Microsoft 공급자 데이터 보호 요건

적용성

Microsoft 공급자 데이터 보호 요건("**DPR**")은 Microsoft와 체결한 계약(예: 구매 주문 약관, 기본 계약서)의 용어(이하 "**수행하다**", "**수행 중**" 또는 "**업무 수행**")에 따라 해당 공급자의 업무 수행(예: 서비스, 소프트웨어 라이선스, 클라우드 서비스 제공)과 관련하여 Microsoft 개인 데이터 또는 Microsoft 기밀 데이터를 처리하는 각 Microsoft 공급자에 적용됩니다.

- DPR의 요건과 공급자 및 Microsoft 간의 계약에 명시된 요건이 상충하는 경우에는 DPR이 우선합니다. 단, 공급자가 해당 데이터 보호 요건을 대체하는 올바른 계약 조항을 확인한 경우는 제외됩니다(이 경우 계약 조항이 우선함).
- 본 문서에 포함된 요건과 법적 또는 법령 요건이 상충하는 경우 법적 또는 법령 요건이 우선합니다.
- Microsoft 공급자가 컨트롤러의 역할을 하는 경우, 공급자는 DPR 요건을 축소할 수 있습니다.
- Microsoft 공급자가 Microsoft 개인 데이터를 처리하지 않고 Microsoft 기밀 데이터만 처리하는 경우, 본 DPR과 관련하여 공급자의 요건이 축소될 수 있습니다.
- DPR의 섹션 K는 AI 시스템을 포함하여 Microsoft에 서비스를 제공하는 공급자에게만 적용됩니다.

데이터의 국외 이전

공급자는 Microsoft가 사전에 서면 승인을 제공하지 않은 이상 Microsoft 개인 데이터를 국외로 이전하지 않으며, 이는 공급자의 다른 의무를 제한하지 않습니다. 또한 공급자는 어떠한 경우에도 데이터 보호 요건을 준수해야 하며, 여기에는 표준계약조항 또는 Microsoft의 재량에 따라 해당 데이터 보호 기관이나 유럽집행위원회(European Commission)에서 승인하고, 해당되는 경우
Microsoft가 채택 또는 동의한 기타 적절한 국외 이전 절차가 포함됩니다. (i) 유럽집행위원회에서 채택하거나 유럽데이터보호감독기구(European Data Protection Supervisor)가 채택하고 유럽집행위원회, (ii) 영국 일반 연방데이터보호법(General Federal Data Protection Act)에 따라 영국, (iii) 스위스연방데이터보호법(Swiss Federal Data Protection Act)에 따라 스위스에서 채택한 후속 표준계약조항 또는 (iv) 스위스, 영국 및 유럽연합/유럽경제지역(European Economic Area)을 구성하는 관할권 이외의 관할권 내 정부에서 공식 채택한 개인 데이터의 국외 이전을 규율하는 조항이 포함되어야 하며 채택일을 기준으로 공급자에게 법적 구속력이 있습니다. 공급자는 또한 모든 하위 처리자(표준계약조항에 정의됨)도 이를 준수하도록 해야 합니다.

주요 정의

본 DPR에서 사용하는 용어와 그 의미는 다음과 같습니다. 본 DPR 전체에 사용된 "포함하는", "~와/과 같은", "예", "예를 들어" 등의 예시 목록은 "오직" 또는 "오로지"와 같은 단어로 단정되는 경우를 제외하고 "제약 없이" 또는 "이에 국한되지 않고"를 포함하는 것으로 이해됩니다. 자세한 정의는 본 문서 후반부에 수록된 용어집을 참조하십시오.

“**AI 시스템(AI Systems)**”이란 시스템이 인간에 의해 정의된 특정한 목적 세트를 위해 시스템이 상호작용하는 환경에 영향을 미치도록 예측하거나*, 권고하거나 결정할 수 있는 최적화된 모델에 적용되는 공학적 시스템을 말합니다. 이러한 시스템은 다양한 자동화 수준과 함께 작동합니다. *예측이란 다양한 종류의 데이터 분석 또는 생성(문장의 번역, 합성 이미지의 생성 또는 이전 전력 장애의 진단)을 지칭할 수 있습니다.

"**컨트롤러(Controller)**"란 개인 데이터 처리의 목적과 수단을 결정하는 주체를 말합니다. "컨트롤러"에는 기업, 컨트롤러(GDPR에 정의된 용어) 및 맥락에 따라 데이터보호법 내의 이에 준하는 용어가 포함됩니다.

"**쿠키(Cookies)**"란 데이터 주체 또는 장치를 인식하는 데 사용되는 정보가 포함된 웹사이트 및/또는 애플리케이션이 장치에 저장하는 작은 텍스트 파일입니다.

"**데이터 사고(Data Incident)**"란 (1) 공급자 또는 그 하도급업자가 전송, 저장 또는 다른 방식으로 처리한 Microsoft 개인 데이터 또는 Microsoft 기밀 데이터의
우발적이거나 불법적인 파괴, 손실, 변경, 무단 공개 또는 액세스로 이어질 수 있는 보안 침해, 또는 (2) Microsoft 개인 데이터 또는 Microsoft 기밀 데이터에 대한 공급자 처리와 관련된 보안 취약성 또는
캐나다 법안 64(2021년, 25장)에 정의된 기밀 사고를 의미합니다.

"**데이터 주체(Data Subject)**"란 특히 성명, 식별 번호, 위치 데이터, 온라인 식별자와 같은 식별자를 참조하거나 해당 자연인의 신체적, 생리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성과 관련된 특정한 하나 이상의 요소를 참조하여 직간접적으로 알아볼 수 있는 식별 가능한 자연인을 말합니다.

"**데이터 주체의 권리(Data Subject Right)**"란 법률에서 요구하는 경우 해당 데이터 주체의 Microsoft 개인 데이터 처리의
접근, 삭제, 편집, 이전, 제한 또는 반대할 수 있는 데이터 주체의 권리를 말합니다.

“**의도된 사용(Intended Uses)**”이란 고객, 공급자 또는 최종 사용자가 시스템을 사용할 것으로 기대되는 기본 목적입니다. 이는 단일 사용 또는 다중 사용 시스템에서의 다중 사용이 될 수 있습니다.

"**법률(Law)**"이란 관할권이 있는 모든 정부 기관(연방, 주, 지역 또는 해외)의 모든 관련 법률, 규칙, 법령, 칙령, 결정, 명령, 규정 판례, 관례, 제정, 결의안 및 요건을 말합니다. "**불법(Unlawful)**"이란 법률 위반을 말합니다.

"**Microsoft 기밀 데이터(Microsoft Confidential Data)**"란 기밀성 또는 무결성 수단을 통해 손상될 경우 Microsoft의 명성 또는 재정에 상당한 손실을 초래할 수 있는 모든 정보입니다. 여기에는 Microsoft 하드웨어 및 소프트웨어 제품, 내부 영업군(line-of-business) 애플리케이션, 사전출시용 마케팅 자료, 제품 라이선스 키, Microsoft 제품 및 서비스와 관련된 기술 문서가 포함됩니다.

"**Microsoft 개인 데이터(Microsoft Personal Data)**"란 Microsoft에서 또는 Microsoft를 대신하여 처리되는 모든 개인 데이터를 의미합니다.

"**개인 데이터(Personal Data)**"란 데이터 주체와 관련된 모든 정보 및 법률에 따라 "개인 데이터" 또는 "개인 정보"를

구성하는 그 밖의 모든 정보를 말합니다.

"**처리(Process)**"란 수집, 기록, 구성, 구조화, 저장, 개조 또는 변경, 검색, 협의, 사용, 이전에 의한 공개, 보급 또는 그 밖의 방식으로의 제공, 정렬 또는 조합, 제한, 삭제 또는 파기와 같은 자동화된 수단 여부에 관계없이 Microsoft 개인 데이터 또는 기밀 데이터에 수행되는 모든 작업 또는 작업들을 말합니다. "처리 중" 및 "처리됨"은 이에 준하는 의미를 갖습니다.

"**처리자(Processor)**"란 다른 기관을 대신하여 개인 데이터를 처리하는 기관을 의미하며 서비스 제공자, 처리자(해당 용어는 GDPR에 정의되어 있음) 및 상황에 따라 데이터보호법에 준하는 용어를 포함합니다.

"**보호되는 건강 정보(Protected Health Information)**" 또는 "**PHI**"는 HIPAA(건강 보호 양도 및 책임에 관한 법, Health Information Portability and Accountability Act)의 보호를 받는 Microsoft 개인 데이터입니다.

"**레드 티밍(Red Teaming)**"이란 일련의 시험자 그룹이 모여서 한계, 위험 표면, 취약점을 식별하기 위해 의도적으로 시스템을 탐색하는 접근 방식입니다. 자세한 내용은 https://aka.ms/CustomerRedTeamingGuide를 참조하십시오.

AI의 "**민감한 사용(Sensitive Use)**"이란 합리적으로 예측 가능한 AI의 사용 또는 남용으로 인해 다음과 같은 방식으로 개인에게 영향을 미칠 수 있는 경우를 말합니다.

- 법적인 위치 또는 생활 기회에 대한 결과적인 영향 발생 .
- 신체적 또는 정신적 상해를 가할 위험.
- 인권에 대한 위협.

"**하도급업자(Subcontractor)**"란 Microsoft와 직접 계약하지 않은 공급자 계열사를 포함하여 공급자의 업무 수행을 책임지는 계약과 관련해 공급자가 그 의무를 위임하는 제3자를 말합니다.

"**하위 처리자(Subprocessor)**"란 Microsoft 업무 수행과 관련한 제3자를 말하며, 업무 수행에는 Microsoft가 처리자인 Microsoft 개인 데이터의 처리가 포함됩니다.

공급자 대응

공급자는 Microsoft에서 관리하는 온라인 서비스를 사용하여 매년 해당 요건을 준수하는지 확인합니다. 규정준수 운영 방식에 대해 자세히 알아보려면 SSPA 프로그램 가이드를 참조하십시오.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 A: 관리	
1	Microsoft와 공급자 간의 각 해당 계약(예: 기본 계약, 작업 명세서, 구매 주문서 및 그 밖의 주문)에는 Microsoft와 공급자 간의 직접적인 비즈니스 관계 이외의 Microsoft 개인 데이터의 판매 및 Microsoft 개인 데이터 처리 금지를 포함하여 해당되는 경우 Microsoft 기밀 데이터 및 개인 데이터와 관련된 개인정보보호 및 보안 데이터 보호 내용이 포함되어 있습니다. Microsoft 개인 데이터와 관련해 업무 수행에 관한 처리자 또는 하위 처리자로 기능하는 회사의 경우 계약에는 처리 주제와 기간, 처리 성격과 목적, Microsoft 개인 데이터의 유형 및 데이터 주체의 범주, Microsoft의 의무와 권리가 포함되어야 합니다.	공급자는 Microsoft와 공급자 간의 해당 계약을 제시해야 합니다. 처리자 및 하위 처리자의 경우 처리 설명은 해당 계약서(*예:* 작업 명세서, 구매 주문서)에 포함됩니다. Microsoft에서 공급자의 업무에 PHI 처리가 수반되어 있음을 확인한 경우 공급자는 Microsoft와 업무 협약 및/또는 기타 계약을 맺어야 합니다. 참고: 구매 주문이 진행 중인 기업은 추후 구매 과정 시 추가된 처리 활동에 대해 필요한 설명을 할 수 있습니다.
2	Microsoft에서 귀사의 하위 처리자 역할 이행을 확인하는 경우, 공급자는 Microsoft와 관련 데이터 보호 계약을 체결해야 합니다. 참고: Microsoft는 본 사안이 적용되는 경우 귀사 프로필에 본 지정 사항을 게시합니다.	표준계약조항, 온라인 고객데이터부칙, 공급자 및 협력사 전문서비스 데이터처리부칙 및/또는 업무 협약.
3	해당 기업 내 지정된 담당자 또는 그룹에 DPR 준수에 대한 책임과 책무를 할당합니다.	Microsoft 공급자 DPR의 규정준수 담당자 또는 그룹의 역할을 지정합니다. 개인정보보호 및/또는 보안 역할을 입증하는 해당인 또는 그룹의 권한과 책임을 설명하는 문서.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 A: 관리(계속)	
4	Microsoft 개인 또는 기밀 데이터에 액세스하는 사람(시스템 관리자, 운영 직원, 경영진, 제3자 등)을 위한 연간 개인정보 보호 및 보안 교육을 수립하고 유지하며 실행합니다. 귀사에 준비된 자료가 없는 경우 이 스토리보드 개요를 사용하여 귀사의 내규에 맞게 변경할 수 있습니다. 참고: 공급자 소속 직원은 Microsoft 부서에서 제공하는 추가 교육을 이수해야 할 수 있습니다.	연례 출석 기록을 이용할 수 있으며 요청 시 이를 Microsoft에 제공할 수 있습니다. 교육 콘텐츠는 정기적으로 업데이트되며, 비밀번호 보호, 로그인 모니터링, 악의적 소프트웨어, 기타 관련 보안 공지 사항을 포함하여 사고 예방 인식과 같은 개인정보 보호 및 보안 원칙을 다룹니다. 교육 요건의 규정준수 문서에는 개인정보보호 규정 요건, 보안 의무, 해당 계약의 요건 및 의무의 규정준수와 관련된 교육 증빙이 포함됩니다. IT 직원은 위기 상황에 효과적으로 대응할 수 있도록 사고 대응, 시뮬레이션 이벤트와 자동화된 방식에 대한 교육을 받아야 합니다. 공급자가 처리하는 Microsoft 개인 데이터에 PHI가 포함된 경우 교육 자료에 공급자의 허가된 사용 및 업무 협약에서 허가하는 공개를 포함하여 HIPAA 교육이 포함되어야 합니다.
5	공급자의 개인정보보호 및 보안 정책을 준수하지 못한 직원에 대해 적절한 제재를 내립니다.	미준수 시 제재(예: 최대 해고)를 설명하는 개인정보보호 및 보안 정책 서류.
6	Microsoft 개인 데이터를 제3국 또는 해외 기관에 이전하는 상황을 포함하여 Microsoft의 문서화된 지침에 따라서만 Microsoft 개인 데이터를 처리합니다. 단, 법률에서 요구하는 경우는 예외에 해당합니다. 그러한 경우, 처리자 또는 하위 처리자(공급자)는 처리 전에 해당 법적 요건을 컨트롤러(Microsoft)에 통지해야 합니다. 단, 해당 법률이 공공의 이익에 중요한 근거로 해당 정보를 금지하는 경우는 제외입니다.	공급자는 업무 수행에 참여하는 공급자의 소속 직원 및 계약자가 쉽게 접근할 수 있는 위치에 모든 Microsoft 문서 지침(예: 계약서, 작업 명세서 또는 주문 문서)을 전자적으로 편찬하고 유지관리합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 B: 고지	
7	공급자는 Microsoft를 대신하여 개인 데이터 수집 시 Microsoft 개인정보취급방침을 사용해야 합니다. 개인정보보호고지는 명확해야 하고 데이터 주체가 자신의 개인 데이터를 공급자에게 제출할지 여부를 결정하는 데 이용 가능해야 합니다. 참고: 귀사가 처리 활동의 컨트롤러인 경우, 내규 개인정보보호고지를 게시해야 합니다.	공급자는 현재 게시된 Microsoft 개인정보취급방침에 대한 fwdlink를 사용합니다. 개인정보취급방침은 사용자의 개인 데이터가 수집되는 모든 상황에 게시됩니다. 해당되는 경우 오프라인 버전을 사용할 수 있으며 이는 데이터 수집 전에 제공됩니다. 사용된 모든 오프라인용 개인정보취급방침은 최신 게시 버전이며 날짜가 적절히 명시됩니다. Microsoft 직원 서비스의 경우 Microsoft 데이터 개인정보보호고지가 사용됩니다.
8	실시간 또는 녹음된 음성 통화를 통해 Microsoft 개인 데이터 수집 시, 공급자는 데이터 주체와 해당 데이터의 수집, 취급, 사용 및 보유 관행을 논의할 수 있도록 준비되어 있어야 합니다.	음성 녹음 스크립트에는 Microsoft 개인 데이터의 처리 방식 및 다음이 포함됩니다. • 수집 • 사용 • 보유.
	섹션 C: 선택 및 동의	
9	해당되는 경우 공급자는 데이터 주체의 개인 데이터를 수집하기 전에 모든 처리 활동(신규 또는 업데이트된 처리 활동 포함)에 대해 데이터 주체의 동의를 얻고 이를 기록해야 합니다. 공급자는 기본 설정 변경을 준수하는 기간에 가장 구속력 있는 현지 법적 요건이 적용되는지 확인하기 위해 기본 설정 관리의 효율성을 추적감시합니다.	공급자는 데이터 주체가 처리 활동에 대한 동의를 제공하는 방법과 동의 범위가 해당 데이터 주체의 개인 데이터와 관련된 모든 공급자의 처리 활동을 포괄함을 입증할 수 있습니다. 공급자는 데이터 주체가 처리 활동에 대한 동의를 철회하는 방법을 입증할 수 있습니다. 공급자는 새로운 처리 활동을 시작하기 전에 기본 설정을 확인하는 방법을 입증할 수 있습니다. 참고: 서비스를 이용한 실험 또는 기술 문서 열람 기회와 같은 사용자 상호교류 스크린샷을 증빙

		자료로 사용할 수 있습니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 C: 선택 및 동의(계속)	
10	Microsoft 웹사이트 및/또는 애플리케이션 또는 Microsoft 브랜드를 취급하는 사이트를 제작 및 관리하는 공급자는 Microsoft 개인정보취급방침 및 현지 법적 요건의 의무에 따라 쿠키 사용에 대한 투명한 고지 및 선택권을 데이터 주체에게 제공해야 합니다. 계약사업부에서 특별히 요청하는 경우를 제외하고, 공급자는 1ES에서 생성한 표준 배너를 사용하여 선택을 관리해야 합니다. 본 요건은 사이트가 유럽연합/유럽경제지역 및 해당 개인정보보호법이 적용되는 그 밖의 지역 내 사용자를 대상으로 하는 경우 및 Microsoft 개인정보취급방침이 사용되는 모든 곳에 적용됩니다. 참고: Microsoft 비즈니스 후원사는 내부 웹 규정준수 포털(http://aka.ms/wcp)에 Microsoft 웹사이트를 등록하여 쿠키 인벤토리를 분류 및 관리해야 합니다.	각 쿠키의 목적은 문서화되어야 하며 시행된 쿠키 유형을 고지해야 합니다. • 세션 쿠키로 충분한 경우에는 영구 쿠키를 사용하지 않아야 합니다. • 영구 쿠키를 사용하는 경우 사용자가 사이트를 방문한 후 13개월을 초과하는 만료일을 지정해서는 안 됩니다. 다음과 같이 해당되는 경우 EU 법률 준수를 확인합니다. • 개인정보취급방침을 위한 라벨링 규칙, “개인정보 보호 및 쿠키” 이용 • 광고 등의 목적으로 "선택" 쿠키 사용 전에 확실한 사용자 동의 확보 • 6개월마다 동의가 만료되거나 다시 동의 확보
	섹션 D: 수집	
11	공급자는 Microsoft 개인 데이터 및/또는 기밀 데이터 수집을 감시추적하여 오직 업무 수행에 필요한 데이터만 수집되는지 확인해야 합니다.	공급자는 수집된 Microsoft 개인 데이터 및/또는 기밀 데이터가 업무 수행에 필요함을 보여주는 문서를 제공할 수 있습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
12	아동으로부터 데이터를 수집하기 전에(해당 관할권에 정의된 바에 따름) 공급자는 현지 개인정보보호법에 따라 동의를 얻어야 합니다.	공급자는 부모/보호자의 동의를 보여주는 문서를 제공할 수 있습니다. 공급자는 요청 시 Microsoft에 증빙 문서를

		제공합니다.
13	공급자가 Microsoft로부터 가명, NPI(식별할 수 없는 상태), 연관 없는 가명, 총계, 익명 또는 이러한 분류 중 하나와 관련이 있는 용어(예: 비식별화)를 포함하여 식별성이 감소한 데이터 집합을 받는 경우 공급자는 받는 당시의 상태로 데이터를 유지관리합니다.	공급자는 데이터 집합의 식별성을 높이지 않습니다(예: 데이터 집합의 일부분을 다른 데이터 집합과 결합하여 개인을 재식별하는 행위 등). 공급자는 비식별화/익명화 데이터 정책/절차를 마련합니다.
#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
섹션 E: 보유		
14	Microsoft 개인 데이터 및 기밀 데이터를 업무 수행에 필요한 기간보다 더 오래 보유하지 않도록 합니다. 단, Microsoft 개인 데이터 및/또는 기밀 데이터의 지속적인 보유가 법률에 의해 요구되는 경우는 제외됩니다.	공급자는 계약서(예: 작업 명세서, 구매 주문서)에서 Microsoft가 지정한 문서화된 보유 정책 또는 보유 요건을 준수합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
15	Microsoft의 단독 재량에 따라 공급자가 소유하거나 통제하는 Microsoft 개인 데이터 및 기밀 데이터는 업무 수행 완료 시 또는 Microsoft의 요청 시 Microsoft로 반환하거나 파기하도록 합니다. 사용자의 명시적인 요청 또는 데이터 사용 기간과 같은 기타 트리거를 근거로 하여 데이터를 애플리케이션에서 삭제할 때 안전하게 삭제되도록 하는 절차가 애플리케이션 내에 마련되어야 합니다. Microsoft 개인 데이터 또는 기밀 데이터의 파기가 필요한 경우, 공급자는 데이터를 읽거나 재구성할 수 없도록 Microsoft 개인 및/또는 기밀 데이터가 포함된 물리적 자산을 소각, 파쇄 또는 파기해야 합니다.	Microsoft 개인 데이터 및 기밀 데이터의 처리 기록을 유지관리합니다(여기에는 파기를 위해 Microsoft에 반환하는 데이터가 포함될 수 있음). Microsoft에서 파기를 요구 또는 요청하는 경우 공급자 소속 담당자가 서명한 파기 증서를 제공합니다.
섹션 F: 데이터 주체		

	데이터 주체는 자신의 개인 데이터 처리와 관련해 접근, 삭제, 편집, 이전, 제한 및 거부할 권리("데이터 주체의 권리")를 포함하여 법률에 따라 일정한 권리를 보유합니다. 데이터 주체가 Microsoft 개인 데이터와 관련하여 법률에 따른 자신의 권리를 행사하려는 경우, 공급자는 Microsoft에서 다음을 수행하도록 허용하거나 Microsoft를 대신하여 이러한 조치를 수행해야 합니다.	
16	가능한 경우 적절한 기술 및 조직적 조치를 통해 Microsoft를 지원하여 데이터 주체의 권리를 행사하려는 데이터 주체의 요청에 지체 없이 응할 의무를 이행하도록 합니다. Microsoft에서 별도의 지시가 있는 경우를 제외하고, 공급자는 공급자에 직접 문의하는 모든 데이터 주체가 Microsoft에 의뢰하여 데이터 주체의 권리를 행사하도록 합니다.	공급자는 데이터 주체의 권리 실행을 지원할 수 있도록 문서화된 과정 및 절차의 증거를 유지관리합니다. 공급자는 문서화된 검사 증거를 유지관리합니다. Microsoft에서 요청 시 증빙 자료를 제공합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 F: 데이터 주체(계속)	
17	데이터 주체에게 직접 응답하거나 공급자가 셀프서비스 온라인 방식을 제공할 경우, 공급자는 요청하는 데이터 주체를 식별하기 위한 과정과 절차를 마련합니다.	공급자는 Microsoft 데이터 주체를 식별하는 데 사용되는 방식을 문서화했습니다. 공급자는 요청 시 Microsoft에 문서화된 증빙 자료를 제공합니다.

18	Microsoft에서 셀프서비스 온라인 방식을 통해 제공되지 않는 데이터 주체와 관련한 Microsoft 개인 데이터를 찾도록 요청하는 경우, 공급자는 요청된 데이터를 찾고 합당한 검색이 이루어졌음을 입증할 수 있는 충분한 기록을 유지하기 위해 합당한 노력을 기울입니다.	공급자는 Microsoft 개인 데이터의 보유 여부를 확인하기 위한 절차와 관련한 문서화된 증거를 유지관리하고 요청 시 Microsoft에 문서를 제공합니다. 공급자는 데이터 주체의 권리 요청을 이행하기 위해 취한 조치를 입증하는 기록을 유지관리합니다. 문서에는 다음이 포함됩니다. • 요청 날짜 및 시간 • 요청에 응하기 위해 취한 조치 및 Microsoft에 통지된 날짜의 기록 공급자는 요청 시 Microsoft에 기록 보관 증거를 제공합니다.
19	공급자는 개인이 Microsoft 개인 데이터에 대한 접근 권한을 얻거나 다른 방법으로 권리를 행사하기 위해 취해야 하는 조치를 데이터 주체에게 전달합니다.	공급자는 Microsoft 개인 데이터에 접근하기 위한 통신 및 절차에 대한 문서화된 증거를 유지관리합니다. 공급자는 문서화된 증거를 유지관리하고 요청 시 Microsoft에 동일한 증거를 제공합니다.
20	데이터 주체의 권리 요청 날짜 및 시간과 이러한 요청에 대해 공급자가 취한 조치를 기록합니다. 요청이 거부된 경우, Microsoft의 지시에 따라 데이터 주체에게 서면 설명을 제공합니다. 요청 시 Microsoft에 데이터 주체의 요청 기록을 제공합니다.	공급자는 Microsoft 개인 데이터에 대한 접근/삭제 요청의 기록 및 문서 변경 사항을 유지관리합니다. 요청이 거부된 사례를 문서화하고 Microsoft 심사 및 승인의 증거를 보유합니다. 공급자는 Microsoft 개인 데이터에 대한 요청 및 접근 거부의 기록 보관에 대한 증거를 제공합니다.
21	공급자는 Microsoft에 허용하거나 인증된 데이터 주체에 대해 요청된 Microsoft 개인 데이터의 사본을 적절한 인쇄, 전자 또는 구두 형식으로 취득해야 합니다.	공급자는 Microsoft 개인 데이터를 데이터 주체와 공급자가 이해할 수 있는 편리한 형식으로 데이터 주체에게 제공합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
섹션 F: 데이터 주체(계속)		

22	공급자는 Microsoft 또는 인증된 데이터 주체에 공개된 Microsoft 개인 데이터가 다른 개인을 식별하는 데 사용될 수 없도록 합당한 예방조치를 취해야 합니다.	공급자는 계약 조항에 반하는 데이터 주체의 식별을 방지하기 위해 예방조치와 관련된 절차의 문서화된 증거를 유지관리합니다 공급자는 요청 시 Microsoft에 증거를 제공합니다.
23	데이터 주체가 자신의 Microsoft 개인 데이터가 완전하고 정확하지 않다고 생각하는 경우, 공급자는 문제를 Microsoft에 보고하고 문제를 해결하는 데 필요한 만큼 Microsoft와 협조해야 합니다.	공급자는 불일치 사례를 문서화하고 문제를 Microsoft에 보고합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
24	액세스를 위한 데이터 주체의 요청과 관련하여, 공급자는 Microsoft 개인 데이터를 공유했거나 공유하는 모든 수신자의 기록을 유지해야 합니다.	요청 시, 공급자는 Microsoft 개인 데이터의 모든 실질적인 수신자 및 가능한 제3자 수신자의 목록을 제공할 수 있습니다.
섹션 G: 하도급업자		
	공급자가 하도급업자를 통해 Microsoft 개인 또는 기밀 데이터를 처리하려는 경우 공급자는 다음을 수행해야 합니다.	
25	서비스를 하도급업자에게 위탁하거나 하도급업자의 추가 또는 교체와 관련한 사항을 변경하기 전에 Microsoft에 통지합니다. 참고: 현재 하도급업자를 고용하지 않지만 추후 고용할 수 있는 경우에도 본 의무사항의 수락 의사를 표시하십시오.	Microsoft 개인 데이터가 해당 계약(예: 작업 명세서, 부칙, 구매 주문서)에서 요구되는 대로 Microsoft에 알려진 기업에서만 처리되거나 SSPA 데이터베이스에 명시되어 있는지 확인합니다. 공급자는 해당 하도급업자 목록을 온라인에 게시하고 SSPA 데이터베이스의 페이지 링크를 포함할 수 있습니다.
26	하도급업자가 개인 데이터를 수탁 처리하는 Microsoft 개인 데이터 및 기밀 데이터의 성질과 범위를 문서화하여 수집된 정보가 업무 수행에 필요한지 확인합니다.	공급자는 하도급업자에 공개 또는 이전된 Microsoft 개인 데이터 및 기밀 데이터에 관한 문서를 유지관리합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 G: 하도급업자(계속)	
27	Microsoft가 Microsoft 개인 데이터의 컨트롤러인 경우, 하도급업자가 데이터 주체의 명시된 연락처 기본 설정에 따라 Microsoft 개인 데이터를 사용하는지 확인합니다.	하도급업자가 Microsoft 데이터 주체 기본 설정을 활용하는 방법을 입증합니다. 하도급업자가 기본 설정 변경 사항을 이행할 수 있는 기간이 포함된 증빙 문서(예: 스크린샷, SLA, SOW 등)를 제공합니다.
28	Microsoft와 공급자 계약을 이행하는 데 필요한 목적으로 하도급업자의 Microsoft 개인 또는 기밀 데이터 처리를 제한합니다. Microsoft 개인 데이터가 PHI인 경우 하도급업자와 비즈니스 협력 계약을 체결하여 하도급업자의 Microsoft 개인 데이터 처리를 제한하고 Microsoft 개인 데이터의 기밀성 및 보안을 Microsoft와 공급자 사이의 업무 협약과 동일한 방식으로 보호합니다.	공급자는 하도급업자에게 제공된 Microsoft 개인 데이터가 업무 수행에 필요함을 보여주는 문서를 제공할 수 있습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다(해당되는 경우 업무 협약 포함).
29	Microsoft 개인 데이터의 무단 또는 불법 처리 표시에 대한 이의제기를 심사합니다.	공급자는 하도급업자의 Microsoft 개인 데이터 무단 사용 또는 공개와 관련된 이의제기를 처리하기 위한 시스템 및 절차가 마련되어 있음을 입증할 수 있습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
30	하도급업자가 업무 수행과 관련된 목적 이외의 용도로 Microsoft 개인 또는 기밀 데이터를 처리했음을 알게 된 즉시 Microsoft에 통지합니다.	공급자는 하도급업자의 Microsoft 데이터 오용을 신고할 수 있는 지침과 수단을 제공했습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
31	공급자가 Microsoft를 대신하여 제3자로부터 개인 데이터를 수집하는 경우, 공급자는 제3자 개인 데이터 보호 정책 및 관행이 Microsoft 및 DPR과의 공급자 계약과 일치하는지 확인해야 합니다.	공급자는 제3자의 데이터 보호 정책 및 관행과 관련하여 수행된 실사 문서를 제공할 수 있습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.

32	하도급업자의 Microsoft 개인 데이터 및 기밀 데이터 무단 또는 불법 처리로 인해 발생하는 실제적 또는 잠재적 피해를 완화하기 위해 즉각적인 조치를 취합니다.	공급자는 계획 및 절차에 대한 증빙 문서를 유지관리하고 요청 시 증빙 문서를 Microsoft에 제공해야 합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 H: 품질	
33	공급자는 모든 Microsoft 개인 데이터의 무결성을 유지하여 데이터가 처리된 명시된 목적과 관련하여 정확하고 완전하며 관련성을 유지하게 해야 합니다.	공급자는 Microsoft 개인 데이터가 수집, 생성 및 갱신될 때 이를 검증하는 절차가 마련되어 있음을 입증할 수 있습니다. 공급자는 지속적으로 정확성을 확인하고 필요에 따라 정정하기 위한 추적감시 및 표본 추출 절차가 마련되어 있음을 입증할 수 있습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
	섹션 I: 추적감시 및 집행	
34	공급자는 계약상의 요건에 따라 또는 데이터 사고를 인지하게 되는 즉시 어느 쪽이든 더 빠른 시기에 지체 없이 Microsoft에 통지하도록 하는 침해 사고 대응 계획을 마련하고 있습니다. 공급자는 Microsoft에 데이터, 정보, 공급자 소속 직원에 대한 접근 또는 법정 검토를 수행하는 데 필요한 하드웨어 제공을 포함하여 Microsoft의 요청 또는 지시에 따라 데이터 사고의 조사, 완화 또는 복원 시 Microsoft와 협조해야 합니다. 또한, 포렌식 검토를 수행하기 위해 필요한 공급자 개인 또는 하드웨어에 대한 액세스가 필요할 수 있습니다. 참고: Microsoft에 데이터 침해 사고를 알리는 방법은 SSPA 프로그램 가이드를 참조하십시오.	공급자는 본 섹션에 설명된 대로 고객(Microsoft)에게 통지하는 조치가 포함된 사고 대응 계획을 마련해두고 있습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.

35	복원 계획을 시행하고 각 데이터 사고의 해결을 추적감시하여 적시에 적절한 수정 조치를 취하도록 합니다.	문제가 해결될 때까지 Microsoft에 시의적절하게 업데이트를 제공하는 것을 포함하여 데이터 사고에 대응하고 종결하기 위해 따라야 하는 절차를 문서화했으며 사고 후 검토를 제공합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 I: 추적감시 및 집행(계속)	
36	Microsoft가 Microsoft 개인 데이터의 컨트롤러인 경우 Microsoft 개인 데이터와 관련된 모든 데이터 보호 이의제기에 대응하기 위한 정식 이의제기 절차를 수립합니다.	공급자는 Microsoft 개인 데이터와 관련된 이의제기 사항을 접수할 수 있는 수단이 있으며 이의제기 사항을 처리하기 위한 문서화된 이의제기 관련 절차를 보유하고 있습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
	섹션 J: 보안	
	공급자는 정책 및 절차가 포함된 정보 보안 프로그램을 수립, 시행 및 유지관리하여 Microsoft 개인 데이터 및 기밀 데이터를 업계 모범 관행에 따라 법률에서 요구하는 대로 안전하게 보호하고 유지해야 합니다. 공급자의 보안 프로그램은 아래 명시된 표준, 요건 37~52를 충족해야 합니다. Microsoft 개인 데이터가 PHI인 경우 공급자는 HIPAA 보안 규정의 요건을 충족하는 범위에서 공급자의 정책 및 절차가 PHI의 보안에 영향을 미치는 환경적 및 운영적 변화에 대응하여 정기적으로 기술적 및 비기술적 평가를 수행해야 합니다.	유효한 ISO 27001 인증은 섹션 J: 보안을 대체할 수 있습니다. 이 대체 항목을 적용하려면 SSPA에 문의하십시오. 참고: 관련 인증을 제공해야 합니다.

37	다음을 포함하는 네트워크 보안 평가를 매년 수행합니다. • Microsoft 개인 데이터의 기밀성, 무결성 및 가용성에 대한 잠재적 위험 및 취약성과 이러한 위험 감소를 위한 조치 구현 평가 • 새 시스템 구성 요소, 네트워크 토폴로지, 방화벽 규칙 등 환경의 중대한 변화 검토 • 변경 로그 유지관리	공급자는 네트워크 평가, 변경 로그 및 검사 결과를 문서화했습니다. 필수 변경 로그는 변경사항을 추적하고 변경 사유에 대한 정보를 제공하고 지정된 승인자의 성명과 직책을 포함해야 합니다. 요청 시 제공 가능한 지난 90일 간의 기록.
38	공급자는 모바일 기기에서 접근 또는 사용하는 Microsoft 개인 데이터 또는 기밀 데이터의 사용을 보호 및 제한하는 모바일 기기 정책을 규정, 전달 및 시행합니다.	공급자는 Microsoft 개인 데이터 또는 기밀 데이터 처리에 모바일 기기 사용이 필요한 경우 호환되는 모바일 기기 정책의 사용을 입증합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 J: 보안(계속)	
39	업무 수행을 지원하는 데 사용되는 모든 자산을 고려해야 하고 식별된 소유자가 있어야 합니다. 공급자는 이러한 정보 자산의 인벤토리를 유지관리하고, 자산의 허용 가능한 승인된 사용을 수립하고, 자산의 수명 주기 동안 적절한 수준의 보호를 제공할 책임이 있습니다.	업무 수행을 지원하는 데 사용되는 기기 자산의 인벤토리. 이러한 자산의 인벤토리는 다음을 포함합니다. • 기기 위치 • 자산에 있는 데이터의 데이터 분류 • 고용 또는 사업 계약 종료 시 자산 복구 기록 • 더 이상 필요하지 않은 경우 데이터 저장 매체의 폐기 기록 • Microsoft 데이터에 액세스하기 위한 @microsoft.com 자격증명을 포함하여 공급자 직원이 사용하는 모든 물리적 및 가상 장치는 Microsoft가 단독으로 완전히 관리하며 Microsoft가 프로비저닝하지 않은 추가적인 보안 소프트웨어를 설치하면 안 됩니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 J: 보안(계속)	
40	공급자가 통제하는 Microsoft 개인 데이터 또는 기밀 데이터에 대한 무단 접근을 방지하기 위해 접근 권한 관리 절차를 수립 및 유지합니다.	공급자는 다음을 포함하는 접근 권한 관리 계획을 시행했음을 입증합니다. • 접근 통제 절차 • 신원 확인 절차 • 시도 실패 후 잠금 절차 • 비활성 상태 이후 자동 로그오프 • 인증 자격 증명을 선택하기 위한 강력한 매개변수 • 고용 종료 시 48시간 이내 사용자 계정(직원 또는 하도급업자가 사용하는 계정 포함) 비활성화 • 길고 복잡한 비밀번호 사용과 재사용을 방지하는 강력한 비밀번호 관리 • 신원 확인을 위해 다중 인증(MFA) 사용 공급자는 최소 권한 원칙을 적용하여 Microsoft 개인 데이터 및 기밀 데이터에 대한 사용자 접근을 검토하는 절차가 확립되어 있음을 입증합니다. 절차에는 다음이 포함됩니다. • 명확하게 규정된 사용자 역할 • 역할에 대한 접근 승인을 검토 및 정당화하는 절차 • Microsoft 데이터 접근 권한이 있는 역할 내의

		사용자가 그룹/역할에 속하는 문서화된 근거가 있는지 테스트 • 계정 또는 비밀번호를 공유하는 행위를 강력하게 금지

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 J: 보안(계속)	
41	Microsoft 개인 데이터 또는 기밀 데이터를 처리하는 데 사용되는 시스템에 대한 보안 패치의 우선순위를 지정하는 패치 관리 절차를 정의 및 시행합니다. 이러한 절차에는 다음이 포함됩니다. • 지난 12개월 동안의 월간 검사를 보여주는 대략적인 규정준수 보고서를 활용하여 월간 취약성 검사 실시 • 보안 패치 우선순위를 지정하도록 정의된 위험 접근 방식 • 긴급 패치를 취급 및 시행하는 기능 • 애플리케이션 서버 및 데이터베이스 소프트웨어와 같은 운영 체제 및 서버 소프트웨어에 대한 적용성 • 패치 완화 위험의 문서화 및 예외 사항 추적 • 승인된 기업에서 더 이상 지원하지 않는 소프트웨어의 폐기 요건	공급자는 본 요건을 충족하고 최소한 다음을 포함하는 구현된 패치 관리 절차를 입증할 수 있습니다. • 심각도 정의를 문서화하고 업데이트에 할당하여 배포 우선순위 통지 • 긴급 패치를 구현하도록 문서화된 절차 • 승인과 예외를 추적하고 패칭 준수 데이터를 포함하는 패치 관리 기록 요청 시 제공 가능한 지난 90일 간의 기록.
42	잠재적으로 유해한 바이러스 및 악성 소프트웨어 애플리케이션으로부터 보호하기 위해 서버, 프로덕션 및 교육용 데스크톱을 포함하여 Microsoft 개인 데이터 및 기밀 데이터를 처리하는 데 사용되는 네트워크에 연결된 장비에 바이러스 백신 및 맬웨어 방지 소프트웨어를 설치합니다. 바이러스 백신 및 맬웨어 방지 소프트웨어의 패치를 정기적으로 적용하고 최신 상태로 유지해야 합니다. 매일 또는 바이러스 백신/맬웨어 방지 소프트웨어 공급자의 지시에 따라 맬웨어 방지 정의를 업데이트합니다. 참고: 이는 Linux를 포함한 모든 운영 체제에 적용됩니다.	바이러스 방지 및 맬웨어 방지 소프트웨어 사용이 활성 상태임을 나타내는 기록이 있습니다. 참고: 이 요건은 모든 운영 체제에 적용됩니다.

43	Microsoft용 소프트웨어를 개발하는 공급자는 보안 기반 설계 원칙을 빌드 프로세스에 포함해야 합니다.	공급자 기술 사양 문서에는 개발 주기의 보안 검증을 위한 점검 사항이 포함되어 있습니다. 공급자는 명백한 결함을 경고하기 위해 일정한 형태의 코드 스캐닝을 사용합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 J: 보안(계속)	
44	애플리케이션, 시스템 및 인프라 수준에서 침입, 손실 및 그 밖의 무단 활동을 방지하기 위해 데이터손실방지("DLP") 프로그램을 사용합니다. 데이터는 적절히 분류, 라벨 표시 및 보호되어야 하며 공급자는 Microsoft 개인 데이터 또는 기밀 데이터가 사용 중인 정보 시스템에서 침입, 손실 및 그 밖의 무단 활동을 추적감시해야 합니다. DLP 프로그램은 최소한 • Microsoft 개인 데이터 또는 기밀 데이터를 보관하는 경우, 업계 표준 호스트, 네트워크 및 클라우드 기반 침입 탐지 시스템(IDS)을 사용해야 합니다. • 데이터 손실을 추적감시하고 적극적으로 중지하도록 구성된 고급 침입방지시스템("IPS")을 구현해야 합니다. • 시스템이 침해된 경우 시스템을 분석하여 남아있는 취약점도 해결되었는지 확인해야 합니다. • 시스템 손상 탐지 도구의 추적감시를 위해 필요한 절차를 설명해야 합니다. • 데이터 사고가 감지될 경우 수행이 필요한 침해 사고 대응 및 관리 프로세스를 수립해야 합니다. • Microsoft 개인 또는 기밀 데이터를 무단으로 다운로드 및 사용하는 것과 관련하여 (공급자 업무 수행에서 제외되는 모든 공급자 직원 및 하도급업자에게) 전달해야 합니다.	문서화된 DLP 프로그램이 침입, 손실 및 그 밖의 무단 활동(최소한 본 섹션에 지정된 모든 항목)을 방지하기 위한 절차와 함께 배치되었습니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 J: 보안(계속)	
45	공급자는 개발 과정의 모든 단계에서 보안정보가 소프트웨어에 내장되거나 하드코딩되지 않도록 해야 합니다.	공급자는 사용자 이름, 비밀번호, SSH 키, API 액세스 토큰 등과 같은 보안정보가 테스트 또는 생산 환경에서 소스나 구성 파일에 통합되지 않도록 하는 절차를 문서화했습니다. 공급자는 다음을 입증할 수 있습니다. • GitHub 고급 보안(GHAS) 또는 그와 유사한 서비스나 도구 등과 같은 기밀정보 노출 예방 도구의 지원되는 최신 버전을 사용합니다. • 소스나 구성 파일에 보안정보가 실수로 포함된 경우 그러한 보안정보는 발견 후 삭제되었다는 사실을 문서화합니다. • 대체 또는 보조 자격증명이 코드에 다시 포함되지 않음을 보장합니다. • 거짓양성과 관련 교정책을 문서화합니다.
46	공급자는 백업 계획 절차가 Microsoft 개인 데이터 및 기밀 데이터를 무단 사용, 접근, 공개, 변경 및 파기로부터 보호하는지 확인해야 합니다.	공급자는 해당 기관에서 지장을 초래하는 사건사고를 관리하고 경영진이 승인한 정보 보안 연속성 목표를 기반으로 사전 결정된 수준으로 정보 보안 유지 방법이 자세히 설명된 문서화된 대응 및 복구 절차를 입증할 수 있습니다. 공급자는 중요 데이터를 주기적으로 백업하고, 안전하게 저장하고, 효과적으로 복구하기 위한 절차를 규정 및 시행했음을 입증할 수 있습니다.

47	비즈니스 연속성 및 재해 복구 계획을 수립 및 테스트합니다.	재해 복구 계획에는 다음이 포함되어야 합니다. • 시스템이 공급자의 비즈니스 운영에 중요한지 결정하기 위해 규정된 기준. • 재해 발생 시 복구 대상이 되어야 하는 규정된 기준에 기반한 주요 시스템 명시. • 시스템에 대해 알지 못하는 엔지니어가 72시간 이내에 앱을 복구할 수 있도록 각 중요 시스템에 규정된 재해 복구 절차. • 복구 목표를 충족할 수 있는지 확인하기 위한 재해 복구 계획에 대한 연례(또는 더 자주) 테스트 및 검토.
#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 J: 보안(계속)	
48	개인에게 Microsoft 개인 또는 기밀 데이터에 대한 접근 권한을 부여하기 전에 해당 개인의 신원을 인증하고, 업무 수행을 지원하기 위해 허용된 특정 개인의 활동 범위로 접근이 제한되도록 합니다.	모든 사용자 ID가 고유하고 각각 Azure Active Directory와 같은 업계 표준 인증 방법이 있는지 확인합니다. 스마트 카드 또는 핸드폰 기반 인증자와 같은 다중 인증(MFA)을 사용해야 합니다. 모든 공급자 소속 직원 및 하도급업자가 Microsoft 개인 데이터 또는 기밀 데이터에 접근하는 것이 업무 수행을 지원하기 위해 더 이상 필요하지 않음을 확인하는 절차를 다루는 문서화된 정보 보안 프로그램.

49	공급자는 네트워크를 통한 전송 중인 업무 수행과 관련하여 처리된 모든 데이터를 전송 계층 보안("**TLS**") 또는 인터넷 프로토콜 보안("**IPsec**")을 사용한 암호화로 보호해야 합니다. 이러한 방법은 NIST 800-52 및 NIST 800-57에 설명되어 있으며, 이에 준하는 산업 표준을 사용할 수도 있습니다. 공급자는 암호화되지 않은 수단을 통해 전송된 Microsoft 개인 또는 기밀 데이터 전달을 거부해야 합니다.	TLS 또는 그 밖의 인증서를 생성, 배포 및 교체하는 절차를 규정 및 시행해야 합니다.
50	Microsoft 개인 또는 기밀 데이터에 접근하거나 이를 취급하는 모든 공급자 기기(노트북, 워크스테이션 등)는 디스크 기반 암호화를 사용해야 합니다.	Microsoft 개인 또는 기밀 데이터를 취급하는 데 사용되는 모든 고객 기기에 대해 BitLocker 또는 이에 준하는 다른 업계 디스크 암호화 솔루션을 충족하도록 모든 기기를 암호화합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 J: 보안(계속)	
51	시스템 및 절차(NIST 800-111 표준에 설명된 것과 같은 현 산업 표준 사용)는 **일체의** Microsoft 개인 데이터 및/또는 기밀 데이터를 휴지 상태에서 암호화할 수 있도록(저장 시) 마련되어 있어야 합니다. 그 예시에는 다음이 포함되지만 이에 국한되지는 않습니다. • 자격 증명 데이터(예: 사용자 이름/비밀번호) • 결제 수단 데이터(예: 신용카드 및 은행 계좌 번호) • 출입국 관련 개인 데이터 • 의료 프로필 데이터(예: 의료 기록 번호 또는 인증 목적으로 사용되는 생체 표식 또는 식별자(예: DNA, 지문, 안구 망막 및 홍채, 음성 패턴, 얼굴 패턴 및 손 측정)) • 정부가 발급한 신원 확인 데이터(예: 사회 보장 또는 운전면허증 번호) • Microsoft 고객(예: SharePoint, O365 문서, OneDrive 고객)에 속한 데이터 • 미공개된 Microsoft 제품 관련 자료 • 생년월일 • 아동 프로필 정보 • 실시간 지리 데이터 • 실제 개인(비사업장) 주소 • 개인(비사업장) 전화번호 • 종교 • 정치적 견해 • 성적 취향/선호	Microsoft 개인 데이터 및 기밀 데이터가 휴지 상태에서 암호화되어 있는지 확인합니다.

	• 보안 질문 답변(예: 2fa, 비밀번호 재설정) • 어머니의 결혼 전 이름	

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 J: 보안(계속)	
52	개발 또는 테스트 환경에서 사용되는 모든 Microsoft 개인 데이터를 익명으로 처리합니다.	Microsoft 개인 데이터는 개발 또는 테스트 환경에서 사용되어서는 안 됩니다. 대안이 없는 경우 데이터 주체를 식별하거나 개인 데이터의 오용을 방지하기 위해 익명화되어야 합니다. 참고: 익명화 데이터는 가명화 데이터와 다릅니다. 익명화 데이터는 개인 데이터의 데이터 주체를 더 이상 알아볼 수 없는 경우 식별되거나 식별 가능한 자연인과 관련이 없는 데이터입니다. Microsoft 개인 데이터가 PHI인 경우 익명화가 HIPAA 비식별화 표준을 충족해야 합니다.
	섹션 K: AI 시스템	
53	서비스 제공과 관련하여 AI 시스템이 포함된 경우, 공급자는 Microsoft와 해당 AI 시스템 약관을 체결해야 합니다. 의도된 사용이 변경된 경우 지체 없이 공개해야 하여 정확성과 규정준수를 위해 적어도 매년 검토해야 합니다.	AI 시스템 계약 조건이 Microsoft와 공급자 간의 계약에 존재합니다.
54	회사 내 지정된 담당자 또는 그룹에 배포 중 및 배포 이후에 AI 시스템에 대한 문제 해결, 관리, 운영, 감독, 및 통제할 책임을 할당합니다.	AI 시스템에 대한 규정준수 담당자 또는 그룹의 역할을 지정합니다. 그러한 담당자 또는 그룹의 권한과 책임을 설명하는 문서.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 K: AI 시스템(계속)	
55	업무 수행과 관련하여 공급자의 AI 시스템 내의 데이터를 액세스하거나 처리하는 담당자에 대한 연간 개인정보 보호 및 보안 교육을 수립, 유지 및 실행합니다.	연례 출석 기록을 이용할 수 있으며 요청 시 이를 Microsoft에 제공할 수 있습니다. 교육 요건의 규정준수 문서에는 지속적인 AI 시스템 사용에 대한 개인정보보호 규정 요건, 보안 의무, 해당 계약의 요건 및 의무의 규정준수와 관련된 교육 증빙이 포함됩니다. 교육 콘텐츠는 매년 검증됩니다.
56	AI 시스템에 대해 명시된 의도된 사용 및 민감한 사용에 부정적인 영향을 미칠 수 있는 데이터 사고 또는 결함 발생을 인지한 경우, 계약 조건 또는 해당 개인정보 보호법에 명시된 기간에 따라, 또는 지체 없이(가장 먼저 도래하는 기간 적용) Microsoft에 통지하는 AI 시스템 사고 대응 계획을 세웁니다. 참고: Microsoft에 데이터 침해 사고를 알리는 방법은 SSPA 프로그램 가이드를 참조하십시오.	공급자는 다음 모든 엔드포인트를 포함하여 AI 시스템 사고 대응 계획을 세웁니다. • 본 요건에 설명된 바와 같이, 고객(Microsoft)에게 통지하는 단계. • 전체 시스템이 복구될 때까지의 경과 시간을 포함하는 시스템 롤백 계획. • 기능이 꺼질 때까지 경과하는 시간을 포함하여 기능이 꺼지도록 지원. • 시스템이 업데이트될 때까지 경과하는 시간을 포함하여 각 모델에 대한 업데이트 및 업데이트를 릴리스하는 프로세스. • 시스템에 대한 변경 사항, 장애에 대해 업데이트된 이해 사항, 최상의 완화 조치를 고객, 파트너 및 최종 사용자에게 통지하는 방법과 관련된 프로세스. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
57	공급자는 AI 시스템에 대한 레드 티밍을 진행해야 합니다. AI 시스템을 배포하기 전에 취약점을 해결해야	공급자는 다음 사항을 문서화했습니다. • 레드 티밍 프로세스가 마련되어 있습니다. • 취약점이 해결되었습니다.

	합니다.	
58	공급자는 하기 사항을 포함하여, 공개 및 문서화를 통해 데이터 규정 준수를 보장할 수 있는 전담 AI 프로그램을 마련합니다.	공급자는 전담 AI 프로그램을 기술하는 문서를 마련합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
59	공급자는 의도된 사용의 투명성을 공개합니다.	요청 시 의도된 사용 투명성 공개가 Microsoft에 제공됩니다.
#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 K: AI 시스템(계속)	
60	**서명한 업무 협약**: AI 공급자를 고용할 경우, 조직은 서명한 업무 협약에서 명백한 계약 조건을 설정해야 합니다. 이러한 업무 협약은 데이터 처리, 기밀 유지, 지적 재산권, 책임, 사고 대응 및 해당하는 민감한 사용을 명시적으로 해결합니다.	공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다(해당되는 경우 협약 포함).
61	**책임**: 조직 내에서 AI 배포 및 위험 관리에 대한 명백한 책무 및 책임 라인을 정의합니다. 조직은 AI 시스템의 결과에 대해 책임지는 당사자를 식별해야 합니다. 여기에는 시간이 지나면서 발생할 수 있는 윤리적 문제, 편향, 기타 문제를 해결하는 책임이 포함됩니다. 윤리 가이드라인에 계속 준수하기 위해 AI 모델을 정기적으로 모니터링하고 감사하는 것은 필수입니다.	공급자는 사람이나 그룹의 책임을 포함하여 전담 AI 프로그램을 기술하는 문서를 마련합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
62	**위험 평가**: 개인정보 보호, 보안, 및/또는 전담 AI 위험 평가를 실시하여 잠재적인 편향, 보안 취약점, 의도치 않은 결과를 고려합니다. 민감한 사용이 포함된 경우, 필수적인 통제 또는 완화 조치를 위한 지침이 포함되어야 합니다.	공급자는 테스트, 시스템 발전의 모니터링, 지속적인 연간 유지관리를 수행하여 알려져 있거나 발견된 오류, 인구통계학적 집단에 대한 불리한 영향, 환각, 기타 필수적인 완화 조치 또는 기술적 통제 조치를 개선함으로써 보안 및 개인정보 보호 규정준수를 유지하는 조치를 포함하여 위험 평가에

		대한 증빙 또는 유사한 문서나 보고서를 유지합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
63	**투명성과 설명 가능성**: AI 시스템은 투명하고 설명 가능해야 합니다. 공급자는 결정을 내리는 방법에 대한 인사이트를 제공해야 합니다. 공개를 통해 모델 설계, 훈련 데이터, 의사 결정 프로세스에 대한 투명성을 강화해야 합니다.	공급자는 의도된 목적에서 벗어나는 모든 시스템 장애 보고서, 변질, 환각 또는 보고된 남용을 기록하고 문제를 해결하기 위해 수행된 조치의 증빙을 제공해야 합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
64	**모니터링 및 적응**: 공급자는 AI 시스템의 지속적인 모니터링을 입증하고 새로운 위험이 대두될 때 AI 시스템을 적응시키고 업데이트해야 합니다.	공급자는 의도된 목적에서 벗어나는 모든 시스템 장애 보고서, 변질, 환각 또는 보고된 남용을 기록하고 문제를 해결하기 위해 수행된 조치의 증빙을 제공해야 합니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 K: AI 시스템(계속)	
65	공급자는 각 의도된 사용에 대한 모든 필수적인 오류 유형, 성능 지표 정의, 데이터 성능, 안전, 및 신뢰도 지표를 포함하여 필수적인 공개, 보고 또는 기타 유사한 문서를 제공해야 합니다.	• 각각의 의도된 사용에 영향을 미치는 각 운영 요소 및 그러한 의도된 사용에 영향을 미칠 수 있는 허용 가능 범위를 좁히거나 허용 가능 오류 비율(거짓 양성 및 거짓 음성 오류 비율 포함)을 낮추는 추가적인 운영 요소를 위한 허용 가능한 오류 범위를 정의하고 제공합니다. • 배포 측면에서 시스템의 신뢰할 수 있는 안전한 사용을 위한 관리에 중요한 시스템 입력, 사용 및 운영 측면의 품질을 포함하여 운영 요소 및/또는 의도된 사용을 식별합니다. • 민감한 사용 사례를 공개 및 문서화합니다. • 자동화 편향(시스템이 생성한 출력을 과도하게 신뢰하는 경향성)을 방지하기 위해 시스템 설계에 효과적인 통제 수단을 구현하고 이를 문서화합니다. • 의도된 사용에 영향을 미칠 수 있는 설계되거나 평가되지 않은 시스템 사용을 포함하여, 시스템 제한, 입력 또는 출력 데이터 모델 제한 또는 예측 가능한 장애를 문서화합니다. • 추론 조작(“탈옥”), 모델 조작(예: 데이터 포이즈닝) 및 추론 정보 공개(예: 프롬프트 추출)와 같은 잘 알려진 AI 위험에 대한 완화 조치와 통제 조치를 구현하고 이를 문서화합니다. • 시스템 정확도, 성능, 그리고 이러한 결과가 사용 사례 전반에 일반화될 수 있는 범위에 대한 증거.

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 K: AI 시스템(계속)	
66	공급자는 민감한 사용 및 의도된 사용의 투명성 공개를 업데이트하고, 다음과 같은 경우에 Microsoft에 통지합니다. • 새로운 사용이 추가됨 • 기능이 변경됨 • 제품이 새로운 릴리스 단계로 이동함 • 의도된 사용에 영향을 미치는 신뢰할 수 있고 안전한 성능에 대한 새로운 정보 • 시스템 정확도 및 성능에 대한 새로운 정보가 제공되는 경우.	공급자는 투명성 정보 공개 업데이트 시 본 섹션에 설명된 대로 Microsoft에 통지하는 조치가 포함된 계획을 마련해두고 있습니다.
67	투명성 공개의 일환으로, 공급자는 다음을 포함하여 각각의 AI 시스템 또는 데이터 모델을 위한 표준 운영 절차 및 시스템 상태 모니터링 실행 계획을 문서화해야 합니다. • 문제 해결을 지원하고 향후 장애를 방지하기 위해 시스템 장애를 재현하는 프로세스 • 모니터링할 이벤트 • 검토를 위해 이벤트의 우선순위를 지정하는 방법 • 그러한 검토의 예상 빈도 • 이벤트에 대한 대응 및 해결 시간의 우선순위를 지정하는 방법 • 오픈 소스 소프트웨어를 포함한 제3자 AI 구성 요소를 최신 상태로 유지.	공급자는 본 섹션에 설명된 대로 각각의 AI 시스템에 대해 따라야 하는 시스템 상태 모니터링 정책과 절차를 문서화했습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.
68	다음을 포함하여, 사용해야 하는 시스템 상태 모니터링 방법에 대한 상세한 인벤토리를 수립하고 문서화합니다. • 데이터 리포지터리, 시스템 분석, 관련 경보로부터 생성된 데이터와 인사이트	공급자는 본 섹션에 설명된 대로 시스템 상태 모니터링 방법을 문서화했습니다. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.

	• 고객이 실패 및 우려 사항에 대한 정보를 제출하는 프로세스, 및 • 일반 대중이 피드백을 제출하는 프로세스.	

#	Microsoft 공급자 데이터 보호 요건	규정준수의 증거
	섹션 K: AI 시스템(계속)	
69	시스템 사용 이전 또는 도중의 어느 시점에 AI 시스템이 의도된 사용에 적합하지 않다는 증거를 발견한 경우, 공급자는 • 고객의 대면하는 자료에서 의도된 사용을 삭제하고, 현재 고객에게 문제에 대해 통지하고, 식별된 격차를 좁히거나 시스템 사용을 중단하는 조치를 취하고 • 의도된 사용과 관련된 문서를 수정하고 • 수정된 문서를 고객에게 공개합니다.	공급자는 본 섹션에 설명된 대로 의도된 사용의 실패에 대해 따라야 하는 정책과 절차를 문서화했습니다.
70	공급자는 AI 시스템의 의도된 사용을 기반으로 더 나쁜 경험을 하거나 부정적인 서비스 품질을 받을 수 있는 소외된 그룹을 포함하여 알려진 모든 인계통계학적 그룹, AI 시스템이 배포된 지리적 영역 또는 AI 시스템 내에 내재된 편향을 식별해야 합니다. 인구통계학적 그룹에는 다음이 포함됩니다. • 단일 요소에 의해 정의된 그룹, 및 • 복합 요소에 의해 정의된 그룹.	공급자는 다음을 설명하는 정황적 요소 및 기타 운영 요소(예: 음성 인식 시스템의 “배경 소음”)와 같은 정당한 요소를 식별하고 문서화해야 합니다. • 식별된 인구통계학적 그룹에 대해 목표로 하는 최소 성능 수준을 충족할 수 없음 • 식별된 인구통계학적 그룹 간에 존재하는 성능 차이. 공급자는 요청 시 Microsoft에 증빙 문서를 제공합니다.

용어집

"**위임 대리인(Authorized Representative)**"이란 회사를 대신하여 서명할 적절한 수준의 권한을 가진 사람입니다. 해당인은 SSPA 프로그램 조치에 대한 응답을 제출하기 전에 필요한 개인정보보호 및 보안 지식을 가지고 있거나 주제 전문가와 상의합니다. 또한 SSPA 양식에 자신의 성명을 추가함으로써 DPR을 읽고 이해했음을 증명합니다.

"**EUDPR**"이란 유럽연합 기관, 기구, 사무소 및 대행사의 개인 데이터 처리와 관련된 자연인 보호 및 해당 정보의 자유로운 이동 및 폐지되는 규정(EC) No. 45/2001 및 결정 No. 1247/2002/EC에 관한 유럽 의회 및 평의회의 규정(EU) 2018/1725(2018년 10월 23일)를 말합니다.

"**프리랜서(Freelancer)**"란 디지털 플랫폼 또는 그 밖의 수단을 통해 조달되는 온디맨드형 작업 또는 서비스를 수행하는 개인을 말합니다.

"**GDPR**"이란 개인 데이터의 처리 및 해당 데이터의 자유로운 이동과 관련된 자연인 보호 및 폐지되는 지침 95/46/EC(일반 데이터보호법)에 관한 유럽 의회 및 평의회 규정(EU) 2016/679(2016년 4월 27일)를 말합니다.

"인간의 감독(Human Oversight)" 이란 의도된 사용에서 AI 시스템 내의 장애가 감지될 경우 적용되는 것으로 공급자가 인간의 감독 및 개입 레벨을 지정한 카테고리입니다.

- 휴먼인더루프(Human-in-the-loop)(시스템의 각 의사 결정 주기에 있어 인간의 개입 역량)
- 휴먼온더루프(Human-on-the-loop)(시스템 설계 주기 중, 그리고 시스템 운영을 모니터링하는 인간의 개입 역량)
- 휴먼인커멘드(Human-in-command)(AI 시스템의 전반적인 활동을 감독하고 특정 상황에서 AI 시스템을 사용하는 시기와 방법을 결정하는 능력)

"**개인정보 데이터 보호 요건(Privacy Data Protection Requirement)**"이란 GDPR, EUDPR, 지역 EU/EEA 데이터보호법, 캘리포니아소비자개인정보 보호법 캘리포니아 민법 § 1798.100 et seq.(*"CCPA"*), 2018년 영국데이터보호법 및 영국에서 적용되는 모든 관련 또는 후속 법률, 규정 및 (a) 개인정보 및 데이터 보안과 관련된 그 밖의 법적 요건 또는 (b) 개인 데이터의 사용, 수집, 보유, 저장, 보안, 공개, 이전, 폐기 및 그 밖의 처리를 말합니다.

"EU 모델 조항(EU Model Clause)" 및 "표준계약조항(Standard Contractual Clause)" 이란 (i) GDPR 제46조에 설명되어 있고 2021년 6월 4일 유럽연합 집행위원회 결정(EU) 2021/914에서 승인한 대로 적절한 수준의 데이터 보호를 보장하지 않는 제3국에 설립된 처리자에게 개인 데이터를 이전하기 위한 표준 데이터 보호 조항, (ii) (a) 유럽집행위원회, (b) 유럽데이터보호감독기구가 채택하고 유럽집행위원회, (c) 영국 일반연방데이터보호법에 따라 영국, (d) 스위스 연방데이터보호법에 따라 스위스에서 승인한 모든 후속 표준계약조항 또는 (e) 스위스, 영국 및 유럽연합/유럽경제지역을 구성하는 관할권 이외의 관할권 내 정부에서 개인 데이터의 국외 이전을 규율하는 조항이 포함되어야 하며 채택일을 기준으로 공급자에게 법적 구속력이 있는

조항을 말합니다.

"**웹사이트 호스팅(Website Hosting)**" 웹사이트 호스팅 서비스는 Microsoft 도메인에서 Microsoft를 대신하여 웹사이트를 생성 및/또는 유지관리하는 온라인 서비스입니다. 즉, 공급자는 사이트를 구축하고 유지관리하는 데 필요한 모든 자료와 서비스를 제공하고 인터넷에서 접근할 수 있도록 합니다. "웹 호스팅 서비스 제공자" 또는 "웹 호스트"란 광고용 쿠키 또는 웹 비콘과 같이 인터넷에서 웹사이트 또는 웹페이지를 보는 데 필요한 도구 및 서비스를 제공하는 공급자입니다.