Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft

Đối tượng áp dụng

Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft ("**DPR**") được áp dụng cho từng nhà cung cấp của Microsoft hiện đang Xử lý Dữ liệu Cá nhân của Microsoft hoặc Dữ liệu Bảo 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 Đơn mua hàng, thỏa thuận khung) (**"Thực hiện",** "**Đang thực hiện**" hoặc "**Việc thực hiện**").

- Trong trường hợp có xung đột giữa DPR này và các yêu cầu được quy định trong các thỏa thuận hợp đồng giữa nhà cung cấp và Microsoft, DPR sẽ được ưu tiên trừ khi nhà cung cấp đó xác định điều khoản chính xác trong hợp đồng sẽ thay thế cho yêu cầu về bảo vệ dữ liệu được áp dụng (trong trường hợp đó, các điều khoản của hợp đồng sẽ được ưu tiên).
- Trong trường hợp có xung đột giữa các yêu cầu trong tài liệu này và bất kỳ yêu cầu pháp lý hoặc theo luật định nào, các yêu cầu pháp lý hoặc theo luật định đó sẽ được ưu tiên.
- Trong trường hợp nhà cung cấp của Microsoft hoạt động dưới vai trò Bên kiểm soát, nhà cung cấp có thể đã giảm bớt các yêu cầu trong DPR này.
- 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, đối với DPR này, nhà cung cấp có thể đã giảm bớt các yêu cầu.

Truyền gửi dữ liệu quốc tế

Không giới hạn các nghĩa vụ khác của mình, nhà cung cấp sẽ không thực hiện bất kỳ việc truyền gửi dữ liệu quốc tế nào đối với Dữ liệu Cá nhân của Microsoft trừ khi Microsoft đưa ra chấp thuận trước bằng văn bản và trong mọi trường hợp, nhà cung cấp phải tuân thủ Yêu cầu Bảo vệ Dữ liệu này, bao gồm các Điều khoản Hợp đồng Tiêu chuẩn, hoặc theo quyết định của Microsoft, các cơ chế truyền gửi xuyên biên giới thích hợp khác được phê duyệt bởi cơ quan bảo vệ dữ liệu thích hợp hoặc Ủy ban Châu Âu, nếu có, và được Microsoft thông qua hoặc đồng ý. Các Điều khoản Hợp đồng Tiêu chuẩn của Bên kế thừa được thông qua bởi (i) Ủy ban Châu Âu hoặc được Cơ quan Giám sát Bảo vệ Dữ liệu Châu Âu thông qua và được Ủy ban Châu Âu phê duyệt, (ii) Vương quốc Anh chiếu theo Đạo luật chung về Bảo vệ Dữ liệu Liên bang của Vương quốc Anh, (iii) Thụy Sĩ theo Đạo luật Bảo vệ Dữ liệu Liên bang Thụy Sĩ, hoặc (iv) các điều khoản điều chỉnh việc truyền gửi dữ liệu cá nhân ra quốc tế được chính phủ chính thức thông qua tại một vùng tài phán khác ngoài Thụy Sĩ, Vương quốc Anh và các vùng tài phán bao gồm Liên minh Châu Âu / Khu vực Kinh tế Châu Âu, sẽ được hợp nhất và có tính ràng buộc đối với Nhà cung cấp kể từ ngày họ thông qua. Nhà cung cấp cũng phải đảm bảo rằng bất kỳ và tất cả các bên xử lý phụ (như được định nghĩa trong Điều khoản Hợp đồng Tiêu chuẩn) cũng phải tuân thủ.

Định nghĩa quan trọng

Các thuật ngữ sau đây được sử dụng trong DPR này có ý nghĩa như sau. Danh sách các ví dụ theo sau từ "bao gồm", "chẳng hạn như", "ví dụ như", "ví dụ", "thí dụ", hoặc tương tự được sử dụng trong toàn bộ DPR này được hiểu là bao gồm "không có giới hạn" hoặc "nhưng không giới hạn ở" trừ khi quy định rõ bởi các từ như "chỉ" hoặc "duy nhất". Để biết thêm các định nghĩa, vui lòng xem Bảng chú giải thuật ngữ ở cuối tài liệu này.

"**Bên kiểm soát"** nghĩa là tổ chức xác định các mục đích và phương tiện của việc Xử lý Dữ liệu Cá nhân đó. "Bên kiểm soát" bao gồm Doanh nghiệp, Người kiểm soát (như được định nghĩa trong GDPR) và các thuật ngữ tương đương trong Luật Bảo vệ Dữ liệu, tùy theo ngữ cảnh yêu cầu.

"**Cookie**" là các tệp văn bản nhỏ được các trang web và/hoặc ứng dụng lưu trữ trên các thiết bị nhằm chứa các thông tin dùng để nhận dạng Chủ thể Dữ liệu hoặc thiết bị.

"**Sự cố dữ liệu**" có nghĩa là (1) vi phạm bảo mật dẫn đến việc vô tình hoặc bất hợp pháp phá hủy, làm mất, thay đổi, tiết lộ hoặc truy cập trái phép vào Dữ liệu Cá nhân của Microsoft hoặc Dữ liệu Bảo mật của Microsoft được truyền gửi, lưu trữ hoặc được Nhà cung cấp hay Nhà thầu phụ của họ xử lý theo cách khác, hoặc (2) lỗ hổng bảo mật liên quan đến việc Nhà cung cấp xử lý Dữ liệu Cá nhân của Microsoft hoặc Dữ liệu Bảo mật của Microsoft.

"**Chủ thể Dữ liệu**" có nghĩa là một thể nhân có thể nhận dạng được, có khả năng được xác định một cách trực tiếp hay gián tiếp, cụ thể là bằng cách tham khảo một yếu tố nhận dạng như họ tên, số căn cước, dữ liệu định vị, một mã định danh trực tuyến hoặc khi tham khảo một hoặc nhiều yếu tố cụ thể theo thông tin nhận dạng về thể chất, sinh lý, di truyền, tâm thần, kinh tế, văn hóa hoặc xã hội của thể nhân đó.

"**Quyền Chủ thể Dữ liệu**" nghĩa là quyền của Chủ thể dữ liệu được tiếp cận, xóa bỏ, chỉnh sửa, xuất ra, hạn chế hoặc phản đối việc Microsoft Xử lý Dữ liệu Cá nhân của Chủ thể Dữ liệu đó nếu Pháp luật yêu cầu.

"**Luật**" có nghĩa là tất cả các luật, quy tắc, quy chế, nghị định, quyết định, lệnh, quy định, bản án, quy chuẩn, ban hành, nghị quyết và các yêu cầu hiện hành của bất kỳ cơ quan chính phủ nào (liên bang, tiểu bang, địa phương hoặc quốc tế) có quyền tài phán. "**Bất hợp pháp**" có nghĩa là bất kỳ hành vi nào vi phạm Pháp luật.

"**Dữ liệu Bảo mật của Microsoft**" là bất kỳ thông tin nào có thể dẫn đến tổn thất tài chính hoặc uy tín đáng kể cho Microsoft nếu bị xâm phạm thông qua những biện pháp về bảo mật hoặc tính toàn vẹn. Nội dung này bao gồm các sản phẩm phần cứng và phần mềm của Microsoft, các ứng dụng nghiệp vụ nội bộ, các tài liệu tiếp thị trước khi 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 Cá nhân của Microsoft**" nghĩa là mọi Dữ liệu Cá nhân được xử lý bởi hoặc thay mặt cho Microsoft.

"**Dữ liệu Cá nhân**" nghĩa là mọi thông tin liên quan đến Chủ thể Dữ liệu và bất kỳ thông tin nào khác cấu thành "dữ liệu cá nhân" hoặc "thông tin cá nhân" theo Luật.

"**Quá trình**" có nghĩa là bất kỳ thao tác hoặc một loạt thao tác nào được thực hiện trên bất cứ Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật nào của Microsoft, dù bằng hoặc không bằng các phương tiện tự động, chẳng hạn như thu thập, ghi lại, tổ chức, cấu trúc, lưu trữ, điều chỉnh hoặc sửa đổi, truy xuất, tư vấn, sử dụng, tiết lộ bằng cách truyền tải, phổ biến hoặc cung cấp, điều chỉnh hay kết hợp, hạn chế, tẩy xóa hoặc phá hủy. "Đang xử lý" và "Đã xử lý" sẽ có các ý nghĩa tương ứng.

"**Bên xử lý**" có nghĩa là một pháp nhân xử lý Dữ liệu Cá nhân thay mặt cho một thực thể khác và bao gồm Nhà cung cấp Dịch vụ, Bên xử lý (như được định nghĩa trong GDPR) và các điều khoản tương đương trong Luật Bảo vệ Dữ liệu, tùy theo ngữ cảnh yêu cầu.

"**Nhà thầu phụ**" có nghĩa là bên thứ ba mà nhà cung cấp ủy quyền các nghĩa vụ của mình liên quan đến hợp đồng quy định Việc thực hiện của họ, bao gồm cả công ty liên kết của nhà cung cấp không ký hợp đồng trực tiếp với Microsoft.

"**Bên xử lý phụ**" có nghĩa là bên thứ ba mà Microsoft đưa vào để Thực hiện, trong đó Việc thực hiện bao gồm Xử lý Dữ liệu Cá nhân của Microsoft mà Microsoft là Bên xử lý.

Phản hồi của Nhà cung cấp

Các nhà cung cấp xác nhận việc tuân thủ những yêu cầu này hằng năm bằng cách sử dụng dịch vụ trực tuyến do Microsoft quản lý. Vui lòng xem mục Hướng dẫn Chương trình SSPA để hiểu rõ cách thức thực hiện việc tuân thủ.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần A: Quản lý	
1	Mỗi thỏa thuận áp dụng giữa Microsoft và nhà cung cấp (ví dụ: thỏa thuận khung, thông báo nhiệm vụ, đơn mua hàng và các đơn hàng khác) có chứa các nội dung bảo vệ dữ liệu bảo mật và quyền riêng tư liên quan đến Dữ liệu Cá nhân và Dữ liệu Bảo mật của Microsoft, nếu có, bao gồm các điều khoản cấm bán Dữ liệu Cá nhân của Microsoft và cấm Xử lý Dữ liệu Cá nhân của Microsoft bên ngoài mối quan hệ kinh doanh trực tiếp giữa Microsoft và nhà cung cấp đó. Đối với các công ty hoạt động với vai trò là Bên xử lý hoặc Bên xử lý phụ liên quan đến Việc thực hiện, liên quan đến Dữ liệu Cá nhân của Microsoft, thỏa thuận đó phải bao gồm nội dung chủ yếu và thời hạn của việc Xử lý, bản chất và mục đích của việc Xử lý, loại Dữ liệu Cá nhân của Microsoft và các danh mục của Chủ thể Dữ liệu cũng như các nghĩa vụ và quyền của Microsoft.	Nhà cung cấp phải xuất trình hợp đồng hiện hành giữa Microsoft và Nhà cung cấp. Đối với Bên xử lý và Bên xử lý phụ, các mô tả về việc Xử lý được đưa vào thỏa thuận hiện hành (*ví dụ*: thông báo nhiệm vụ, đơn mua hàng). Lưu ý: Các công ty có đơn mua hàng chưa hoàn thành có thể được bổ sung bản mô tả cần thiết về các hoạt động Xử lý sau này trong quá trình mua hàng.
2	Khi Microsoft xác nhận rằng các cam kết của bạn hoàn thành vai trò Bên xử lý phụ, Nhà cung cấp phải có các thỏa thuận bảo vệ dữ liệu hiện hành với Microsoft. Lưu ý: Microsoft sẽ đăng tải nội dung chỉ định này vào hồ sơ của bạn khi điều này được áp dụng.	Các Điều khoản Hợp đồng Tiêu chuẩn, Phụ lục Dữ liệu Khách hàng Trực tuyến và/hoặc Phụ lục Xử lý Dữ liệu Dịch vụ Chuyên nghiệp của Nhà cung cấp và Đối tác.
3	Giao trách nhiệm và trách nhiệm giải trình về việc tuân thủ DPR cho một người hoặc nhóm được chỉ định trong công ty.	Đặt tên cho vai trò 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 quyền hạn và trách nhiệm giải trình của người hoặc nhóm này thể hiện được vai trò quyền riêng tư và/hoặc bảo mật.
4	Thiết lập, duy trì và thực hiện hoạt động đào tạo hàng năm về quyền riêng tư và bảo mật cho các nhân viên sẽ có quyền truy cập vào Dữ liệu Cá nhân được Xử lý bởi nhà cung cấp liên quan đến Việc thực hiện hoặc Dữ liệu Bảo mật của Microsoft. Nếu công ty của bạn không có nội dung chuẩn bị sẵn, bạn có thể sử dụng bản tóm lược nội dung và điều chỉnh tài liệu này phù hợp với công ty của bạn. Lưu ý: Nhân viên của nhà cung cấp có thể được yêu cầu hoàn thành các khóa đào tạo bổ sung do các bộ phận của Microsoft cung cấp.	Hồ sơ tham dự hàng năm luôn có sẵn và có thể được cung cấp cho Microsoft theo yêu cầu. Nội dung đào tạo bao gồm các nguyên tắc về quyền riêng tư và bảo mật. Tài liệu về việc tuân thủ có các yêu cầu đào tạo sẽ bao gồm bằng chứng về việc đào tạo liên quan đến các yêu cầu quy định về quyền riêng tư, nghĩa vụ bảo mật và việc tuân thủ các yêu cầu và nghĩa vụ hợp đồng hiện hành.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần A: Quản lý (tiếp)	
5	Chỉ xử lý Dữ liệu Cá nhân của Microsoft theo các hướng dẫn được lập thành văn bản của Microsoft, bao gồm các tình huống liên quan đến việc truyền gửi Dữ liệu Cá nhân của Microsoft đến một quốc gia thứ ba hoặc một tổ chức quốc tế, trừ khi Luật pháp yêu cầu làm vậy; trong trường hợp như vậy, Bên xử lý hoặc Bên xử lý phụ (nhà cung cấp) phải thông báo cho bên kiểm soát (Microsoft) về yêu cầu pháp lý đó trước khi Xử lý, trừ khi Luật nghiêm cấm những thông tin đó dựa trên các lý do quan trọng về lợi ích chung.	Nhà cung cấp sẽ biên soạn và duy trì tất cả các hướng dẫn bằng văn bản của Microsoft (ví dụ: thỏa thuận, thông báo nhiệm vụ hoặc tài liệu đơn hàng) dưới dạng điện tử, ở một nơi dễ tiếp cận đối với các nhân viên và nhà thầu của nhà cung cấp đang tham gia vào Việc thực hiện.
	Phần B: Thông báo	
6	Nhà cung cấp phải sử dụng Tuyên bố về Quyền riêng tư của Microsoft khi thay mặt Microsoft thu thập Dữ liệu Cá nhân. Thông báo về quyền riêng tư này phải rõ ràng và được cung cấp cho Chủ thể Dữ liệu để giúp họ quyết định có gửi Dữ liệu Cá nhân của họ cho nhà cung cấp hay không. Lưu ý: Trong trường hợp công ty của bạn là Bên kiểm soát hoạt động Xử lý, bạn sẽ đăng thông báo về quyền riêng tư của riêng mình.	Nhà cung cấp sử dụng fwdlink đến Tuyên bố về Quyền riêng tư mới nhất đã được Microsoft công bố. Tuyên bố về Quyền riêng tư được đăng tải trong bất kỳ bối cảnh nào mà Dữ liệu Cá nhân của người dùng sẽ được thu thập. Nếu có thể, một phiên bản ngoại tuyến sẽ có sẵn và được cung cấp trước khi thu thập dữ liệu. Bất kỳ Tuyên bố về Quyền riêng tư ngoại tuyến nào được sử dụng đều là phiên bản mới nhất, đã phát hành và được ghi ngày tháng chính xác. Thông báo về Quyền riêng tư Dữ liệu của Microsoft sẽ được sử dụng cho các dịch vụ dành cho nhân viên của Microsoft.
7	Khi thu thập Dữ liệu Cá nhân của Microsoft qua cuộc gọi thoại trực tiếp hoặc được ghi âm, các nhà cung cấp phải chuẩn bị để thảo luận về các phương pháp thu thập, xử lý, sử dụng và lưu giữ dữ liệu hiện hành với Chủ thể Dữ liệu.	Kịch bản cho các bản ghi âm giọng nói sẽ có chứa cách Xử lý Dữ liệu Cá nhân của Microsoft và bao gồm: ▪ việc thu thập, ▪ sử dụng và ▪ lưu giữ

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần C: Lựa chọn và Chấp thuận	
8	Nếu có thể, nhà cung cấp phải lấy được và ghi lại sự chấp thuận của Chủ thể Dữ liệu đối với tất cả các hoạt động Xử lý của mình (bao gồm mọi hoạt động Xử lý mới và được cập nhật) trước khi thu thập Dữ liệu Cá nhân của Chủ thể dữ liệu đó. Nhà cung cấp sẽ giám sát hiệu quả của việc quản lý tùy chọn nhằm đảm bảo khung thời gian để thực hiện thay đổi tùy chọn là yêu cầu pháp lý của địa phương hạn chế nhất được áp dụng.	Nhà cung cấp có thể chứng minh cách thức Chủ thể Dữ liệu đưa ra sự chấp thuận cho một hoạt động Xử lý và phạm vi của sự chấp thuận đó 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 thức Chủ thể Dữ liệu rút lại sự chấp thuận đối với hoạt động Xử lý. Nhà cung cấp có thể chứng minh cách kiểm tra các tùy chọn trước khi triển khai một hoạt động Xử lý mới. Lưu 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 các tài liệu kỹ thuật.
9	Các nhà cung cấp tạo và quản lý các trang web và/hoặc ứng dụng của Microsoft hoặc trang web mang thương hiệu Microsoft phải cung cấp cho Chủ thể Dữ liệu thông báo và lựa chọn minh bạch về việc sử dụng cookie phù hợp với các cam kết trong Tuyên bố về Quyền riêng tư của Microsoft và các yêu cầu pháp lý của địa phương. Trừ khi được đơn vị kinh doanh ký hợp đồng yêu cầu cụ thể, các nhà cung cấp nên sử dụng Biểu ngữ Tiêu chuẩn do 1ES tạo để quản lý các biện pháp kiểm soát lựa chọn. Yêu cầu này được áp dụng khi các trang web nhắm mục tiêu đến người dùng bên trong Liên minh Châu Âu/Khu vực Kinh tế Châu Âu và các khu vực khác có các luật hiện hành về quyền riêng tư cũng như bất cứ nơi nào sử dụng Tuyên bố về Quyền riêng tư của Microsoft. Lưu ý: Các nhà tài trợ kinh doanh của Microsoft bắt buộc phải đăng ký các trang web của Microsoft trong cổng thông tin Tuân thủ Web nội bộ (http://aka.ms/wcp) để được tạo danh mục và quản lý kho cookie.	Mục đích của mỗi cookie phải được lập thành văn bản và phải thông báo về loại cookie được triển khai. ▪ Không được sử dụng cookie liên tục khi có đủ cookie phiên truy cập. ▪ Khi sử dụng cookie liên tục, ngày hết hạn của các cookie này không được vượt quá 13 tháng sau khi người dùng đã truy cập trang web đó. Xác thực việc tuân thủ Luật Liên minh Châu Âu nếu có, chẳng hạn như: ▪ việc sử dụng quy ước ghi nhãn, “Quyền riêng tư & Cookie” cho tuyên bố về quyền riêng tư, ▪ đảm bảo sự chấp thuận chắc chắn của người dùng trước khi sử dụng cookie “không cần thiết” cho các mục đích như quảng cáo, và ▪ việc chấp thuận phải hết hạn hoặc được xin phép lại không quá 6 tháng một lần.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần D: Thu thập	
10	Nhà cung cấp phải giám sát việc thu thập Dữ liệu Cá nhân và/hoặc Dữ liệu Bảo mật của Microsoft để đảm bảo rằng chỉ thu thập các dữ liệu cần thiết để Thực hiện.	Nhà cung cấp có thể cung cấp tài liệu cho thấy Dữ liệu Cá nhân và/hoặc Dữ liệu Bảo mật của Microsoft được thu thập là cần thiết để Thực hiện. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
11	Trước khi thu thập dữ liệu từ trẻ em (theo định nghĩa của vùng tài phán hiện hành), Nhà cung cấp phải có được sự chấp thuận theo các luật về quyền riêng tư của địa phương.	Nhà cung cấp có thể cung cấp tài liệu thể hiện sự chấp thuận của cha mẹ/người giám hộ. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
	Phần E: Lưu giữ	
12	Đảm bảo rằng Dữ liệu Cá nhân và Dữ liệu Bảo mật của Microsoft được lưu giữ không lâu hơn mức cần thiết để Thực hiện trừ khi Luật pháp yêu cầu tiếp tục lưu giữ các Dữ liệu Cá nhân và/hoặc Dữ liệu Bảo mật của Microsoft.	Nhà cung cấp tuân thủ các chính sách lưu giữ được lập thành văn bản hoặc các yêu cầu lưu giữ do Microsoft quy định trong hợp đồng (ví dụ: thông báo nhiệm vụ, đơn mua hàng). Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
13	Đảm bảo rằng, theo quyết định riêng của Microsoft, Dữ liệu Cá nhân và Dữ liệu Bảo mật của Microsoft thuộc quyền sở hữu của nhà cung cấp hoặc dưới sự kiểm soát của họ sẽ được trả lại cho Microsoft hoặc bị tiêu hủy sau khi hoàn thành Việc thực hiện hoặc theo yêu cầu của Microsoft. Bên trong các ứng dụng, các quá trình phải được thực hiện để đảm bảo rằng khi dữ liệu bị xóa khỏi ứng dụng một cách rõ ràng bởi người dùng hoặc dựa trên các yếu tố kích hoạt khác như độ tuổi của dữ liệu, thì dữ liệu đó sẽ được xóa một cách an toàn. Khi cần thiết phải tiêu hủy Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft, nhà cung cấp phải đốt, nghiền nát hoặc cắt vụn các tài sản vật lý có chứa Dữ liệu Cá nhân và/hoặc Dữ liệu Bảo mật của Microsoft để không thể đọc hoặc tái tạo được các thông tin đó.	Duy trì hồ sơ về việc xử lý Dữ liệu Cá nhân và Dữ liệu Bảo mật của Microsoft (điều này có thể bao gồm việc trả lại cho Microsoft để tiêu hủy). Nếu Microsoft bắt buộc hoặc yêu cầu tiêu hủy, nhà cung cấp cần đưa ra chứng nhận tiêu hủy có chữ ký của nhân viên nhà cung cấp.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần F: Chủ thể Dữ liệu	
	Chủ thể Dữ liệu có một số quyền nhất định theo Luật, bao gồm quyền tiếp cận, xóa bỏ, chỉnh sửa, xuất ra, hạn chế và phản đối việc Xử lý Dữ liệu Cá nhân của họ ("**Quyền Chủ thể Dữ liệu**"). Khi một Chủ thể Dữ liệu tìm cách thực thi các quyền của họ theo Luật đối với Dữ liệu Cá nhân của Microsoft, nhà cung cấp phải cho phép Microsoft thực hiện những việc sau hoặc thực hiện những hành động này thay mặt cho Microsoft:	
14	Hỗ trợ Microsoft, thông qua các biện pháp kỹ thuật và tổ chức thích hợp, nếu có thể, để thực hiện các nghĩa vụ của mình trong việc phản hồi các yêu cầu cho Chủ thể Dữ liệu đang tìm cách thực thi Quyền Chủ thể Dữ liệu của họ mà không bị chậm trễ quá mức. Trừ khi có chỉ dẫn khác của Microsoft, Nhà cung cấp sẽ chuyển tất cả các Chủ thể Dữ liệu liên hệ trực tiếp với Nhà cung cấp đến Microsoft để thực thi các Quyền Chủ thể Dữ liệu của họ.	Nhà cung cấp sẽ lưu giữ bằng chứng về các quá trình và thủ tục được lập thành văn bản để hỗ trợ việc thực thi Quyền Chủ thể Dữ liệu. Nhà cung cấp sẽ lưu giữ bằng chứng được lập thành văn bản về việc kiểm tra. Bằng chứng sẽ được cung cấp theo yêu cầu của Microsoft.
15	Khi phản hồi trực tiếp với Chủ thể Dữ liệu hoặc khi Nhà cung cấp đưa ra cơ chế trực tuyến tự phục vụ, Nhà cung cấp có các quy trình và thủ tục để xác định được 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. Nhà cung cấp sẽ cung cấp bằng chứng bằng văn bản cho Microsoft theo yêu cầu.
16	Nếu được Microsoft yêu cầu xác định Dữ liệu Cá nhân của Microsoft về một Chủ thể Dữ liệu không có sẵn thông qua cơ chế trực tuyến tự phục vụ, Nhà cung cấp sẽ nỗ lực hợp lý để tìm các dữ liệu được yêu cầu và lưu giữ đầy đủ hồ sơ để chứng minh rằng việc tìm kiếm hợp lý đã được thực hiện.	Nhà cung cấp sẽ lưu giữ bằng chứng được lập thành văn bản về các quy trình để xác định xem Dữ liệu Cá nhân của Microsoft có đang được lưu giữ hay không và sẽ cung cấp tài liệu cho Microsoft theo yêu cầu. Nhà cung cấp lưu giữ hồ sơ thể hiện các bước được thực hiện nhằm đáp ứng các yêu cầu về Quyền Chủ thể Dữ liệu. Các tài liệu này bao gồm: ▪ ngày và giờ của yêu cầu, ▪ các hành động được thực hiện để phản hồi yêu cầu đó, và hồ sơ về thời điểm Microsoft được thông báo. Nhà cung cấp sẽ cung cấp bằng chứng về việc lưu trữ hồ sơ cho Microsoft theo yêu cầu.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần F: Chủ thể Dữ liệu (tiếp)	
17	Nhà cung cấp sẽ thông báo cho Chủ thể Dữ liệu các bước mà người đó phải thực hiện để có quyền tiếp cận hoặc thực thi các quyền của họ liên quan đến Dữ liệu Cá nhân của Microsoft.	Nhà cung cấp sẽ lưu giữ bằng chứng được lập thành văn bản về các thông tin trao đổi và thủ tục để tiếp cận Dữ liệu Cá nhân của Microsoft. Nhà cung cấp sẽ lưu giữ bằng chứng được lập thành văn bản và cung cấp bằng chứng tương tự cho Microsoft theo yêu cầu.
18	Ghi lại ngày và giờ của các yêu cầu về Quyền Chủ thể Dữ liệu cũng như các hành động mà nhà cung cấp thực hiện để phản hồi các yêu cầu đó. Nếu yêu cầu của họ bị từ chối, theo hướng dẫn của Microsoft, hãy cung cấp cho Chủ thể Dữ liệu văn bản giải thích. Cung cấp hồ sơ về các yêu cầu của Chủ thể Dữ liệu cho Microsoft khi có yêu cầu.	Nhà cung cấp lưu giữ hồ sơ về các yêu cầu tiếp cận/xóa bỏ và các thay đổi của tài liệu được thực hiện đối với Dữ liệu Cá nhân của Microsoft. Ghi lại các trường hợp yêu cầu bị từ chối và lưu lại bằng chứng về việc xem xét và phê duyệt của Microsoft. Nhà cung cấp sẽ cung cấp bằng chứng về việc lưu giữ hồ sơ các yêu cầu và việc từ chối tiếp cận Dữ liệu Cá nhân của Microsoft.
19	Nhà cung cấp phải cho phép Microsoft hoặc có được bản sao Dữ liệu Cá nhân của Microsoft được yêu cầu cho Chủ thể Dữ liệu đã được xác thực ở định dạng bản in, điện tử hoặc lời nói thích hợp.	Nhà cung cấp sẽ cung cấp Dữ liệu Cá nhân của Microsoft cho Chủ thể Dữ liệu ở định dạng dễ hiểu và theo hình thức thuận tiện cho Chủ thể Dữ liệu và nhà cung cấp.
20	Nhà cung cấp phải thực hiện các biện pháp phòng ngừa hợp lý để đảm bảo rằng không ai có thể dùng Dữ liệu Cá nhân của Microsoft được phát hành cho Microsoft hoặc Chủ thể Dữ liệu đã xác thực để nhận dạng một người khác.	Nhà cung cấp sẽ lưu giữ bằng chứng được lập thành văn bản về các thủ tục liên quan đến các biện pháp phòng ngừa để tránh xác định Chủ thể Dữ liệu trái với các điều khoản Thỏa thuận. Nhà cung cấp sẽ cung cấp bằng chứng cho Microsoft theo yêu cầu.
21	Nếu một Chủ thể Dữ liệu tin rằng Dữ liệu Cá nhân của Microsoft của họ không đầy đủ và chính xác, nhà cung cấp phải báo cáo vấn đề đó với Microsoft cũng như hợp tác với Microsoft khi cần thiết để giải quyết vấn đề. Nếu nhà cung cấp có ý định sử dụng nhà thầu phụ để Xử lý Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft thì nhà cung cấp phải:	Nhà cung cấp sẽ ghi lại các trường hợp bất đồng và chuyển vấn đề lên Microsoft. Nhà cung cấp sẽ cung cấp cho Microsoft bằng chứng dạng tài liệu theo yêu cầu.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần G: Nhà thầu phụ	
22	Thông báo cho Microsoft trước khi thực hiện các dịch vụ giao thầu phụ hoặc thực hiện bất cứ thay đổi nào liên quan đến việc bổ sung hoặc thay thế các nhà thầu phụ. Lưu ý: Cho biết rằng bạn chấp nhận nghĩa vụ này ngay cả khi bạn hiện không thuê nhà thầu phụ nhưng có thể thuê họ trong tương lai.	Xác thực rằng Dữ liệu Cá nhân của Microsoft chỉ được Xử lý bởi các công ty được Microsoft biết đến theo yêu cầu trong hợp đồng hiện hành (ví dụ: thông báo nhiệm vụ, phụ lục hợp đồng, đơn mua hàng) hoặc được thu thập trong cơ sở dữ liệu SSPA. Nhà cung cấp có thể đăng tải danh sách nhà thầu phụ của họ trực tuyến và bao gồm một liên kết dẫn đến trang đó trong cơ sở dữ liệu SSPA.
23	Ghi lại tính chất và mức độ của Dữ liệu Bảo mật và Dữ liệu Cá nhân của Microsoft do các nhà thầu phụ Xử lý, đảm bảo rằng thông tin thu thập được là cần thiết để Thực hiện.	Nhà cung cấp lưu giữ tài liệu liên quan đến Dữ liệu Cá nhân và Dữ liệu Bảo mật của Microsoft được tiết lộ hoặc chuyển giao cho các nhà thầu phụ. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
24	Trong trường hợp Microsoft là bên kiểm soát Dữ liệu Cá nhân của Microsoft, hãy đảm bảo nhà thầu phụ sử dụng Dữ liệu Cá nhân của Microsoft phù hợp với các tùy chọn liên lạc đã nêu của Chủ thể Dữ liệu.	Chứng minh cách các nhà thầu phụ sử dụng tùy chọn Chủ thể Dữ liệu Microsoft. Cung cấp tài liệu hỗ trợ (ví dụ: ảnh chụp màn hình, SLA, SOW, v.v.) bao gồm khung thời gian để nhà thầu phụ thực hiện thay đổi tùy chọn.
25	Giới hạn việc nhà thầu phụ Xử lý Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft theo những mục đích cần thiết để hoàn thành hợp đồng của nhà cung cấp với Microsoft.	Nhà cung cấp có thể cung cấp tài liệu cho thấy Dữ liệu Cá nhân của Microsoft được cung cấp cho nhà thầu phụ là cần thiết để Thực hiện. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
26	Xem xét các khiếu nại để biết các dấu hiệu về bất cứ hoạt động Xử lý trái phép hoặc bất hợp pháp Dữ liệu Cá nhân của Microsoft.	Nhà cung cấp có thể chứng minh các hệ thống và quy trình được cung cấp để giải quyết các khiếu nại liên quan đến việc nhà thầu phụ sử dụng hoặc tiết lộ trái phép Dữ liệu Cá nhân của Microsoft. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần G: Nhà thầu phụ (tiếp)	
27	Thông báo ngay cho Microsoft khi biết rằng một nhà thầu phụ đã Xử lý Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft cho bất kỳ mục đích nào khác ngoài mục đích liên quan đến Việc thực hiện.	Nhà cung cấp đã đưa ra hướng dẫn và phương tiện để nhà thầu phụ báo cáo việc sử dụng sai dữ liệu của Microsoft. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
28	Nếu nhà cung cấp thu thập Dữ liệu Cá nhân từ các bên thứ ba thay mặt cho Microsoft thì nhà cung cấp đó phải xác thực rằng các chính sách và thông lệ bảo vệ dữ liệu của bên thứ ba đó phù hợp với hợp đồng của nhà cung cấp với Microsoft và DPR này.	Nhà cung cấp có thể cung cấp tài liệu về quá trình thẩm định được thực hiện liên quan đến các chính sách và thông lệ bảo vệ dữ liệu của bên thứ ba. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
29	Kịp thời thực hiện các hành động để giảm thiểu bất kỳ tác hại thực tế hoặc tiềm ẩn nào gây ra bởi việc nhà thầu phụ Xử lý trái phép hoặc bất hợp pháp Dữ liệu Bảo mật và Dữ liệu Cá nhân của Microsoft.	Nhà cung cấp phải lưu giữ bằng chứng tài liệu về kế hoạch và quy trình cũng như cung cấp bằng chứng tài liệu cho Microsoft khi có yêu cầu.
	Phần H: Chất lượng	
30	Nhà cung cấp phải duy trì tính toàn vẹn của tất cả Dữ liệu Cá nhân của Microsoft, đảm bảo dữ liệu đó vẫn chính xác, đầy đủ và phù hợp với các mục đích Xử lý dữ liệu đã nêu.	Nhà cung cấp có thể chứng minh rằng các thủ tục được áp dụng để xác thực Dữ liệu Cá nhân của Microsoft khi dữ liệu đó được thu thập, tạo ra và cập nhật. Nhà cung cấp có thể chứng minh rằng luôn có sẵn các thủ tục giám sát và lấy mẫu để xác minh tính chính xác trên cơ sở thường xuyên và sửa chữa khi cần thiết. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần I: Giám sát và Thực thi	
31	Nhà cung cấp có kế hoạch ứng phó sự cố trong đó yêu cầu Nhà cung cấp thông báo cho Microsoft theo các quy định của hợp đồng hoặc không chậm trễ quá mức, tùy thời điểm nào sớm hơn, khi phát hiện ra Sự cố Dữ liệu. Theo yêu cầu hoặc chỉ đạo của Microsoft, Nhà cung cấp phải hợp tác với Microsoft trong mọi cuộc điều tra, giảm nhẹ hoặc khắc phục Sự cố, bao gồm việc cung cấp cho Microsoft dữ liệu, thông tin, quyền tiếp cận nhân viên của Nhà cung cấp hoặc cung cấp phần cứng cần thiết để tiến hành đánh giá điều tra. Lưu ý: Xin vui lòng xem Hướng dẫn Chương trình SSPA để biết cách thông báo cho Microsoft về sự cố.	Nhà cung cấp có kế hoạch ứng phó sự cố bao gồm bước thông báo cho khách hàng (Microsoft) như được mô tả trong phần này. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
32	Thực hiện kế hoạch khắc phục và theo dõi việc giải quyết từng Sự cố Dữ liệu để đảm bảo rằng hành động khắc phục thích hợp được thực hiện kịp thời.	Nhà cung cấp đã ghi lại các thủ tục sẽ thực hiện để ứng phó với Sự cố Dữ liệu cho đến khi kết thúc. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.
33	Trong trường hợp Microsoft là bên kiểm soát Dữ liệu Cá nhân của Microsoft, hãy thiết lập một quy trình xử lý khiếu nại chính thức để phản hồi tất cả các khiếu nại về bảo vệ dữ liệu liên quan đến Dữ liệu Cá nhân của Microsoft.	Nhà cung cấp có phương tiện tiếp nhận các khiếu nại liên quan đến Dữ liệu Cá nhân của Microsoft và có quy trình xử lý khiếu nại được lập thành văn bản để giải quyết khiếu nại. Nhà cung cấp sẽ cung cấp bằng chứng dạng tài liệu cho Microsoft theo yêu cầu.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần J: Bảo mật	
	Nhà cung cấp phải thiết lập, triển khai và duy trì một chương trình bảo mật thông tin bao gồm các chính sách và thủ tục, nhằm bảo vệ và lưu giữ an toàn các Dữ liệu Bảo mật và Dữ liệu Cá nhân của Microsoft theo thông lệ đạt chuẩn của ngành cũng như theo yêu cầu của Luật pháp. Chương trình bảo mật của nhà cung cấp phải đáp ứng các tiêu chuẩn được quy định dưới đây, các yêu cầu 34-50.	Chứng nhận ISO 27001 hợp lệ là phương án thay thế có thể chấp nhận được cho Phần J. Hãy liên hệ với SSPA để áp dụng phương án thay thế này. Lưu ý: Bạn sẽ cần cung cấp chứng nhận này.
34	Thực hiện các bài đánh giá an ninh mạng hàng năm bao gồm: ▪ xem xét các thay đổi lớn đối với môi trường, chẳng hạn như thành phần hệ thống mới, cấu trúc liên kết mạng, quy tắc tường lửa, ▪ tiến hành quét lỗ hổng bảo mật, và ▪ lưu giữ các nhật ký thay đổi.	Nhà cung cấp đã ghi lại các bài đánh giá hệ thống 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 về lý do thay đổi cũng như bao gồm tên và chức danh của người phê duyệt được chỉ định.
35	Nhà cung cấp xác định, truyền đạt và triển khai chính sách thiết bị di động nhằm bảo mật và giới hạn việc sử dụng Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft được truy cập hoặc sử dụng trên thiết bị di động.	Nhà cung cấp chứng minh việc có sử dụng chính sách thiết bị di động tuân thủ trong đó việc Xử lý Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft đòi hỏi sử dụng thiết bị di động.
36	Tất cả các tài sản được sử dụng để hỗ trợ Việc thực hiện phải được hạch toán và xác định chủ sở hữu. Nhà cung cấp phải chịu trách nhiệm về việc duy trì kiểm kê các tài sản thông tin này; thiết lập việc sử dụng tài sản được chấp nhận và được phép; và cung cấp mức độ bảo vệ thích hợp cho tài sản trong suốt vòng đời của chúng.	Bản kiểm kê nội dung các thiết bị được dùng để hỗ trợ Việc thực hiện. Bản kiểm kê các tài sản này cần bao gồm: ▪ vị trí của thiết bị, ▪ phân loại dữ liệu của dữ liệu trên tài sản đó, ▪ hồ sơ về thu hồi tài sản khi chấm dứt hợp đồng lao động hoặc công việc, và ▪ hồ sơ về việc thải bỏ phương tiện lưu trữ dữ liệu khi không còn cần thiết.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần J: Bảo mật (tiếp)	
37	Thiết lập và duy trì các quy trình quản lý quyền truy cập để ngăn chặn truy cập trái phép vào bất kỳ Dữ liệu Bảo mật hoặc Dữ liệu Cá nhân nào của Microsoft dưới sự kiểm soát của nhà cung cấp.	Nhà cung cấp chứng minh rằng họ đã thực hiện một kế hoạch quản lý quyền truy cập bao gồm: ▪ các quy trình kiểm soát truy cập, ▪ các quy trình nhận dạng, ▪ các quy trình khóa lại sau một số lần thử không thành công, ▪ các tham số hiệu quả để lựa chọn thông tin xác thực, và ▪ hủy kích hoạt tài khoản người dùng khi chấm dứt hợp đồng lao động trong vòng 48 giờ ▪ các biện pháp kiểm soát mật khẩu hữu hiệu buộc áp dụng độ dài và độ phức tạp của mật khẩu và ngăn ngừa sử dụng lại Nhà cung cấp chứng minh rằng họ có một quy trình đã thiết lập để xem xét quyền truy cập của người dùng vào Dữ liệu Cá nhân và Dữ liệu Bảo mật của Microsoft, buộc thực thi nguyên tắc đặc quyền thấp nhất. Quá trình này bao gồm: ▪ các vai trò người dùng được định nghĩa rõ ràng, ▪ các quy trình để xem xét và biện minh cho việc phê duyệt quyền truy cập vào các vai trò, và ▪ thử nghiệm xem người dùng trong các vai trò có quyền truy cập vào dữ liệu Microsoft có xác minh đã được ghi chép theo dõi lại cho việc tham gia vào nhóm/vai trò đó hay không.
38	Xác định và triển khai các quy trình quản lý bản vá nhằm ưu tiên các bản vá bảo mật cho các hệ thống được sử dụng để Xử lý Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft. Các quy trình này bao gồm: ▪ cách tiếp cận rủi ro đã xác định 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 bất cứ trường hợp ngoại lệ nào, và ▪ các yêu cầu về việc loại bỏ phần mềm không còn được công ty sản xuất phần mềm hỗ trợ.	Nhà cung cấp có thể chứng minh một quy trình quản lý bản vá đã thực hiện có đáp ứng yêu cầu này và tối thiểu bao gồm các nội dung sau: ▪ Chỉ định mức độ nghiêm trọng để thông báo mức độ ưu tiên. (Định nghĩa về mức độ nghiêm trọng được ghi chép theo dõi.) ▪ Quy trình triển khai các bản vá khẩn cấp được ghi chép theo dõi. ▪ Xác nhận không sử dụng hệ điều hành không còn được hỗ trợ bởi công ty sản xuất hệ điều hành. ▪ Hồ sơ quản lý bản vá nhằm theo dõi các lần phê duyệt và trường hợp ngoại lệ.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần J: Bảo mật (tiếp)	
39	Cài đặt phần mềm chống vi-rút và chống phần mềm độc hại trên thiết bị được kết nối với mạng lưới được dùng để Xử lý Dữ liệu Bảo mật và Dữ liệu Cá nhân của Microsoft, bao gồm máy chủ, máy tính để bàn sản xuất và đào tạo để bảo vệ khỏi vi-rút có hại tiềm ẩn và các ứng dụng phần mềm độc hại. Cập nhật các định nghĩa chống phần mềm độc hại hàng ngày hoặc theo chỉ dẫn của nhà cung cấp phần mềm chống vi-rút/phần mềm độc hại. Lưu ý: Quy định này áp dụng cho mọi hệ điều hành bao gồm Linux.	Hồ sơ tồn tại cho thấy việc sử dụng phần mềm chống vi-rút và chống phần mềm độc hại đang hoạt động. Lưu ý: Yêu cầu này áp dụng cho tất cả các hệ điều hành.
40	Các nhà cung cấp phát triển phần mềm cho Microsoft phải kết hợp các nguyên tắc bảo mật theo thiết kế trong quá trình xây dựng phần mềm.	Các tài liệu thông số kỹ thuật của nhà cung cấp bao gồm các điểm kiểm tra để xác nhận tính bảo mật trong các chu kỳ phát triển của họ.
41	Sử dụng chương trình Phòng chống Mất Dữ liệu ("**DLP**") để ngăn chặn sự xâm nhập, mất mát và các hoạt động trái phép khác. Dữ liệu phải được phân loại, ghi nhãn và bảo vệ thích hợp và nhà cung cấp phải giám sát các hệ thống thông tin đang được sử dụng trong đó Xử lý các Dữ liệu Bảo mật hoặc Dữ liệu Cá nhân của Microsoft nhằm phát hiện xâm nhập, mất mát và hoạt động trái phép khác. Chương trình DLP, ở mức tối thiểu: ▪ yêu cầu việc sử dụng máy chủ lưu trữ, mạng và Hệ thống Phát hiện Xâm nhập ("**IDS**") trên nền đám mây theo tiêu chuẩn của ngành nếu bạn giữ lại Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft, ▪ yêu cầu triển khai Hệ thống Bảo vệ Chống xâm nhập ("**IPS**") tiên tiến được cấu hình để theo dõi và chủ động ngăn ngừa mất dữ liệu, ▪ trong trường hợp hệ thống bị xâm phạm, sẽ yêu cầu phân tích hệ thống để đảm bảo mọi lỗ hổng còn sót lại cũng được giải quyết, ▪ mô tả các quy trình cần thiết để giám sát các công cụ phát hiện xâm phạm hệ thống, ▪ thiết lập một quy trình quản lý và ứng phó sự cố bắt buộc phải thực hiện khi phát hiện được Sự cố Dữ liệu, và ▪ yêu cầu việc trao đổi thông tin (với tất cả nhân viên của nhà cung cấp và nhà thầu phụ đang được đưa ra ngoài Việc thực hiện của nhà cung cấp) đối với	Chương trình DLP lập thành văn bản được triển khai với các quy trình tại chỗ để ngăn chặn sự xâm nhập, mất mát và hoạt động trái phép khác (và ở mức tối thiểu là tất cả các mục được quy định trong phần này).

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần J: Bảo mật (tiếp)	
	việc tải về và sử dụng trái phép Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft.	
42	Thông báo kịp thời các kết quả Điều tra từ quá trình ứng phó sự cố cho quản lý cấp cao và cho Microsoft.	Các hệ thống và quy trình phải có sẵn để thông báo kết quả điều tra ứng phó sự cố cho Microsoft.
43	Quản trị viên hệ thống, nhân viên vận hành, ban giám đốc và các bên thứ ba phải trải qua khóa đào tạo bảo mật hàng năm.	Thiết lập một chương trình đào tạo bảo mật bao gồm: ▪ đào tạo hàng năm để ứng phó sự cố, và ▪ các sự kiện mô phỏng và cơ chế tự động để tạo điều kiện ứng phó hiệu quả với các tình huống khủng hoảng. ▪ Nhận thức về phòng ngừa sự cố chẳng hạn như rủi ro liên quan đến việc tải về phần mềm độc hại.
44	Nhà cung cấp phải đảm bảo rằng các quy trình lập kế hoạch sao lưu sẽ bảo vệ Dữ liệu Bảo mật và Dữ liệu Cá nhân của Microsoft khỏi việc sử dụng, truy cập, tiết lộ, thay đổi và tiêu hủy trái phép.	Nhà cung cấp có thể chứng minh các quy trình ứng phó và phục hồi được lập thành văn bản có nêu chi tiết cách tổ chức sẽ kiểm soát một sự kiện gây gián đoạn và sẽ duy trì tính bảo mật thông tin của mình ở mức độ xác định sẵn dựa trên các mục tiêu về tính liên tục bảo mật thông tin đã được ban lãnh đạo phê duyệt. Nhà cung cấp có thể chứng minh rằng họ đã xác định và thực hiện các quy trình để sao lưu định kỳ, lưu trữ an toàn và khôi phục hiệu quả các dữ liệu quan trọng.
45	Thiết lập và kiểm tra tính liên tục của hoạt động kinh doanh và các kế hoạch phục hồi sau thảm họa.	Một kế hoạch khắc phục sau thảm họa phải bao gồm các nội dung sau: ▪ Các tiêu chí được định nghĩa để xác định xem một hệ thống có tối quan trọng đối với hoạt động kinh doanh của nhà cung cấp hay không. ▪ Liệt kê các hệ thống tối quan trọng dựa trên các tiêu chí đã định nghĩa phải được nhắm mục tiêu nhằm khôi phục trong trường hợp xảy ra thảm họa. ▪ Quy trình khôi phục sau thảm họa được xác định cho từng hệ thống tối quan trọng nhằm đảm bảo một kỹ sư không biết rõ về hệ thống có thể khôi phục ứng dụng trong vòng chưa đầy 72 giờ. ▪ Kiểm tra hàng năm (hoặc thường xuyên hơn) và xem xét các kế hoạch phục hồi sau thảm họa để đảm bảo có thể đáp ứng các mục tiêu phục hồi.
46	Xác thực danh tính của một cá nhân trước khi cấp cho cá nhân đó quyền truy cập vào Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft và đảm bảo rằng quyền	Đảm bảo rằng tất cả ID người dùng đều là duy nhất và mỗi ID đều có phương pháp xác thực theo tiêu chuẩn ngành, chẳng hạn như Azure Active Directory.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần J: Bảo mật (tiếp)	
	truy cập đó bị giới hạn trong phạm vi hoạt động của cá nhân cụ thể được phép hỗ trợ Việc thực hiện.	Quyền truy cập nâng cao (quản trị hoặc các loại đặc quyền nâng cao khác) phải yêu cầu việc sử dụng yếu tố thứ hai, chẳng hạn như thẻ thông minh hoặc công cụ xác thực trên điện thoại. Chương trình bảo mật thông tin được lập thành văn bản bao gồm quy trình đảm bảo rằng tất cả nhân viên của nhà cung cấp và nhà thầu phụ truy cập vào Dữ liệu Bảo mật hoặc Dữ liệu Cá nhân của Microsoft không nhiều hơn hoặc lâu hơn mức cần thiết để hỗ trợ Việc thực hiện.
47	Nhà cung cấp phải bảo vệ tất cả dữ liệu được Xử lý liên quan đến Việc thực hiện của mình khi truyền qua các hệ thống mạng bằng mã hóa 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 một tiêu chuẩn ngành tương đương. Nhà cung cấp phải từ chối cung cấp bất kỳ Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật nào của Microsoft được truyền tải qua các phương tiện không được mã hóa.	Quá trình tạo ra, triển khai và thay thế TLS hoặc các chứng chỉ khác phải được xác định và buộc thực thi.
48	Tất cả các 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 Bảo mật của Microsoft đều phải sử dụng mã hóa dựa trên ổ đĩa.	Mã hóa tất cả các thiết bị để đáp ứng chuẩn BitLocker hoặc một giải pháp mã hóa ổ đĩa tương đương khác trong ngành cho tất cả các thiết bị máy khách được dùng để xử lý Dữ liệu Cá nhân hoặc Dữ liệu Bảo mật của Microsoft.
49	Các hệ thống và quy trình (sử dụng các tiêu chuẩn ngành hiện hành như được mô tả trong tiêu chuẩn **NIST 800-111**) đều phải sẵn sàng mã hóa ở trạng thái nghỉ (khi được lưu trữ) bất kỳ và tất cả Dữ liệu Cá nhân và/hoặc Dữ liệu Bảo mật của Microsoft, các ví dụ bao gồm nhưng không giới hạn ở: ▪ dữ liệu thông tin xác thực (ví dụ: tên người dùng/mật khẩu) ▪ dữ liệu công cụ thanh toán (ví dụ: thẻ tín dụng và số tài khoản ngân hàng) ▪ dữ liệu cá nhân liên quan đến nhập cư	Kiểm tra xem Dữ liệu Cá nhân và Dữ liệu Bảo mật của Microsoft đã được mã hóa ở chế độ nghỉ chưa.

#	Yêu cầu Bảo vệ Dữ liệu dành cho Nhà cung cấp của Microsoft	Bằng chứng Tuân thủ
	Phần J: Bảo mật (tiếp)	
	▪ dữ liệu hồ sơ y tế (ví dụ: mã số hồ sơ y tế hoặc dấu ấn hay nhận dạng sinh trắc học, chẳng hạn như DNA, dấu vân tay, võng mạc mắt và mống mắt, mẫu hình giọng nói, mẫu khuôn mặt và số đo bàn tay, được sử dụng cho mục đích xác thực) ▪ dữ liệu mã số định danh do chính phủ cấp (ví dụ: số an sinh xã hội hoặc số giấy phép lái xe) ▪ dữ liệu thuộc về khách hàng của Microsoft (ví dụ: SharePoint, tài liệu O365, khách hàng dịch vụ OneDrive) ▪ tài liệu liên quan đến các sản phẩm không được công bố của Microsoft ▪ Ngày sinh ▪ Thông tin hồ sơ trẻ em ▪ dữ liệu địa lý theo thời gian thực ▪ địa chỉ thực của cá nhân (không phải doanh nghiệp) ▪ số điện thoại cá nhân (không phải doanh nghiệp) ▪ tôn giáo ▪ quan điểm chính trị ▪ xu hướng/sở thích tình dục ▪ câu trả lời cho câu hỏi bảo mật (ví dụ: xác thực 2 yếu tố, đặt lại mật khẩu) ▪ tên thời con gái của người mẹ	
50	Ẩn danh tất cả Dữ liệu Cá nhân của Microsoft được sử dụng trong môi trường phát triển hoặc thử nghiệm.	Không được phép sử dụng Dữ liệu Cá nhân của Microsoft trong môi trường phát triển hoặc thử nghiệm; khi không có giải pháp nào thay thế, dữ liệu này phải được ẩn danh để ngăn chặn việc nhận dạng được Chủ thể Dữ liệu hoặc sử dụng sai Dữ liệu Cá nhân. Lưu ý: Dữ liệu ẩn danh sẽ khác với Dữ liệu giả danh. Dữ liệu ẩn danh là dữ liệu không liên quan đến một thể nhân được xác định hoặc có thể nhận dạng được trong đó chủ thể dữ liệu của dữ liệu cá nhân đó không thể hoặc không còn nhận dạng được nữa.

Bảng chú giải

“Đại diện được ủy quyền” là người có thẩm quyền phù hợp để ký kết thay mặt công ty. Người này sẽ có kiến thức cần thiết về quyền riêng tư và bảo mật hoặc đã tham khảo ý kiến của một chuyên gia về vấn đề quan trọng trước khi gửi phản hồi của họ cho một hành động của Chương trình SSPA. Ngoài ra, bằng cách thêm tên của họ vào biểu mẫu SSPA, họ chứng nhận rằng họ đã đọc và hiểu rõ DPR này.

“EUDPR” có nghĩa là Quy định (EU) 2018/1725 của Nghị viện Châu Âu và của Hội đồng ngày 23 tháng 10 năm 2018 về bảo vệ thể nhân liên quan đến việc xử lý dữ liệu cá nhân của các tổ chức, cơ quan, văn phòng và đại lý của Liên minh, và về việc di chuyển tự do dữ liệu đó và bãi bỏ Quy định (EC) số 45/2001 và Quyết định số 1247/2002/EC.

“Người làm nghề tự do” nghĩa là các cá nhân thực hiện các nhiệm vụ hoặc dịch vụ theo yêu cầu, có được thông qua các nền tảng kỹ thuật số hoặc các phương tiện khác.

“GDPR” có nghĩa là Quy định (EU) 2016/679 của Nghị viện Châu Âu và của Hội đồng ngày 27 tháng 4 năm 2016 về bảo vệ thể nhân liên quan đến việc xử lý dữ liệu cá nhân và di chuyển tự do dữ liệu đó và bãi bỏ Chỉ thị 95/46/EC (Quy định chung về Bảo vệ Dữ liệu).

“Yêu cầu Bảo vệ Dữ liệu Quyền riêng tư” nghĩa là GDPR, EUDPR, Luật Bảo vệ Dữ liệu Địa phương của EU/EEA, Đạo luật về Quyền riêng tư của Người tiêu dùng của California, Bộ luật Dân sự California § 1798.100 và theo đó (“*CCPA*”), Đạo luật Bảo vệ Dữ liệu của Vương quốc Anh năm 2018 và bất kỳ luật, quy định và yêu cầu pháp lý nào khác có liên quan hoặc tiếp theo áp dụng ở Vương quốc Anh, cũng như mọi luật, quy định hiện hành và các yêu cầu pháp lý khác liên quan đến (a) quyền riêng tư và bảo mật dữ liệu; hoặc (b) việc sử dụng, thu thập, lưu giữ, lưu trữ, bảo mật, tiết lộ, chuyển giao, thải bỏ và xử lý bất kỳ Dữ liệu Cá nhân nào khác.

“Điều khoản Mẫu của Liên minh Châu Âu” và “Điều khoản Hợp đồng Tiêu chuẩn” nghĩa là (i) các điều khoản bảo vệ dữ liệu tiêu chuẩn đối với việc truyền gửi dữ liệu cá nhân đến các bên xử lý được thiết lập ở các quốc gia thứ ba không đảm bảo mức độ bảo vệ dữ liệu thích hợp, như được mô tả trong Điều 46 của GDPR và được phê duyệt bởi quyết định của Ủy ban Châu Âu (EU) 2021/914 ngày 4 tháng 6 năm 2021; (ii) bất kỳ điều khoản hợp đồng tiêu chuẩn bên kế thừa nào được thông qua bởi (a) Ủy ban Châu Âu, (b) Cơ quan Giám sát Bảo vệ Dữ liệu Châu Âu và được Ủy ban Châu Âu phê duyệt, (c) Vương quốc Anh chiếu theo Đạo luật chung về Bảo vệ Dữ liệu Liên bang của Vương quốc Anh, (d) Thụy Sĩ theo Đạo luật Bảo vệ Dữ liệu Liên bang Thụy Sĩ, hoặc (e) bởi chính phủ ở vùng tài phán khác ngoài Thụy Sĩ, Vương quốc Anh và các vùng tài phán bao gồm Liên minh Châu Âu / Khu vực Kinh tế Châu Âu nơi các điều khoản chi phối việc truyền gửi dữ liệu cá nhân ra quốc tế, sẽ được hợp nhất và có tính ràng buộc đối với Nhà cung cấp kể từ ngày họ thông qua.

“Lưu trữ trang web” Dịch vụ lưu trữ trang web là một dịch vụ trực tuyến nhằm tạo và/hoặc duy trì các trang web thay mặt cho Microsoft theo tên miền của Microsoft, tức là nhà cung cấp sẽ cung cấp tất cả các tài liệu và dịch vụ cần thiết để họ tạo lập và duy trì một trang web và khiến cho nó có thể truy cập được trên internet. “Nhà cung cấp dịch vụ lưu trữ web” hoặc “máy chủ lưu trữ web” là nhà cung cấp mà sẽ cung cấp các công cụ và dịch vụ cần thiết cho trang web hoặc trang được xem trên Internet, chẳng hạn như Cookie hoặc đèn hiệu web cho quảng cáo.