Yêu cầu bảo vệ dữ liệu dành cho nhà cung cấp của Microsoft

Tính ứng dụng

Yêu cầu bảo vệ dữ liệu ("**DPR**") dành cho nhà cung cấp của Microsoft áp dụng cho mọi nhà cung cấp xử lý Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft liên quan đến việc thực hiện của nhà cung cấp (ví dụ: cung cấp dịch vụ, giấy phép phần mềm, dịch vụ đám mây) theo các điều khoản trong hợp đồng của họ với Microsoft (ví dụ: Điều khoản đặt mua hàng, hợp đồng chính) ("**Thực hiện,**" "**Đang thực hiện**" hoặc "**Việc thực hiện**").

- Trong trường hợp có xung đột giữa các yêu cầu có ở đây và các yêu cầu được quy định trong thỏa thuận hợp đồng giữa nhà cung cấp và Microsoft, thì Yêu cầu bảo vệ dữ liệu (DPR) sẽ được ưu tiên. Trừ khi trong mẫu đơn xác nhận Yêu cầu bảo vệ dữ liệu (DPR), nhà cung cấp khẳng định cung cấp đúng quy định trong hợp đồng xung đột với phần Yêu cầu bảo vệ dữ liệu (DPR) hiện hành (trong trường hợp đó, các điều khoản của hợp đồng được ưu tiên).
- Trong trường hợp có xung đột giữa các yêu cầu có ở đây và bất kỳ yêu cầu theo luật hoặc pháp lý nào thì các yêu cầu theo luật hoặc pháp lý đó sẽ được ưu tiên.
- Trong trường hợp nhà cung cấp của Microsoft là Bên kiểm soát, thì chỉ áp dụng các yêu cầu trong phần J Bảo mật và phần A Quản lý của Yêu cầu bảo vệ dữ liệu (DPR) này đối với các hoạt động Xử lý của nhà cung cấp đó.
- Trong trường hợp nhà cung cấp của Microsoft không Xử lý Dữ liệu cá nhân của Microsoft mà chỉ xử lý Dữ liệu bảo mật của Microsoft, thì chỉ áp dụng các yêu cầu trong phần A Quản lý, phần E Lưu giữ và phần J Bảo mật của Yêu cầu bảo vệ dữ liệu (DPR) này đối với việc Xử lý của nhà cung cấp đó cho Dữ liệu mật của Microsoft.

Chuyển dữ liệu trên phạm vi quốc tế

Không bị giới hạn về các nghĩa vụ khác, nhà cung cấp sẽ không thực hiện hoạt động chuyển Dữ liệu cá nhân của Microsoft trên phạm vi quốc tế, trừ khi Microsoft có văn bản phê duyệt trước. Đồng thời, trong bất kỳ trường hợp nào, nhà cung cấp phải tuân thủ các yêu cầu bảo vệ dữ liệu của mọi điều khoản tiêu chuẩn theo hợp đồng, quy tắc ràng buộc của công ty hoặc kế hoạch khác do bất kỳ cơ quan bảo vệ dữ liệu nào, Ủy ban Bảo vệ Dữ liệu Châu Âu hoặc Ủy ban Châu Âu phê duyệt và được Microsoft chấp nhận hoặc đồng ý, bao gồm khuôn khổ Bảo vệ Quyền riêng tư của Liên minh châu Âu-Hoa Kỳ và Thụy Sĩ-Hoa Kỳ cũng như Quy định Bảo vệ Dữ liệu Chung của Liên minh Châu Âu. Nhà cung cấp đồng ý thông báo cho Microsoft trong trường hợp Nhà cung cấp đưa ra quyết định rằng họ không thể đáp ứng nghĩa vụ cung cấp cùng một mức bảo vệ theo yêu cầu của nguyên tắc Bảo vệ Quyền riêng tư được nữa. Nhà cung cấp cũng phải đảm bảo rằng bất kỳ và mọi bên xử lý phụ (như định nghĩa trong Điều 1(d) của các Điều khoản Tiêu chuẩn theo Hợp đồng năm 2010 được xuất bản dưới dạng Phụ lục cho Nghị quyết của Ủy ban Châu Âu C(2010)593) cũng tuân thủ các yêu cầu này.

Định nghĩa chính

Các thuật ngữ sau đây được sử dụng trong Yêu cầu bảo vệ dữ liệu (DPR) này và có nghĩa như sau. Các thuật ngữ về ví dụ như "bao gồm", "chẳng hạn như", "ví dụ", "ví dụ như" hoặc các thuật ngữ tương tự được sử dụng trong Yêu cầu bảo vệ dữ liệu (DPR) này được hiểu là bao gồm nhưng " không giới hạn" hoặc "nhưng không giới hạn" trừ khi bị hạn chế bằng các từ như là "chỉ" hoặc "chỉ duy nhất".

"**Bên kiểm soát**" là cá nhân hoặc pháp nhân, cơ quan công quyền, cơ quan hoặc bất kỳ cơ quan nào khác mà một mình hoặc cùng với bên khác xác định mục đích và phương tiện của việc Xử lý dữ liệu cá nhân; trường hợp Luật Liên minh Châu Âu ("**EU**") hoặc Luật thành viên của Nhà nước quyết định mục đích và phương tiện Xử lý, thì bên kiểm soát (hoặc các tiêu chuẩn để chỉ định bên kiểm soát) có thể được những luật nàychỉ định.

"**Bên xử lý**" là cá nhân hoặc pháp nhân, cơ quan công quyền, cơ quan chức năng hoặc cơ quan khác Xử lý Dữ liệu cá nhân thay mặt cho Bên kiểm soát.

“**Dữ liệu cá nhân**” là mọi thông tin liên quan đến một cá nhân đã được nhận dạng hoặc có thể nhận dạng (“**Chủ thể dữ liệu**”); một cá nhân có thể nhận dạng là một người có thể được xác định, trực tiếp hoặc gián tiếp, đặc biệt là bằng cách tham chiếu một mã định danh như tên, số nhận dạng, dữ liệu vị trí, mã định danh trực tuyến hoặc tham chiếu một hoặc nhiều yếu tố cụ thể cho nhận dạng thể chất, sinh lý học, gien, tâm thần, kinh tế, văn hóa hoặc xã hội của cá nhân đó.

“**Dữ liệu cá nhân của Microsoft**” là mọi thông tin có thể gây ra thiệt hại về danh tiếng hoặc tài chính cho Microsoft nếu bị xâm phạm về tính bảo mật hoặc tính toàn vẹn thông tin. Dữ liệu mật của Microsoft bao gồm sản phẩm phần cứng và phần mềm của Microsoft, ứng dụng dòng nghiệp vụ nội bộ, tài liệu tiếp thị trước phát hành, khóa cấp phép sản phẩm và tài liệu kỹ thuật liên quan đến các sản phẩm và dịch vụ của Microsoft.

“**Dữ liệu mật của Microsoft**” nghĩa là mọi Dữ liệu cá nhân do Microsoft hoặc đại diện của Microsoft Xử lý.

“**Pháp luật**” có nghĩa là tất cả các luật, quy định, quy chế, nghị định, quyết định, lệnh, quy định phán quyết, bộ luật, nghị quyết và yêu cầu hiện hành của bất kỳ cơ quan chính phủ nào (liên bang, tiểu bang, địa phương hoặc quốc tế) có thẩm quyền. “**Bất hợp pháp**” có nghĩa là mọi hành vi vi phạm Pháp luật.

“**Quy trình**” nghĩa là một thao tác hoặc nhóm thao tác bất kỳ được thực hiện đối với mọi Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft, dù bằng phương pháp tự động hay không tự động, như thu thập, ghi âm, tổ chức, cấu trúc, lưu trữ, điều chỉnh hoặc thay thế, truy xuất, tư vấn, sử dụng, tiết lộ bằng cách truyền, phân phối hoặc cung cấp, căn chỉnh hay kết hợp, hạn chế, xóa hoặc hủy. "Đang xử lý" và "Đã xử lý" sẽ có ý nghĩa tương ứng.

“**Quyền của Chủ thể dữ liệu**” là quyền truy cập, xóa, chỉnh sửa, xuất, hạn chế hoặc phản đối việc Xử lý dữ liệu cá nhân của họ nếu được Pháp luật yêu cầu.

“**Vi phạm dữ liệu**” là vi phạm bảo mật dẫn đến phá hủy, mất mát, thay thế, tiết lộ trái phép hoặc truy cập vào Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft được truyền, lưu trữ hay nói cách khác là Được xử lý do vô tình hay Bất hợp pháp.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần A: Quản lý		
1	Mỗi thỏa thuận áp dụng giữa Microsoft và nhà cung cấp (ví dụ: Hợp đồng chính, tuyên bố nhiệm vụ, đơn mua hàng và các đơn đặt hàng khác) phải có nội dung về bảo vệ quyền riêng tư và dữ liệu bảo mật liên quan đến Dữ liệu cá nhân và Dữ liệu mật của Microsoft, nếu áp dụng. Đối với các công ty như Bên xử lý, thỏa thuận phải bao gồm vấn đề và thời gian của việc Xử lý, bản chất và mục đích của việc Xử lý, loại Dữ liệu cá nhân của Microsoft và các hạng mục Chủ thể dữ liệu cũng như các quyền và nghĩa vụ của Microsoft.	Nhà cung cấp phải trình hợp đồng đang có hiệu lực giữa Microsoft và Nhà cung cấp. Đối với Bên xử lý, phần mô tả Xử lý nằm trong hợp đồng áp dụng (*ví dụ:* tuyên bố nhiệm vụ, đơn mua hàng). Chú ý: Các công ty có đơn mua hàng trên chuyến bay có thể có phần mô tả cần thiết về các hoạt động Xử lý được thêm vào sau trong quy trình mua hàng.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
2	Giao trách nhiệm và nghĩa vụ tuân thủ DPR cho một người hoặc nhóm được chỉ định trong công ty.	Tên của người hoặc nhóm được giao trách nhiệm đảm bảo tuân thủ Yêu cầu bảo vệ dữ liệu (DPR) dành cho Nhà cung cấp của Microsoft. Tài liệu mô tả thẩm quyền và trách nhiệm giải trình của người hoặc nhóm này thể hiện vai trò bảo mật và/hoặc quyền riêng tư.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
3	Thiết lập, duy trì và thực hiện đào tạo hàng năm về quyền riêng tư và bảo mật cho nhân viên sẽ có quyền truy cập vào Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft. Nếu công ty của bạn chưa có nội dung được chuẩn bị sẵn, bạn có thể dùng tài liệu phân cảnh này và điều chỉnh tài liệu phù hợp với công ty của bạn.	Có sẵn hồ sơ tham dự hàng năm. Nội dung đào tạo bao gồm các nguyên tắc bảo mật và quyền riêng tư.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
4	Chỉ xử lý Dữ liệu cá nhân của Microsoft theo tài liệu hướng dẫn của Microsoft, bao gồm cả hướng dẫn về việc chuyển Dữ liệu cá nhân của Microsoft cho quốc gia thứ ba hoặc tổ chức quốc tế, trừ khi Luật hiện hành yêu cầu như vậy; trong trường hợp đó, Bên xử lý (nhà cung cấp) sẽ thông báo cho bên kiểm soát (Microsoft) về yêu cầu pháp lý trước khi Xử lý, trừ khi Luật pháp nghiêm cấm thông tin như vậy dựa trên cơ sở quan trọng về lợi ích chung.	Bằng chứng về tài liệu hướng dẫn như đã nêu trong hợp đồng (ví dụ: tuyên bố nhiệm vụ hoặc đơn mua hàng) hoặc được ghi trong hệ thống điện tử đã sử dụng khi Thực hiện.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần B: Thông báo		
5	Nhà cung cấp phải sử dụng Điều khoản về quyền riêng tư của Microsoft khi thay mặt Microsoft thu thập Dữ liệu cá nhân. Thông báo về quyền riêng tư phải rõ ràng và được cung cấp cho Chủ thể dữ liệu nhằm giúp họ quyết định có gửi Dữ liệu cá nhân của mình cho nhà cung cấp hay không. Chú ý: Trường hợp công ty của bạn là Bên kiểm soát hoạt động Xử lý, bạn sẽ đăng thông báo bảo mật của riêng mình. *Hãy liên hệ với SSPAHelp@microsoft.com để truy cập vào các thông báo chính xác của Microsoft.*	Nhà cung cấp sử dụng một nối kết chuyển tiếp tới Điều khoản về quyền riêng tư của Microsoft đã được công bố và đang áp dụng. Điều khoản về quyền riêng tư được đăng trong bất kỳ ngữ cảnh nào mà Dữ liệu cá nhân của người dùng sẽ được thu thập. Một phiên bản ngoại tuyến sẽ có sẵn và được cung cấp trước khi thu thập dữ liệu. Mọi phiên bản ngoại tuyến của Điều khoản về quyền riêng tư được sử dụng là phiên bản được xuất bản gần đây nhất và được cập nhật đúng cách. Thông báo bảo vệ dữ liệu của Microsoft được sử dụng cho các dịch vụ dành cho nhân viên của Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
6	Khi thu thập Dữ liệu cá nhân của Microsoft thông qua gọi điện trực tiếp hoặc cuộc gọi thoại có ghi âm, nhà cung cấp phải sẵn sàng thảo luận về các quy định thu thập, xử lý, sử dụng và lưu giữ dữ liệu với Chủ thể dữ liệu.	Tập lệnh cho bản ghi âm giọng nói bao gồm cách Dữ liệu cá nhân của Microsoft được Xử lý, bao gồm: ▪ thu thập, ▪ sử dụng và ▪ duy trì.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần C: Lựa chọn và Đồng ý		
7	Nếu nhà cung cấp lấy sự đồng ý của Chủ thể dữ liệu làm cơ sở pháp lý để Xử lý dữ liệu thì họ phải xin phép và ghi lại sự đồng ý của Chủ thể dữ liệu đối với tất cả các hoạt động Xử lý (bao gồm mọi hoạt động Xử lý mới và cập nhật) trước khi thu thập Dữ liệu cá nhân của Chủ thể dữ liệu.	Nhà cung cấp có thể chứng minh cách Chủ thể dữ liệu đồng ý cho hoạt động Xử lý và phạm vi đồng ý bao gồm tất cả các hoạt động Xử lý của nhà cung cấp liên quan đến Dữ liệu cá nhân của Chủ thể dữ liệu đó. Nhà cung cấp có thể chứng minh cách một Chủ thể dữ liệu rút lại sự đồng ý cho một hoạt động Xử lý. Nhà cung cấp có thể chứng minh cách các tùy chọn được kiểm tra trước khi khởi chạy một hoạt động Xử lý mới. Nhà cung cấp phải giám sát hiệu quả quản lý tùy chọn để đảm bảo khung thời gian để thực hiện thay đổi tùy chọn là yêu cầu pháp lý địa phương hạn chế nhất được áp dụng. Chú ý: Bằng chứng có thể là ảnh chụp màn hình tương tác của người dùng; thử nghiệm với dịch vụ hoặc cơ hội để xem tài liệu kỹ thuật.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần C: Lựa chọn và Đồng ý (tiếp theo)		
8	Cookie là tệp văn bản nhỏ được các trang web và/hoặc ứng dụng lưu trữ trên thiết bị. Cookie chứa thông tin dùng để nhận dạng Chủ thể dữ liệu hoặc thiết bị. Nhà cung cấp tạo và quản lý các trang web và/hoặc ứng dụng của Microsoft phải cung cấp cho Chủ thể dữ liệu thông báo và lựa chọn rõ ràng về việc sử dụng cookie. Nhà cung cấp tạo và quản lý các trang web và/hoặc ứng dụng của Microsoft phải đảm bảo rằng việc sử dụng cookie tuân thủ các cam kết trong Điều khoản về quyền riêng tư của Microsoft cũng như các yêu cầu pháp lý của địa phương như các quy tắc do Liên minh Châu Âu đặt ra.	Nhà cung cấp phải ghi chép mục đích của mỗi cookie và phải thông báo loại cookie được triển khai. ▪ Không được sử dụng cookie dài hạn khi có đủ cookie phiên truy cập. ▪ Khi sử dụng cookie dài hạn, ngày hết hạn của những cookie này không được vượt quá 2 năm sau khi người dùng đã truy cập vào trang web. Đối với người dùng ở Liên minh Châu Âu, ngày hết hạn của một cookie dài hạn không được vượt quá 13 tháng. Xác thực việc tuân thủ Pháp luật hiện hành ở Liên minh Châu Âu, ví dụ như: ▪ sử dụng quy ước về gắn nhãn, “Quyền riêng tư và Cookie” cho điều khoản về quyền riêng tư, và ▪ đảm bảo có sự đồng ý chắc chắn của người dùng trước khi sử dụng cookie cho các mục đích “không cần thiết” như quảng cáo.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần D: Thu thập		
9	Nhà cung cấp phải giám sát việc thu thập Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft nhằm đảm bảo chỉ thu thập dữ liệu cần thiết để Thực hiện.	Nhà cung cấp có thể cung cấp tài liệu cho thấy rằng việc thu thập Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft là cần phải Thực hiện.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
10	Nếu nhà cung cấp thay mặt cho Microsoft thu thập Dữ liệu cá nhân từ các bên thứ ba, nhà cung cấp phải xác nhận rằng các chính sách và phương pháp bảo vệ dữ liệu của bên thứ ba phù hợp với hợp đồng của nhà cung cấp với Microsoft và Yêu cầu bảo vệ dữ liệu (DPR).	Nhà cung cấp có thể cung cấp tài liệu về việc đã thực hiện thẩm định đối với chính sách và phương pháp bảo vệ dữ liệu của bên thứ ba.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
11	Trước khi thu thập Dữ liệu cá nhân của Microsoft thông qua cài đặt hoặc sử dụng phần mềm thực thi trên thiết bị của Chủ thể dữ liệu, nhu cầu thu thập thông tin này phải được ghi trong hợp đồng đã thực thi giữa nhà cung cấp và Microsoft.	Thỏa thuận của Microsoft về sử dụng phần mềm thực thi trên thiết bị của Chủ thể dữ liệu được ghi chú trong hợp đồng thực hiện.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
12	Trước khi thu thập Dữ liệu cá nhân nhạy cảm của Microsoft (dữ liệu thể hiện nguồn gốc chủng tộc hoặc dân tộc, quan điểm chính trị, tín ngưỡng tôn giáo hoặc triết học hoặc tư cách thành viên công đoàn, dữ liệu di truyền, dữ liệu sinh trắc học, dữ liệu về sức khỏe hoặc dữ liệu về đời sống tình dục hoặc khuynh hướng tình dục của một cá nhân), thì sự cần thiết phải thu thập Dữ liệu cá nhân đó phải được ghi trong hợp đồng đã thực thi giữa nhà cung cấp và Microsoft.	Sự cần thiết phải thu thập Dữ liệu cá nhân nhạy cảm của Microsoft được ghi chú trong hợp đồng thực thi với Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần E: Duy trì		
13	Đảm bảo lưu giữ Dữ liệu cá nhân và Dữ liệu mật của Microsoft không quá thời gian cần thiết để Thực hiện, trừ khi Luật quy định phải tiếp tục lưu giữ Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft.	Nhà cung cấp tuân theo các chính sách lưu giữ hoặc yêu cầu lưu giữ đã lập thành văn bản do Microsoft chỉ định trong hợp đồng (ví dụ: tuyên bố nhiệm vụ, đơn mua hàng).	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
14	Đảm bảo rằng, theo quyết định riêng của Microsoft, Dữ liệu cá nhân và Dữ liệu mật của Microsoft mà nhà cung cấp đang sở hữu hoặc kiểm soát được trả lại cho Microsoft hoặc tiêu hủy khi hoàn thành việc Thực hiện hoặc theo yêu cầu của Microsoft. Nhà cung cấp phải có các quy trình trong phạm vi ứng dụng để đảm bảo rằng dữ liệu bị xóa khỏi ứng dụng rõ ràng bởi người dùng hoặc dựa vào các yếu tố kích hoạt khác như tuổi của dữ liệu, thì dữ liệu đó được xóa an toàn. Khi cần tiêu hủy Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft, nhà cung cấp phải đốt, nghiền nát hoặc xé vụn các tài sản hữu hình chứa Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft để không ai có thể đọc hoặc tái tạo thông tin đó.	Lưu giữ hồ sơ sử dụng Dữ liệu cá nhân và Dữ liệu mật của Microsoft (bao gồm cả việc trả lại cho Microsoft để tiêu hủy). Trường hợp được Microsoft đề nghị hoặc yêu cầu tiêu hủy, nhà cung cấp phải đưa cho Microsoft chứng nhận tiêu hủy có chữ ký của nhân viên của nhà cung cấp.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần F: Chủ thể Dữ liệu		
	Chủ thể dữ liệu có quyền truy cập, xóa, chỉnh sửa, xuất, hạn chế và phản đối việc Xử lý Dữ liệu cá nhân của họ ("**Quyền của Chủ thể dữ liệu**"). Khi Chủ thể dữ liệu muốn thực hiện quyền của mình theo Pháp luật đối với Dữ liệu cá nhân của Microsoft, nhà cung cấp phải:		
15	Thông qua các biện pháp kỹ thuật và tổ chức thích hợp, hỗ trợ Microsoft trong phạm vi có thể để thực hiện nghĩa vụ trả lời các yêu cầu của Chủ thể dữ liệu muốn thực hiện Quyền của chủ thể dữ liệu.	Các quy trình và thủ tục được áp dụng để hỗ trợ thực thi Quyền của Chủ thể dữ liệu.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
16	Trả lời mọi yêu cầu về Quyền của Chủ thể Dữ liệu mà không chậm trễ quá mức.	Nhà cung cấp tiến hành kiểm tra định kỳ nhằm đảm bảo họ có thể hỗ trợ Quyền của Chủ thể dữ liệu.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
17	Trừ khi có hướng dẫn khác của Microsoft, Nhà cung cấp sẽ giới thiệu tất cả Chủ thể Dữ liệu vốn liên hệ trực tiếp với Nhà cung cấp với Microsoft để thực hiện quyền của Chủ thể Dữ liệu. Nhà cung cấp sẽ trao đổi với Chủ thể dữ liệu về các bước mà cá nhân đó phải thực hiện để có thể truy cập hoặc thực hiện quyền của họ đối với Dữ liệu cá nhân của Microsoft. *Liên hệ với SSPAHelp@microsoft.com để được trợ giúp về yêu cầu này.*	Nhà cung cấp thông báo các bước cần thực hiện để truy cập vào Dữ liệu cá nhân cũng như các phương pháp sẵn có để cập nhật dữ liệu đó.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
18	Khi trả lời trực tiếp Chủ thể Dữ liệu, hãy xác nhận danh tính của Chủ thể Dữ liệu đưa ra yêu cầu.	Nhà cung cấp đã ghi lại phương pháp dùng để xác định Chủ thể dữ liệu của Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần F: Chủ thể Dữ liệu (tiếp theo)		
	Sau khi đã xác thực Chủ thể Dữ liệu đó, nhà cung cấp phải:		
19	Xác định xem chủ thể đó nắm giữ hay kiểm soát Dữ liệu cá nhân của Microsoft về Chủ thể dữ liệu đó.	Nhà cung cấp luôn có sẵn các quy trình để xác định Dữ liệu cá nhân có được lưu giữ hay không.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
20	Thực hiện các nỗ lực hợp lý để tìm Dữ liệu cá nhân của Microsoft được yêu cầu và lưu giữ đầy đủ hồ sơ để chứng minh rằng công tác tra soát hợp lý đã được tiến hành.	Nhà cung cấp lưu giữ hồ sơ về các bước đã thực hiện để đáp ứng yêu cầu Quyền của chủ thể dữ liệu. Tài liệu bao gồm: ▪ ngày và thời gian yêu cầu, ▪ các hành động được thực hiện để phản hồi yêu cầu, và ▪ bản ghi lại thời điểm đã thông báo cho Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
21	Ghi lại ngày và giờ của yêu cầu về Quyền của chủ thể dữ liệu cũng như hành động mà nhà cung cấp đã thực hiện nhằm phản hồi các yêu cầu đó. Cung cấp hồ sơ về yêu cầu của Chủ thể Dữ liệu cho Microsoft khi có yêu cầu.	Nhà cung cấp lưu giữ hồ sơ về yêu cầu truy cập và ghi lại các thay đổi đã thực hiện đối với Dữ liệu cá nhân.	
	Sau khi đã xác thực Chủ thể dữ liệu và nhà cung cấp đã xác thực rằng họ có Dữ liệu cá nhân của Microsoft được yêu cầu, nhà cung cấp phải:		
22	Đối với các yêu cầu nhận bản sao Dữ liệu cá nhân, hãy cung cấp Dữ liệu cá nhân của Microsoft cho Chủ thể dữ liệu ở định dạng in, điện tử hoặc bằng lời nói thích hợp.	Nhà cung cấp sẽ cung cấp Dữ liệu cá nhân cho Chủ thể dữ liệu theo định dạng dễ hiểu và hình thức thuận tiện cho Chủ thể dữ liệu và nhà cung cấp.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
23	Theo hướng dẫn của Microsoft, nếu yêu cầu của Chủ thể Dữ liệu bị từ chối, hãy cung cấp cho họ văn bản giải thích nhất quán với bất kỳ hướng dẫn nào có liên quan mà Microsoft đã cung cấp trước đó. *Liên hệ với SSPAHelp@microsoft.com để được trợ giúp về yêu cầu này.*	Ghi lại các trường hợp từ chối yêu cầu và giữ lại bằng chứng xem xét và phê duyệt của Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần F: Chủ thể Dữ liệu (tiếp theo)		
24	Nhà cung cấp phải có biện pháp phòng ngừa hợp lý nhằm đảm bảo rằng không ai có thể sử dụng Dữ liệu cá nhân của Microsoft được cung cấp cho Chủ thể dữ liệu để nhận dạng cá nhân khác.	Nhà cung cấp phải chứng minh rằng mình đã thực hiện các biện pháp phòng ngừa hợp lý để không ai có thể sử dụng thông tin đã tiết lộ để nhận dạng một cá nhân khác (ví dụ: không thể sao chụp toàn bộ trang dữ liệu khi Dữ liệu cá nhân được yêu cầu cho Chủ thể dữ liệu chỉ xuất hiện trên một dòng).	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
25	Nếu Chủ thể dữ liệu và nhà cung cấp không thống nhất được Dữ liệu cá nhân của Microsoft có đầy đủ và chính xác hay không, thì nhà cung cấp phải thông báo với Microsoft về vấn đề này và hợp tác với Microsoft để cùng giải quyết vấn đề này nếu cần. *Liên hệ với SSPAHelp@microsoft.com để được trợ giúp về yêu cầu này.*	Nhà cung cấp dẫn chứng bằng tài liệu về các trường hợp không đồng ý và thông báo vấn đề này với Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần G: Tiết lộ cho Bên Thứ ba		
	Nếu nhà cung cấp định sử dụng nhà thầu phụ để Xử lý Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft, nhà cung cấp phải:		
26	Có được sự đồng ý rõ ràng bằng văn bản của Microsoft trước khi thầu lại dịch vụ hoặc thực hiện bất kỳ thay đổi nào có liên quan đến việc thêm hoặc thay thế nhà thầu phụ. *Hãy liên hệ với SSPAHelp@microsoft.com để được giúp đỡ về yêu cầu này.*	Xác thực rằng chỉ những công ty do Microsoft chỉ định mới được Xử lý Dữ liệu cá nhân của Microsoft theo yêu cầu trong hợp đồng áp dụng (ví dụ: tuyên bố nhiệm vụ, phụ lục, đơn mua hàng) hoặc được ghi lại trong cơ sở dữ liệu SSPA.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
27	Ghi lại tính chất và mức độ của Dữ liệu cá nhân và Dữ liệu mật của Microsoft do nhà thầu phụ xử lý, đảm bảo rằng thông tin thu thập là thông tin bắt buộc phải có để Thực hiện.	Nhà cung cấp lưu giữ tài liệu liên quan đến Dữ liệu cá nhân và Dữ liệu mật của Microsoft đã tiết lộ hoặc chuyển giao cho nhà thầu phụ.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
28	Đảm bảo rằng nhà thầu phụ sử dụng Dữ liệu cá nhân của Microsoft theo đúngtùy chọn liên hệ đã nêu của Chủ thể dữ liệu.	Chứng minh cách nhà thầu phụ sử dụng tùy chọn Chủ thể dữ liệu của Microsoft. Cung cấp tài liệu hỗ trợ bao gồm khung thời gian cho nhà thầu phụ để thực hiện thay đổi tùy chọn.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
29	Nhà thầu phụ chỉ được Xử lý dữ liệu cá nhân của Microsoft cho các mục đích cần thiết để hoàn thành hợp đồng của nhà cung cấp với Microsoft.	Nhà cung cấp có thể đưa ra tài liệu cho thấy rằng Dữ liệu cá nhân của Microsoft cung cấp cho nhà thầu phụ là việc cần phải Thực hiện.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
30	Xem lại các khiếu nại để biết các dấu hiệu về việc Xử lý dữ liệu cá nhân của Microsoft trái phép hoặc Bất hợp pháp.	Nhà cung cấp có thể chứng minh rằng họ luôn có sẵn hệ thống và quy trình để giải quyết các khiếu nại về việc nhà thầu phụ sử dụng hoặc tiết lộ trái phép Dữ liệu cá nhân của Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần G: Tiết lộ cho Bên Thứ ba (tiếp theo)		
31	Thông báo ngay cho Microsoft khi biết rằng nhà thầu phụ đã Xử lý dữ liệu cá nhân hoặc dữ liệu mật của Microsoft cho bất kỳ mục đích nào ngoài mục đích có liên quan đến việc Thực hiện.	Nhà cung cấp đã cung cấp cho nhà thầu phụ các hướng dẫn và phương tiện để báo cáo việc sử dụng sai dữ liệu của Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
32	Hành động ngay để giảm thiểu bất kỳ thiệt hại thực sự hoặc tiềm ẩn nào do nhà thầu phụ Xử lý trái phép hoặc bất hợp pháp Dữ liệu cá nhân và Dữ liệu mật của Microsoft.	Nhà cung cấp có thể chứng minh rằng họ luôn có sẵn kế hoạch và thủ tục nếu nhà thầu phụ sử dụng sai mục đích Dữ liệu cá nhân và Dữ liệu mật của Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
	Phần H: Chất lượng		
33	Nhà cung cấp phải duy trì tính toàn vẹn của tất cả Dữ liệu cá nhân của Microsoft, đảm bảo thông tin vẫn chính xác, đầy đủ và có liên quan đến mục đích Xử lý đã nêu.	Nhà cung cấp có thể chứng minh rằng họ luôn có sẵn thủ tục để xác thực Dữ liệu cá nhân của Microsoft khi những dữ liệu này được thu thập, tạo và cập nhật. Nhà cung cấp có thể chứng minh rằng họ luôn có sẵn thủ tục giám sát và lấy mẫu để xác minh tính chính xác trên cơ sở hiện hành và sửa chữa khi cần thiết.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần I: Giám sát và Thực thi		
34	Nhà cung cấp có kế hoạch phản hồi sự việc yêu cầu Nhà cung cấp phải thông báo cho Microsoft không chậm trễ quá mức khi phát hiện ra Vi phạm dữ liệu hoặc lỗ hổng bảo mật liên quan đến việc nhà cung cấp xử lý Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft. *Hãy liên hệ với SSPAHelp@microsoft.com để báo cáo sự việc.*	Nhà cung cấp có kế hoạch phản hồi sự việc trong đó có bước thông báo cho khách hàng (Microsoft) như mô tả trong phần này.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
35	Trừ khi được pháp luật quy định, không đưa ra thông cáo báo chí hoặc bất kỳ thông báo công khai nào khác về việc Vi phạm dữ liệu có liên quan đến Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft khi chưa được Microsoft phê duyệt.	Nhà cung cấp đồng ý thực hiện yêu cầu này nếu sự kiện xảy ra.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
36	Thực hiện kế hoạch khắc phục và giám sát việc giải quyết các Vi phạm dữ liệu và lỗ hổng bảo mật liên quan đến Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft để đảm bảo thực hiện kịp thời biện pháp khắc phục phù hợp.	Nhà cung cấp đã ghi lại thủ tục sẽ thực hiện để phản hồi nhằm giải quyết việc Vi phạm dữ liệu.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
37	Thiết lập quy trình xử lý khiếu nại chính thức để phản hồi mọi khiếu nại về bảo vệ dữ liệu liên quan đến Dữ liệu cá nhân của Microsoft.	Nhà cung cấp có phương tiện để nhận khiếu nại liên quan đến Dữ liệu cá nhân của Microsoft và ghi lại thủ tục khiếu nại để giải quyết khiếu nại.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật		
	Nhà cung cấp phải thiết lập, triển khai và duy trì chương trình bảo mật thông tin bao gồm các chính sách và quy trình để bảo vệ và giữ an toàn cho Dữ liệu cá nhân và Dữ liệu mật của Microsoft theo phương pháp phù hợp của ngành cũng như theo quy định luật hiện hành Chương trình bảo mật của nhà cung cấp phải đáp ứng các tiêu chuẩn đã thu thập dưới đây, các yêu cầu 38 -56.	Các biện pháp bảo vệ có thể nhiều hơn những trường hợp được liệt kê khi cần thiết nhằm đáp ứng hệ thống điều tiết (ví dụ: HIPAA, GLBA) hoặc các yêu cầu theo hợp đồng. Báo cáo ISO 27001 hoặc Báo cáo SOC 2 hợp lệ có bảo mật là các sản phẩm thay thế được chấp nhận cho Mục J. Hãy liên hệ với SSPAHelp@microsoft.com để áp dụng thay thế này. Chú ý: Bạn sẽ cần cung cấp tài liệu mô tả phạm vi của các chứng nhận/báo cáo này.	
38	Thực hiện đánh giá bảo mật mạng hàng năm, bao gồm: ▪ xem lại các thay đổi lớn đối với môi trường như thành phần hệ thống mới, tôpô mạng, quy tắc tường lửa, ▪ tiến hành quét tìm lỗ hổng bảo mật, và ▪ duy trì nhật ký thay đổi.	Nhà cung cấp đã ghi lại các đánh giá mạng, nhật ký thay đổi và kết quả quét. Nhật ký thay đổi bắt buộc phải theo dõi các thay đổi, cung cấp thông tin liên quan đến lý do thay đổi cũng như phải bao gồm tên và tiêu đề của người phê duyệt được chỉ định.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
39	Nhà cung cấp xác định, truyền đạt và triển khai chính sách thiết bị di động giúp đảm bảo và giới hạn việc sử dụng Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft được truy cập hoặc sử dụng trên thiết bị di động.	Nhà cung cấp chứng minh việc sử dụng chính sách thiết bị di động tuân thủ trong trường hợp việc Xử lý Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft yêu cầu sử dụng thiết bị di động.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật (tiếp theo)		
40	Mọi tài sản dùng để hỗ trợ việc Thực hiện phải được giải trình và có chủ sở hữu được xác định. Nhà cung cấp chịu trách triệm duy trì bản tóm tắt các tài sản thông tin này; thiết lập hoạt động sử dụng tài sản được ủy quyền và chấp nhận được; và cung cấp mức độ bảo vệ tài sản một cách thích hợp thông qua vòng đời của chúng.	Bản tóm tắt các tài sản thiết bị được dùng để hỗ trợ việc Thực hiện. Bản tóm tắt các tài sản này bao gồm: ▪ vị trí thiết bị, ▪ phân loại dữ liệu của dữ liệu về tài sản, ▪ bản ghi khôi phục tài sản khi chấm dứt thỏa thuận lao động hoặc kinh doanh, và ▪ bản ghi thải bỏ phương tiện lưu trữ dữ liệu khi không còn cần thiết.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật (tiếp theo)		
41	Thiết lập và duy trì các quy trình quản lý quyền truy cập nhằm ngăn truy cập trái phép vào bất kỳ Dữ liệu cá nhân hoặc Dữ liệu mật nào của Microsoft dưới sự kiểm soát của nhà cung cấp.	Nhà cung cấp chứng minh rằng họ đã triển khai kế hoạch quản lý quyền truy cập bao gồm: ▪ quy trình kiểm soát truy cập, ▪ quy trình nhận dạng, ▪ quy trình khóa sau nhiều lần thử không thành công, ▪ cần phải thường xuyên đặt lại mật khẩu nhưng không quá 90 ngày một lần, ▪ các tham số hiệu quả để chọn thông tin đăng nhập xác thực, và ▪ hủy kích hoạt tài khoản của người dùng khi chấm dứt hợp đồng lao động trong vòng 48 giờ. Nhà cung cấp chứng minh rằng họ đã thiết lập một quy trình xem xét quyền truy cập của người dùng vào Dữ liệu cá nhân và Dữ liệu mật của Microsoft, thực thi nguyên tắc đặc quyền tối thiểu. Quy trình này bao gồm: ▪ xác định rõ vai trò người dùng, ▪ các quy trình xem xét và xác minh phê duyệt quyền truy cập vào vai trò, và ▪ kiểm tra xemnhững người dùng đảm nhận vai trò có quyền truy cập vào dữ liệu của Microsoft có xác minh đã ghi lại đối với nhóm/vai trò hay không.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật (tiếp theo)		
42	Xác định và triển khai các quy trình quản lý bản vá để ưu tiên các bản vá bảo mật cho các hệ thống dùng để Xử lý dữ liệu cá nhân hoặc dữ liệu mật của Microsoft. Các quy trình này bao gồm: ▪ xác định cách tiếp cận rủi ro để ưu tiên các bản vá bảo mật ▪ khả năng xử lý và triển khai các bản vá khẩn cấp, ▪ khả năng áp dụng cho Hệ điều hành và phần mềm máy chủ như máy chủ ứng dụng và phần mềm cơ sở dữ liệu, ▪ ghi lại rủi ro mà bản vá giúp giảm nhẹ và theo dõi mọi trường hợp ngoại lệ, và ▪ yêu cầu loại bỏ phần mềm không còn được công ty sản xuất phần mềm này hỗ trợ nữa.	Nhà cung cấp có thể chứng minh là đã triển khai quy trình quản lý vá đáp ứng yêu cầu này và bao gồm, tối thiểu, như sau: ▪ Chỉ định mức độ nghiêm trọng để ưu tiên thông báo. (Ghi lại định nghĩa mức độ nghiêm trọng.) ▪ Quy trình tiến hành vá khẩn cấp được ghi vào tài liệu. ▪ Xác nhận là không sử dụng các hệ điều hành không còn được công ty sản xuất các hệ điều hành này hỗ trợ nữa. ▪ Bản ghi quản lý bản vá theo dõi phê duyệt và ngoại lệ.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
43	Cài đặt phần mềm chống vi-rút và chống phần mềm độc hại trên thiết bị được kết nối với mạng dùng để Xử lý dữ liệu cá nhân và dữ liệu mật của Microsoft, bao gồm máy chủ, máy tính để bàn dành cho sản xuất và đào tạo nhằm chống lại vi-rút có thể gây hại và các ứng dụng phần mềm độc hại. Cập nhật định nghĩa chống phần mềm độc hại hàng ngày và theo hướng dẫn của nhà cung cấp dịch vụ chống vi-rút/chống phần mềm độc hại. Chú ý: Điều này áp dụng cho tất cả các hệ điều hành bao gồm cả Linux.	Các bản ghi dùng để hiển thị phần mềm chống vi-rút và phần mềm chống phần mềm độc hại đang hoạt động. Chú ý: Yêu cầu này áp dụng cho tất cả các hệ điều hành.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
44	Nhà cung cấp phát triển phần mềm cho Microsoft phải kết hợp các nguyên tắc an toàn theo thiết kế trong quá trình xây dựng.	Tài liệu kỹ thuật của nhà cung cấp bao gồm các điểm kiểm tra để xác nhận bảo mật trong chu kỳ phát triển của họ.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật (tiếp theo)		
45	Sử dụng chương trình Ngăn mất dữ liệu ("**DLP**"). Dữ liệu phải được phân loại, dán nhãn và bảo vệ đúng cách. Nhà cung cấp phải giám sát các hệ thống thông tin đang sử dụng khi xử lý Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft để tránh việc xâm nhập, làm mất dữ liệu và các hoạt động trái phép khác. Chương trình Ngăn mất dữ liệu (DLP), ở mức tối thiểu, ▪ yêu cầu sử dụng Hệ thống phát hiện xâm nhập ("**IDS**") trên nền máy chủ, mạng và trên nền điện toán đám mây theo tiêu chuẩn ngành nếu bạn lưu giữ Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft, ▪ yêu cầu triển khai các Hệ thống ngăn xâm nhập tiên tiến ("**IPS**") được cấu hình để giám sát và chủ động ngăn mất dữ liệu, ▪ trong trường hợp hệ thống bị xâm phạm, yêu cầu phân tích hệ thống nhằm đảm bảo mọi lỗ hổng bảo mật còn lại cũng được xử lý. ▪ mô tả các quy trình được yêu cầu để giám sát các công cụ phát hiện xâm nhập hệ thống, và ▪ thiết lập quy trình quản lý và phản hồi sự việc bắt buộc phải thực hiện khi phát hiện một sự kiện vi phạm dữ liệu.	Ghi lại Hệ thống phát hiện xâm nhập/Hệ thống ngăn xâm nhập (IDS/IPS) bằng các thủ tục có sẵn để phản hồi trực tiếp khi phát hiện lỗ hổng bảo mật hoặc Vi phạm dữ liệu.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
46	Thông báo ngay kết quả Điều tra từ phản hồi sự việc cho quản lý cấp cao và cho Microsoft. *Hãy liên hệ với SSPAHelp@microsoft.com để thông báo cho Microsoft.*	Các hệ thống và quy trình phải được áp dụng để thông báo kết quả điều tra phản hồi sự việc cho Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
47	Quản trị viên hệ thống, nhân viên thực thi, quản lý và các bên thứ ba phải được đào tạo về bảo mật hàng năm.	Thiết lập chương trình đào tạo về bảo mật bao gồm: ▪ đào tạo hàng năm về phản hồi sự việc, và ▪ cơ chế tự động và sự cố được mô phỏng để giúp phản hồi hiệu quả cho các tình huống khủng hoảng. Nhận thức về phòng ngừa sự cố như các rủi ro liên quan đến việc tải xuống phần mềm độc hại.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật (tiếp theo)		
48	Nhà cung cấp phải đảm bảo rằng các quy trình lập kế hoạch sao lưu bảo vệ Dữ liệu cá nhân và Dữ liệu mật của Microsoft không bị sử dụng, truy cập, tiết lộ, thay đổi và tiêu hủy trái phép.	Nhà cung cấp có thể chứng minh rằng quy trình phản hồi và khôi phục đã ghi lại nêu chi tiết cách tổ chức sẽ quản lý sự cố gây phiền toái và sẽ duy trì bảo mật thông tin ở cấp xác định trước dựa vào việc quản lý các mục tiêu liên tục bảo mật thông tin đã phê duyệt. Nhà cung cấp có thể chứng minh là đã xác định và triển khai quy trình để sao lưu định kỳ, lưu trữ an toàn và khôi phục hiệu quả dữ liệu quan trọng.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
49	Thiết lập và kiểm tra các kế hoạch kinh doanh liên tục và khắc phục thảm họa.	Kế hoạch khắc phục thảm họa phải bao gồm tất cả những mục sau: ▪ Tiêu chí đã xác định để định rõ xem hệ thống có quan trọng với hoạt động kinh doanh của nhà cung cấp hay không. ▪ Liệt kê các hệ thống quan trọng dựa vào các tiêu chí đã xác định phải được nhắm mục tiêu để khôi phục trong trường hợp xảy ra thảm họa. ▪ Quy trình khắc phục thảm họa đã xác định cho mỗi hệ thống quan trọng giúp đảm bảo kỹ sư không biết hệ thống có thể khôi phục ứng dụng trong vòng 72 giờ. ▪ Kiểm tra và xem lại các kế hoạch khắc phục thảm họa hàng năm (hoặc thường xuyên hơn) nhằm đảm bảo có thể đáp ứng các mục tiêu khôi phục.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật (tiếp theo)		
50	Xác thực danh tính của cá nhân trước khi trao quyền truy cập vào Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft cho cá nhân đó.	Đảm bảo rằng tất cả ID người dùng là duy nhất và mỗi ID có phương pháp xác thực tiêu chuẩn của ngành như Azure Active Directory. Tăng quyền truy cập (quản trị hoặc các loại đặc quyền nâng cao khác) phải yêu cầu sử dụng một yếu tố phụ như trình xác thực dựa vào thẻ thông minh hoặc điện thoại.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
51	Nhà cung cấp phải bảo vệ Dữ liệu cá nhân và Dữ liệu mật của Microsoft khi chuyển qua mạng có mã hóa bằng cách sử dụng Bảo mật lớp truyền tải ("**TLS**") hoặc Bảo mật giao thức Internet ("**IPsec**"). Các phương pháp này được mô tả trong NIST 800-52 và NIST 800-57; cũng có thể sử dụng tiêu chuẩn ngành tương ứng. Nhà cung cấp phải từ chối giao bất kỳ Dữ liệu cá nhân hoặc Dữ liệu mật nào của Microsoft được truyền qua phương thức không được mã hóa.	Quy trình tạo, triển khai và thay thế TLS hoặc các chứng chỉ khác phải được xác định và thực thi.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
52	Tất cả thiết bị của nhà cung cấp (máy tính xách tay, máy trạm, v.v) sẽ truy cập hoặc xử lý Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft phải sử dụng mã hóa dựa trên đĩa.	Mã hóa tất cả thiết bị để đáp ứng Bitlocker hoặc giải pháp mã hóa đĩa tương ứng của ngành khác dành cho tất cả thiết bị khách được sử dụng để xử lý Dữ liệu cá nhân hoặc Dữ liệu mật của Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật (tiếp theo)		
53	Các hệ thống và quy trình (sử dụng các tiêu chuẩn ngành hiện hành như được mô tả trong tiêu chuẩn NIST 800-111) phải luôn có sẵn để mã hóa phần còn lại (khi được lưu trữ) của bất kỳ và mọi Dữ liệu cá nhân và/hoặc Dữ liệu mật của Microsoft, bao gồm tất cả những dữ liệu sau đây: ▪ dữ liệu thông tin đăng nhập (ví dụ: tên người dùng/mật khẩu) ▪ dữ liệu công cụ thanh toán (ví dụ: số tài khoản ngân hàng và thẻ tín dụng) ▪ dữ liệu cá nhân liên quan đến di trú ▪ dữ liệu hồ sơ y tế (ví dụ: số hồ sơ y tế hoặc sinh trắc học hoặc số nhận dạng như DNA, vân tay, võng mạc mắt, mẫu giọng nói, mẫu khuôn mặt và số đo bàn tay, dùng cho mục đích xác thực) ▪ dữ liệu mã định danh do chính phủ cấp (ví dụ: số giấy phép lái xe hoặc số an sinh xã hội) ▪ dữ liệu thuộc về khách hàng của Microsoft (ví dụ: Sharepoint, tài liệu Office 365, khách hàng One Drive) ▪ tài liệu liên quan đến sản phẩm không công bố của Microsoft ▪ Ngày sinh ▪ Thông tin hồ sơ của trẻ em ▪ dữ liệu địa lý thời gian thực ▪ địa chỉ cá nhân (phi doanh nghiệp) ▪ số điện thoại cá nhân (phi doanh nghiệp) ▪ tôn giáo ▪ quan điểm chính trị ▪ xu hướng tình dục/sở thích ▪ câu trả lời cho câu hỏi bảo mật (ví dụ: 2fa, đặt lại mật khẩu) ○ tên thời con gái của mẹ	Kiểm tra xem Dữ liệu cá nhân và Dữ liệu mật của Microsoft liệt kê trong hàng này có được mã hóa không.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
54	Khi xử lý thẻ tín dụng thay mặt cho Microsoft, hãy tuân thủ các tiêu chuẩn xử lý thẻ tín dụng hiện hành cho mỗi công ty phát hành thẻ.	Chứng minh tuân thủ bằng cách xuất trình chứng chỉ Tiêu chuẩn Dịch vụ Dữ liệu Ngành Thẻ Thanh toán ("**PCI-DSS**") hàng năm. *Gửi chứng chỉ PCI DSS tới SSPA. Vui lòng liên hệ với SSPAHelp@microsoft.com nếu có bất kỳ câu hỏi nào.*	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng tuân thủ	Phản hồi
	Phần J: Bảo mật (tiếp theo)		
55	Nhà cung cấp phải cất giữ các tài sản hữu hình của Microsoft trong môi trường có kiểm soát hoạt động truy cập.	Hệ thống và quy trình phải được áp dụng để quản lý việc truy cập vật lý vào các bản sao kỹ thuật số, bản sao cứng, bản lưu trữ và bản sao sao lưu dữ liệu của Microsoft. Phải theo dõi chuỗi công việc bảo quản để di chuyển và hủy phương tiện vật lý chứa dữ liệu của Microsoft.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*
56	Ẩn danh tất cả Dữ liệu cá nhân của Microsoft được sử dụng trong môi trường phát triển hoặc thử nghiệm.	Không được sử dụng Dữ liệu cá nhân của Microsoft trong môi trường phát triển hoặc thử nghiệm; khi không có biện pháp thay thế, thông tin này phải được ẩn danh để ngăn chặn việc nhận dạng Chủ thể dữ liệu hoặc sử dụng sai Dữ liệu cá nhân. Chú ý: Dữ liệu ẩn danh khác với Dữ liệu theo bí danh. Dữ liệu ẩn danh là dữ liệu không liên quan đến một cá nhân đã được nhận dạng hoặc có thể nhận dạng được trong trường hợp chủ thể của dữ liệu cá nhân không hoặc không còn có thể nhận dạng được nữa.	*<Tuân thủ>* *<Không tuân thủ>* *<Không áp dụng>* *<Xung đột Pháp lý>* *<Xung đột Hợp đồng>*