Nhóm SSPA không được phép gia hạn thời gian cho nhiệm vụ này.

Các đại diện có thẩm quyền hoàn thành việc tự chứng thực phải đảm bảo họ có đầy đủ thông tin từ các chuyên gia để trả lời từng yêu cầu một cách tự tin. Ngoài ra, khi thêm tên của họ vào biểu mẫu SSPA, họ chứng nhận rằng họ đã đọc và hiểu rõ DPR này. Các nhà cung cấp có thể thêm các liên hệ khác vào công cụ trực tuyến để hỗ trợ hoàn thành các yêu cầu.

Đại diện được ủy quyền (xem DPR để biết định nghĩa), phải:

1. Xác định những yêu cầu nào được áp dụng.
2. Trả lời từng yêu cầu được áp dụng.
3. Ký tên và gửi chứng thực trong Cổng tuân thủ dành cho Nhà cung cấp của Microsoft.

Phạm vi áp dụng

Các nhà cung cấp phải đáp ứng tất cả yêu cầu DPR hiện hành được đưa ra dựa trên Hồ sơ xử lý dữ liệu. Trong các yêu cầu đã đưa ra, dự kiến một số yêu cầu có thể không áp dụng cho hàng hóa hoặc dịch vụ mà nhà cung cấp đó cung cấp cho Microsoft. Các yêu cầu này có thể được đánh dấu là "không áp dụng", cùng với một nhận xét chi tiết để người đánh giá SSPA xác nhận.

Thông tin được gửi theo DPR sẽ được nhóm SSPA xem xét để xác nhận các lựa chọn "không áp dụng", "xung đột với luật pháp địa phương" hoặc "xung đột với hợp đồng" so với các yêu cầu đã đưa ra. Nhóm SSPA có thể yêu cầu làm rõ một hoặc nhiều lựa chọn. Xung đột với luật pháp địa phương và hợp đồng chỉ được chấp nhận nếu cung cấp tài liệu tham khảo và xung đột có thể xác định rõ ràng.

Yêu cầu Đánh giá độc lập

Vui lòng xem Yêu cầu theo phê duyệt trong Phụ lục A để xem các phê duyệt xử lý dữ liệu kích hoạt yêu cầu này.

Các nhà cung cấp có thể thay đổi phê duyệt bằng cách cập nhật Hồ sơ xử lý dữ liệu của họ. Tuy nhiên, nếu nhà cung cấp có vai trò Xử lý dữ liệu là “Bên xử lý phụ” thì nhà cung cấp đó không thể thay đổi phê duyệt này và sẽ phải thực hiện Đánh giá độc lập hằng năm.

Để đảm bảo các phê duyệt yêu cầu xác minh độc lập về sự tuân thủ, các nhà cung cấp sẽ cần chọn một chuyên gia đánh giá độc lập để xác nhận việc tuân thủ theo DPR. Chuyên gia đánh giá phải lập thư tư vấn, cung cấp các đảm bảo tuân thủ cho Microsoft. Thư này phải không hạn chế và tất cả các vấn đề không tuân thủ phải được giải quyết và khắc phục trước khi thư xác nhận được gửi tới Cổng tuân thủ dành cho Nhà cung cấp của Microsoft để nhóm SSPA xem xét. Chuyên gia đánh giá có thể tải xuống mẫu thư tư vấn đã được phê duyệt, đính kèm bản PDF “Chuyên gia đánh giá ưu tiên” có sẵn tại đây.

Phụ lục A liệt kê các loại chứng nhận thay thế được chấp nhận nếu bạn chọn không sử dụng một chuyên gia đánh giá độc lập để xác minh sự tuân thủ theo DPR (nếu cần, chẳng hạn như đối với nhà cung cấp SaaS, nhà cung cấp dịch vụ lưu trữ trang web hoặc nhà cung cấp có Nhà thầu phụ). Các tiêu chuẩn ISO 27701 (quyền riêng tư) và ISO 27001 (bảo mật) được sử dụng để đối chiếu với các yêu cầu DPR.

Trong trường hợp Nhà cung cấp là nhà cung cấp dịch vụ y tế tại Hoa Kỳ hoặc pháp nhân liên quan, chúng tôi sẽ chấp nhận báo cáo HITRUST về phạm vi bảo mật và quyền riêng tư.

SSPA có thể tự tiến hành đánh giá độc lập nếu các trường hợp nằm ngoài các yếu tố kích hoạt tiêu chuẩn cần phải tiến hành thẩm định bổ sung. Ví dụ bao gồm yêu cầu từ bộ phận quyền riêng tư hoặc bảo mật; xác nhận việc khắc phục sự cố dữ liệu; hoặc yêu cầu tự động thực thi quyền của chủ thể dữ liệu.

Hướng dẫn về cách tiếp cận yêu cầu này:

1. Việc đánh giá phải do một chuyên gia đánh giá được đào tạo đầy đủ về kỹ thuật và kiến thức về chủ đề để đánh giá đầy đủ sự tuân thủ thực hiện.

2. Chuyên gia đánh giá phải là thành viên liên kết của Liên đoàn Kế toán Quốc tế (IFAC) hoặc Viện Kế toán Công chứng Hoa Kỳ (AICPA) hoặc phải có chứng chỉ từ các tổ chức bảo mật và quyền riêng tư liên quan khác, chẳng hạn như Hiệp hội Quốc tế về Quyền riêng tư (IAPP) hoặc Hiệp hội Kiểm tra và Kiểm soát Hệ thống Thông tin (ISACA).
3. Chuyên gia đánh giá phải sử dụng DPR mới nhất bao gồm các bằng chứng cần thiết để hỗ trợ từng yêu cầu. **Các nhà cung cấp sẽ cần xuất trình các phản hồi chứng thực DPR được phê duyệt gần đây nhất của họ cho chuyên gia đánh giá.**
4. Nếu là nhà cung cấp mới đăng ký, chuyên gia đánh giá sẽ kiểm tra thiết kế các biện pháp kiểm soát quá trình. Trong tất cả các trường hợp khác, chuyên gia đánh giá sẽ kiểm tra tính hiệu quả của các biện pháp kiểm soát.
5. Phạm vi đánh giá chỉ giới hạn trong Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft liên quan đến Việc thực hiện của nhà cung cấp đó.
6. Phạm vi thuê tuyển được giới hạn là tất cả hoạt động xử lý dữ liệu trong phạm vi được thực hiện theo số tài khoản nhà cung cấp đã nhận được yêu cầu. Nếu nhà cung cấp chọn mờ nhiều tài khoản nhà cung cấp cùng một lúc thì **thư chứng thực phải bao gồm danh sách các tài khoản của nhà cung cấp có trong bản đánh giá và các địa chỉ liên quan.**
7. Thư gửi cho SSPA không được bao gồm bất kỳ tuyên bố nào cho biết nhà cung cấp không thể đáp ứng Yêu cầu Bảo vệ dữ liệu theo quy định. Các vấn đề này phải được khắc phục trước khi gửi thư chứng thực này.

SSPA đã cung cấp sẵn một danh sách chuyên gia đánh giá ưu tiên. Các công ty này đã quen quy trình thực hiện đánh giá SSPA. Các nhà cung cấp phải trả tiền cho quy trình đánh giá này; chi phí sẽ thay đổi tùy theo quy mô và phạm vi xử lý dữ liệu.

Yêu cầu Chứng nhận PCI DSS

Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS) là một khuôn khổ để phát triển khả năng bảo mật dữ liệu thẻ thanh toán mạnh mẽ bao gồm ngăn chặn, phát hiện và phản ứng thích hợp trước các sự cố bảo mật. Khung này được xây dựng bởi Hội đồng Tiêu chuẩn Bảo mật PCI, một tổ chức ngành tự quản lý. Mục đích của các yêu cầu PCI DSS là xác định các lỗ hổng công nghệ và quy trình gây rủi ro bảo mật cho dữ liệu chủ thẻ được xử lý.

Microsoft được yêu cầu tuân thủ các tiêu chuẩn này. Nếu nhà cung cấp thay mặt Microsoft xử lý thông tin thẻ thanh toán, chúng tôi yêu cầu bằng chứng về việc tuân thủ các tiêu chuẩn này. Tham vấn Hội đồng Tiêu chuẩn Bảo mật PCI để hiểu các yêu cầu do tổ chức PCI đặt ra.

Tùy theo khối lượng giao dịch được xử lý, nhà cung cấp sẽ được yêu cầu phải thuê Chuyên gia Đánh giá Bảo mật đủ điều kiện chứng nhận sự tuân thủ hoặc có thể hoàn thành biểu mẫu bảng câu hỏi tự đánh giá.

Các thương hiệu thẻ thanh toán quy định ngưỡng cho loại đánh giá, thường là:

- Cấp 1: Cung cấp chứng chỉ PCI AOC của Chuyên gia đánh giá bên thứ 3
- Cấp 2 hoặc 3: Cung cấp Bảng câu hỏi tự đánh giá PCI DSS (SAQ) có chữ ký của nhân chức đại diện của nhà cung cấp.

Gửi chứng nhận áp dụng và đáp ứng các yêu cầu của PCI.

Yêu cầu Phần mềm dạng dịch vụ

Các nhà cung cấp đáp ứng định nghĩa SaaS có trong Hồ sơ xử lý dữ liệu có thể được yêu cầu cung cấp chứng chỉ ISO 27001 hợp lệ nếu chứng chỉ này được yêu cầu trong Thỏa thuận dịch vụ đám mây của Microsoft.

Người đánh giá SSPA sẽ xác nhận rằng nội dung bạn gửi đáp ứng nghĩa vụ hợp đồng.

Vui lòng không gửi chứng nhận trung tâm dữ liệu. Chúng tôi yêu cầu chứng nhận ISO 27001 áp dụng cho (các) dịch vụ phần mềm được ghi trong hợp đồng của bạn với Microsoft.

Sử dụng Nhà thầu phụ

Microsoft coi việc sử dụng các nhà thầu phụ là một yếu tố rủi ro cao. Các nhà cung cấp sử dụng nhà thầu phụ để xử lý Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft sẽ phải tiết lộ các nhà thầu phụ đó. Ngoài ra, nhà cung cấp cũng phải tiết lộ các quốc gia nơi dữ liệu cá nhân sẽ được xử lý bởi mỗi nhà thầu phụ.

Sự cố dữ liệu

Nếu nhà cung cấp biết về sự cố dữ liệu bảo mật hoặc quyền riêng tư thì phải thông báo cho Microsoft như được nêu chi tiết và quy định trong DPR.

Báo cáo sự cố dữ liệu qua SupplierWeb hoặc gửi email đến SuppIR@microsoft.com

Hãy ghi rõ:

- Ngày xảy ra Sự cố dữ liệu:
- Tên Nhà cung cấp:
- Mã số Nhà cung cấp:
- Đầu mối liên hệ được thông báo ở Microsoft:
- PO liên quan, nếu có:
- Tóm tắt Sự cố dữ liệu:

Phụ lục A

Yêu cầu dựa trên Phê duyệt hồ sơ

#	Hồ sơ	Yêu cầu Đảm bảo	Tùy chọn Đánh giá độc lập
1	**Phạm vi:** Cá nhân, Mật **Địa điểm xử lý:** Tại địa điểm của Microsoft hoặc Khách hàng **Vai trò xử lý:** Bên xử lý hoặc Bên quản lý **Loại dữ liệu:** Mật **hoặc** Tuyệt mật **Thẻ thanh toán:** Không áp dụng **SaaS:** Không áp dụng **Sử dụng Nhà thầu phụ:** Không áp dụng **Lưu trữ trang web:** Không áp dụng	Tự chứng thực việc tuân thủ DPR	
2	**Phạm vi:** Mật **Địa điểm xử lý:** Tại địa điểm của Nhà cung cấp **Vai trò xử lý:** Không áp dụng **Loại dữ liệu:** Mật **Thẻ thanh toán:** Không áp dụng **SaaS:** Không áp dụng **Sử dụng Nhà thầu phụ:** Không áp dụng **Lưu trữ trang web:** Không áp dụng	Tự chứng thực việc tuân thủ DPR	
3	**Phạm vi:** Mật **Địa điểm xử lý:** Tại địa điểm của Nhà cung cấp **Vai trò xử lý:** Bên xử lý **Loại dữ liệu:** Tuyệt mật **Thẻ thanh toán:** Không áp dụng **SaaS:** Không áp dụng **Sử dụng Nhà thầu phụ:** Không áp dụng **Lưu trữ trang web:** Không áp dụng	Tự chứng thực việc tuân thủ DPR **và** Đánh giá độc lập việc tuân thủ	Các tùy chọn Đánh giá độc lập: 1. Hoàn thành Đánh giá độc lập theo DPR, **hoặc** 2. Gửi chứng chỉ ISO 27001

#	Hồ sơ	Yêu cầu Đảm bảo	Tùy chọn Đánh giá độc lập
4	**Phạm vi:** Cá nhân, Mật **Địa điểm xử lý:** Tại địa điểm của Nhà cung cấp **Vai trò xử lý:** Bên xử lý **Loại dữ liệu:** Tuyệt mật **Thẻ thanh toán:** Không áp dụng **SaaS:** Không áp dụng **Sử dụng Nhà thầu phụ:** Không áp dụng **Lưu trữ trang web:** Không áp dụng	Tự chứng thực việc tuân thủ DPR **và** Đánh giá độc lập việc tuân thủ	Các tùy chọn Đánh giá độc lập: 1. Hoàn thành Đánh giá độc lập theo DPR, 2. Đánh giá độc lập theo phần A-I của DPR và ISO 27001, **hoặc** 3. Gửi chứng chỉ ISO 27701 **và** ISO 27001
5	**Phạm vi:** Cá nhân, Mật **Địa điểm xử lý:** Tại địa điểm của Nhà cung cấp **Vai trò xử lý:** Bên xử lý **Loại dữ liệu:** Mật **Thẻ thanh toán:** Không áp dụng **SaaS:** Không áp dụng **Sử dụng Nhà thầu phụ:** Không áp dụng **Lưu trữ trang web:** Không áp dụng	Tự chứng thực việc tuân thủ DPR	
6	**Phạm vi:** Cá nhân, Mật **Địa điểm xử lý:** Tại địa điểm của Nhà cung cấp **Vai trò xử lý:** Bên quản lý **Loại dữ liệu:** Tuyệt mật hoặc Mật **Thẻ thanh toán:** Không áp dụng **SaaS:** Không áp dụng **Sử dụng Nhà thầu phụ:** Không áp dụng **Lưu trữ trang web:** Không áp dụng	Tự chứng thực việc tuân thủ DPR	

#	Hồ sơ	Yêu cầu Đảm bảo	Tùy chọn Đánh giá độc lập
7	**Phạm vi:** Cá nhân, Mật **Địa điểm xử lý:** Bất kỳ **Vai trò xử lý:** Bên xử lý phụ (Vai trò này được xác định bởi Microsoft – hồ sơ sẽ là "Phê duyệt Bên xử lý phụ: Có") **Loại dữ liệu:** Tuyệt mật hoặc Mật **Thẻ thanh toán:** Không áp dụng **SaaS:** Không áp dụng **Sử dụng Nhà thầu phụ:** Không áp dụng **Lưu trữ trang web:** Không áp dụng	Tự chứng thực việc tuân thủ DPR **và** Đánh giá độc lập việc tuân thủ	Các tùy chọn Đánh giá độc lập: 1. Hoàn thành Đánh giá độc lập theo DPR, 2. Đánh giá độc lập theo phần A-I của DPR và ISO 27001, **hoặc** 3. Gửi chứng chỉ ISO 27701 **và** ISO 27001

#	Hồ sơ	Yêu cầu Đảm bảo	Tùy chọn Đánh giá độc lập
Tác động của việc thêm SaaS, Nhà thầu phụ, Dịch vụ lưu trữ trang web			
8	**Phạm vi:** Cá nhân, Mật **Địa điểm xử lý:** Tại địa điểm của Nhà cung cấp **Vai trò xử lý:** Bên xử lý **Loại dữ liệu:** Tuyệt mật hoặc Mật **Thẻ thanh toán:** Không áp dụng **Nhà thầu phụ:** CÓ hoặc **SaaS:** CÓ hoặc **Lưu trữ trang web:** CÓ	Tự chứng thực việc tuân thủ DPR **và** Đánh giá độc lập việc tuân thủ	Các tùy chọn Đánh giá độc lập: 1. Hoàn thành Đánh giá độc lập theo DPR, 2. Đánh giá độc lập theo phần A-I của DPR và ISO 27001, **hoặc** 3. Gửi chứng chỉ ISO 27701 **và** ISO 27001
9	**Phạm vi:** Cá nhân, Mật **Địa điểm xử lý:** Tại địa điểm của Nhà cung cấp **Vai trò xử lý:** Bên quản lý **Loại dữ liệu:** Tuyệt mật hoặc Mật **Thẻ thanh toán:** Không áp dụng **Nhà thầu phụ:** CÓ hoặc **SaaS:** CÓ hoặc **Lưu trữ trang web:** CÓ	Tự chứng thực việc tuân thủ DPR	

#	Hồ sơ	Yêu cầu Đảm bảo	Tùy chọn Đánh giá độc lập
Đảm bảo bổ sung cho Thẻ thanh toán và SaaS			
10	Bất kỳ hồ sơ nào ở trên và **Thẻ thanh toán**	Các yêu cầu trên được áp dụng **và** Đảm bảo ngành Thẻ thanh toán	Gửi Chứng nhận PCI DSS
11	Bất kỳ hồ sơ nào ở trên và **Phần mềm dạng dịch vụ (SaaS)**	Các yêu cầu trên được áp dụng **và** gửi chứng chỉ ISO 27001 bắt buộc theo hợp đồng của bạn bao gồm các dịch vụ chức năng.	Gửi chứng chỉ ISO 27001 với phạm vi chức năng của (các) dịch vụ được cung cấp.