Microsoft 공급업체 데이터 보호 요구 사항

적용 가능성

Microsoft 공급업체 데이터 보호 요구 사항(“**DPR**”)은 Microsoft와 체결한 계약 조건(예: 구매 주문 조건, 마스터 계약)(“**업무 수행,**” “**서비스 제공**” 또는 “**성과**”)에 따라 공급업체의 업무 수행(예: 서비스 프로비전, 소프트웨어 라이선스, 클라우드 서비스)과 관련해서 Microsoft 개인 데이터 또는 Microsoft 기밀 데이터를 처리하는 각 Microsoft 공급업체에 적용됩니다.

- 여기에 포함된 요구 사항과 공급업체 및 Microsoft 간 계약에 지정된 요구 사항이 상충할 경우 DPR이 우선합니다. 단, 해당 공급업체가 DPR 증명 양식에서 해당 DPR 섹션과 상충하는 계약의 올바른 프로비전을 식별하는 경우에는 계약 조건이 우선합니다.
- 여기에 포함된 요구 사항과 법적 또는 법정 요구 사항이 상충할 경우 법적 또는 법정 요구 사항이 우선합니다.
- Microsoft 공급업체가 컨트롤러로 운영되는 경우 이 DPR과 관련해서 섹션 J 보안과 섹션 A 관리의 요구 사항만 해당 공급업체의 처리 활동에 적용됩니다.
- Microsoft 공급업체가 Microsoft 개인 데이터는 처리하지 않고 Microsoft 기밀 데이터만 처리하는 경우 이 DPR과 관련해서 섹션 A 관리, 섹션 E 보존 및 섹션 J 보안의 요구 사항만 해당 공급업체의 Microsoft 기밀 데이터 처리에 적용됩니다.

데이터 국제 전송

기타 의무를 제한하지 않고, 공급업체는 Microsoft가 사전 서면 승인하지 않은 경우 Microsoft 개인 데이터를 국제 전송하지 않으며, 어떠한 경우에도 표준 계약 조건, 귀속된 회사 규정 또는 데이터 보호 기관인 유럽데이터보호위원회(European Data Protection Board) 또는 유럽연합 집행위원회(European Commission)에서 승인하고 Microsoft에서 채택하거나 동의한 기타 제도(EU-U.S. 및 Swiss-U.S. 개인 정보 보호 프레임워크와 EU 일반 데이터 보호 규정 포함)의 데이터 보호 요구 사항을 준수합니다. 공급업체는 개인 정보 보호 원칙에서 요구하는 동일한 수준의 보호를 제공하는 의무를 더 이상 이행할 수 없다고 결정하는 경우 Microsoft에 알리는 데 동의합니다. 공급업체는 모든 하위 프로세서(유럽연합 집행위원회 결정 C(2010)593의 부록으로 게시된 2010년 표준 계약 조항의 1(d)절에 명시)도 준수합니다.

주요 정의

이 DPR에서 사용된 용어의 의미는 다음과 같습니다. 이 DPR에서 사용된 “포함”, “등”, “예”, “예를 들어” 다음에 나오는 예제 목록은 "오직" 또는 "단지" 등의 단어로 한정되지 않는 한, "제한 없이" 또는 "이에만 국한되지 않고" 포함하는 것으로 해석됩니다.

“**Microsoft 개인 데이터**”는 Microsoft에서 처리하거나 Microsoft를 대신하여 처리한 모든 개인 데이터를 의미합니다.

“**Microsoft 기밀 데이터**”는 관련 기밀성 또는 무결성을 유지하지 않을 경우 Microsoft에 상당한 명예 또는 재정적 손실을 초래할 수 있는 모든 정보를 의미합니다. Microsoft 하드웨어 및 소프트웨어 제품, 내부적 기간 업무 응용 프로그램, 시험판 마케팅 자료, 제품 라이선스 키, Microsoft 제품 및 서비스 관련 기술 설명서가 포함됩니다.

“**개인 데이터**”는 식별되거나 식별 가능한 자연인(“**데이터 주체**”)과 관련된 모든 정보를 의미합니다. 식별 가능한 자연인이란 예를 들어 이름, 식별번호, 위치 데이터, 온라인 식별자와 같은 식별자나 해당 자연인의 신체적, 생리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성과 관련된 하나 이상의 요소를 참조하여 직간접적으로 식별 가능한 사람입니다.

"**데이터 주체 권한**"은 법률에 따라 요구되는 경우 해당 데이터 주체의 Microsoft 개인 데이터 처리를 액세스, 삭제, 편집, 내보내기, 제한 또는 반대할 수 있는 데이터 주체의 권한을 의미합니다.

"**데이터 침해**"는 전송, 저장 또는 다른 방법으로 처리되는 개인 데이터 또는 Microsoft 기밀 데이터의 우발적 또는 불법적 삭제, 손실, 변경, 무단 공개, 액세스 등을 초래하는 보안 위반을 의미합니다.

"**법률**"은 관할권이 있는 정부 기관(연방, 주, 지방 또는 국제)의 모든 관련 법률, 규칙, 법규, 법령, 결정, 명령, 규정, 판결, 관례, 입법, 결의 및 요구 사항을 의미합니다. "**불법**"은 위법 행위를 의미합니다.

"**처리**"는 Microsoft 개인 데이터 또는 기밀 데이터에 대해 수행하는 수집, 기록, 조직, 구성, 저장, 적응 또는 변경, 검색, 참조, 사용, 전송, 배포 또는 다른 제공 방법을 통한 공개, 맞춤 또는 조합, 제한, 지우기 또는 삭제 등과 같은 자동이나 자동이 아닌 방식의 작업을 의미합니다. "처리하는" 및 "처리된"은 동일한 의미가 있습니다.

"**컨트롤러**"는 단독으로 또는 다른 사람과 더불어 개인 데이터 처리의 목적과 수단을 결정하는 자연인 또는 법인, 공공 기관, 대리인 또는 기타 단체를 의미합니다. 여기서 처리의 목적과 수단은 유럽연합("**EU**") 또는 회원국의 법률에 따라 결정되며, 컨트롤러(또는 컨트롤러 지명 기준)는 해당 법률에 따라 지정될 수 있습니다.

"**프로세서**"는 컨트롤러를 대신해서 개인 데이터를 처리하는 자연인 또는 법인, 공공 기관, 대리인 또는 기타 단체를 의미합니다.

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 A: 관리		
1	Microsoft와 공급업체 간의 각 관련 계약(예: 마스터 계약, 작업 명세서, 구매 주문 및 기타 주문)에는 해당하는 경우 Microsoft 개인 데이터 및 기밀 데이터와 관련된 개인 정보 및 보안 데이터 보호 규정이 포함됩니다. 프로세서로 운영되는 회사의 경우 처리의 대상 및 기간, 처리의 특성 및 목적, Microsoft 개인 데이터의 유형, 데이터 주체의 범주, Microsoft의 권리와 의무가 계약에 포함되어야 합니다.	공급업체는 Microsoft와 공급업체 간의 관련 계약을 제공해야 합니다. 프로세서의 경우 처리 설명이 관련 계약에 포함됩니다(*예:* 작업 명세서, 구매 주문). 참고: 진행 중인 구매 주문이 있는 회사에는 구매 과정에서 나중에 추가되는 처리 활동에 대한 필요한 설명이 있을 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
2	DPR을 준수할 의무와 책임을 지정된 사내 담당자나 그룹에 할당합니다.	Microsoft 공급업체 DPR 준수 책임이 있는 개인이나 그룹의 이름입니다. 이 개인이나 그룹의 권한과 책임을 설명하는 문서로, 개인 정보 보호 및/또는 보안 역할을 보여 줍니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
3	Microsoft 개인 데이터 또는 기밀 데이터에 액세스할 직원에 대한 연간 개인 정보 보호 및 보안 교육을 수립, 유지 및 수행합니다. 회사에 준비된 콘텐츠가 없는 경우 이 스토리보드 개요를 사용하고 회사에 맞게 조정할 수 있습니다.	연간 참석 기록을 사용할 수 있습니다. 교육 콘텐츠에는 개인 정보 보호 및 보안 원칙이 포함됩니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
4	Microsoft의 문서화된 지침에 의거해서만 Microsoft 개인 데이터를 처리합니다. 예를 들어 법률에서 요구하는 경우 외에는 Microsoft 개인 데이터를 제삼국이나 국제 조직에 전송해서는 안 됩니다. 그러한 경우 프로세서(공급업체)는 해당 법률에서 중요한 공공 이익을 이유로 이러한 정보를 금지하지 않는 한, 처리하기 전에 법적 요구 사항을 컨트롤러(Microsoft)에게 알립니다.	계약(예: 작업 명세서 또는 구매 주문)에 설명되어 있거나 업무 수행에서 사용되는 전자 시스템의 일부로 캡처된 지침의 문서화된 증빙입니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 B: 알림		
5	공급업체는 Microsoft를 대신하여 개인 데이터를 수집할 경우 Microsoft 개인정보처리방침을 사용해야 합니다. 데이터 주체가 개인 데이터를 공급업체에 제출할지를 결정하는 데 도움이 되도록 개인 정보 알림은 명확하고 데이터 주체가 사용할 수 있어야 합니다. 참고: 회사가 처리 활동의 컨트롤러인 경우 자체 개인 정보 알림을 게시합니다. *올바른 Microsoft 알림에 액세스하려면 SSPAHelp@microsoft.com 으로 문의하십시오.*	공급업체는 게시된 최신 Microsoft 개인정보처리방침에 대한 fwdlink를 사용합니다. 개인정보처리방침은 사용자의 개인 데이터가 수집되는 모든 컨텍스트에 게시됩니다. 해당하는 경우 오프라인 버전을 사용할 수 있으며, 데이터를 수집하기 전에 제공됩니다. 사용되는 오프라인 개인정보처리방침은 게시된 최신 버전이며 올바르게 날짜가 명시됩니다. Microsoft 직원 서비스의 경우 Microsoft Data Protection 고지사항이 사용됩니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
6	공급업체는 라이브 또는 녹음된 음성 통화를 통해 Microsoft 개인 데이터를 수집할 때 해당 데이터 수집, 처리, 사용 및 보존 방식을 데이터 주체와 논의할 준비를 해야 합니다.	음성 녹음의 스크립트에는 Microsoft 개인 데이터의 처리 방법과 다음이 포함됩니다. ▪ 수집 ▪ 사용 ▪ 보존	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 C: 선택 기회 및 동의		
7	공급업체에게 데이터 처리에 대한 법적 근거로 동의가 필요한 경우 공급업체는 데이터 주체의 개인 데이터를 수집하기 전에 모든 처리 활동(새 처리 활동 및 업데이트된 처리 활동 포함)에 대한 데이터 주체의 동의를 얻고 이를 기록해야 합니다.	공급업체는 데이터 주체가 처리 활동에 대한 동의를 제공하는 방법 및 동의의 범위에 데이터 주체의 개인 데이터와 관련된 공급업체의 모든 처리 활동이 포함됨을 보여 줄 수 있습니다. 공급업체는 데이터 주체가 처리 활동에 대한 동의를 철회하는 방법을 보여 줄 수 있습니다. 공급업체는 새 처리 활동을 시작하기 전에 기본 설정을 확인하는 방법을 보여 줄 수 있습니다. 공급업체는 기본 설정 관리의 효율성을 모니터링하여 기본 설정 변경을 반영하는 시간이 적용되는 가장 제한적인 지역 법률 요구 사항인지 확인합니다. 참고: 증빙은 사용자 조작 스크린샷, 서비스 실험 또는 기술 설명서를 확인할 기회일 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 C: 선택 및 동의(계속)		
8	쿠키는 웹 사이트 및/또는 응용 프로그램에서 장치에 저장하는 작은 텍스트 파일로 데이터 주체나 장치를 인식하는 데 사용되는 정보를 포함합니다. Microsoft 웹 사이트 및/또는 응용 프로그램을 만들고 관리하는 공급업체는 데이터 주체에게 쿠키 사용과 관련된 투명한 알림 및 선택 항목을 제공해야 합니다. Microsoft 웹 사이트 및/또는 응용 프로그램을 만들고 관리하는 공급업체는 쿠키 사용이 Microsoft 개인정보처리방침의 약정 및 EU에서 설정한 규칙과 같은 지역 법률 요구 사항에 부합되는지 확인해야 합니다.	각 쿠키의 용도를 문서화해야 하며 구현된 쿠키 유형을 알려야 합니다. ▪ 세션 쿠키로 충분할 때는 영구 쿠키를 사용하면 안 됩니다. ▪ 영구 쿠키를 사용할 때는 사용자가 사이트를 방문한 후 2년을 초과하는 만료 날짜를 지정하면 안 됩니다. EU 사용자의 경우 영구 쿠키의 만료 날짜는 13개월을 초과하면 안 됩니다. 해당하는 경우 다음과 같은 EU 법률 준수를 확인합니다. ▪ 개인정보처리방침에 레이블 지정 규칙 “개인 정보 및 쿠키” 사용 ▪ 광고와 같은 "꼭 필요하지 않은" 용도로 쿠키를 사용하려면 먼저 확실한 사용자 동의 확보	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 D: 수집		
9	공급업체는 Microsoft 개인 데이터 및/또는 기밀 데이터의 수집을 모니터링하여 업무 수행에 필요한 데이터만 수집되는지 확인해야 합니다.	공급업체는 수집되는 Microsoft 개인 데이터 및/또는 기밀 데이터가 업무 수행에 필요함을 보여 주는 문서를 제공할 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
10	공급업체는 Microsoft 대신 제3자로부터 개인 데이터를 수집하는 경우 제3자 데이터 보호 정책 및 사례가 Microsoft 및 DPR을 포함하는 공급업체 계약과 일치하는지 확인해야 합니다.	공급업체는 제3자의 데이터 보호 정책 및 사례와 관련해서 수행된 실사에 대한 문서를 제공할 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
11	데이터 주체의 장치에 실행 가능한 소프트웨어를 설치하거나 활용하는 과정에서, Microsoft 개인 데이터를 수집하기 전에 이 정보를 수집해야 할 필요성을 Microsoft와의 이행된 공급업체 계약에 문서화해야 합니다.	데이터 주체의 장치에서 실행 가능한 소프트웨어를 사용할 경우의 Microsoft 계약은 실행된 계약에 명시됩니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
12	중요한 Microsoft 개인 데이터(인종 또는 민족 출신, 정치적 견해, 종교나 철학적 신념 또는 노동 조합원을 노출하는 데이터, 유전자 데이터, 생체 데이터, 건강 관련 데이터 또는 자연인의 성생활이나 성적 취향 관련 데이터)를 수집하기 전에 Microsoft 개인 데이터를 수집해야 할 필요성을 Microsoft와의 이행된 공급업체 계약에 문서화해야 합니다.	중요한 Microsoft 개인 데이터를 수집해야 하는 필요성은 Microsoft와의 이행된 계약에 명시됩니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 E: 보존		
13	Microsoft 개인 데이터 및 기밀 데이터는 법률에서 Microsoft 개인 데이터 및/또는 기밀 데이터 보존을 계속 요구하는 경우가 아니면, 업무 수행에 필요한 기간만 보존해야 합니다.	공급업체는 계약(예: 작업 명세서 또는 구매 주문)에서 Microsoft가 지정한 문서화된 보존 정책이나 보존 요구 사항을 준수합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
14	Microsoft의 자유재량에 따라, 공급업체가 소유하거나 관리하는 Microsoft 개인 데이터 및 기밀 데이터는 업무 수행이 완료되거나 Microsoft의 요청이 있을 때 Microsoft로 반환하거나 폐기해야 합니다. 응용 프로그램에서 사용자에 의해 명시적으로 또는 데이터 보존 기관과 같은 다른 트리거를 기반으로 데이터가 제거될 때 데이터가 안전하게 삭제되도록 하기 위한 프로세스가 응용 프로그램 내에 있어야 합니다. Microsoft 개인 데이터 또는 기밀 데이터를 폐기해야 하는 경우 공급업체는 Microsoft 개인 데이터 및/또는 기밀 데이터가 포함된 실제 자산을 소각하거나 분쇄하거나 파기하여 정보를 읽거나 다시 구성할 수 없게 해야 합니다.	Microsoft 개인 데이터 또는 기밀 데이터의 처리 기록을 유지 관리합니다(폐기를 위해 Microsoft에 반환하는 경우도 포함될 수 있음). Microsoft에서 폐기를 요구하거나 요청하는 경우 공급업체 담당자가 서명한 폐기 인증서를 제공합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 F: 데이터 주체		
	데이터 주체는 개인 데이터 처리를 액세스, 삭제, 편집, 내보내기, 제한 및 반대할 수 있는 권한("**데이터 주체 권한**")이 있습니다. 데이터 주체가 Microsoft 개인 데이터와 관련해서 법률에 따라 해당 권한을 행사하려고 하는 경우 공급업체는 다음을 수행해야 합니다.		
15	가능한 한 적절한 기술 및 조직적 수단을 통해 Microsoft가 데이터 주체 권한을 행사하려는 데이터 주체의 요청에 대처할 의무를 이행하도록 지원합니다.	데이터 주체 권한 실행을 지원하기 위한 프로세스와 절차가 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
16	모든 데이터 주체 권한 요청에 바로 응답합니다.	공급업체는 정기 테스트를 수행하여 데이터 주체 권한을 지원할 수 있는지 확인합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
17	Microsoft에서 달리 안내한 경우 외에는 공급업체는 공급업체에 문의하는 모든 데이터 주체를 Microsoft로 직접 안내하여 데이터 주체 권한을 행사하도록 합니다. 공급업체는 개인이 자신의 Microsoft 개인 데이터에 액세스하거나 그 외 개인 데이터 관련 권한을 행사하기 위해 수행해야 하는 단계를 데이터 주체에게 전달합니다. *이 요구 사항과 관련된 도움을 받으려면 SSPAHelp@microsoft.com으로 문의하십시오.*	공급업체는 개인 데이터에 액세스하기 위해 수행할 단계와 해당 데이터를 업데이트하는 데 사용할 수 있는 방법을 전달합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
18	데이터 주체에 직접 응답할 경우 요청하는 데이터 주체의 ID를 확인합니다.	공급업체는 Microsoft 데이터 주체를 식별하는 데 사용되는 방법을 문서화했습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 F: 데이터 주체(계속)		
	데이터 주체가 인증되면 공급업체는 다음을 수행해야 합니다.		
19	해당 데이터 주체에 대한 Microsoft 개인 데이터를 보유할지 또는 관리할지를 결정합니다.	공급업체에 개인 데이터가 보유되는지 여부를 설정하기 위한 절차가 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
20	요청된 Microsoft 개인 데이터를 찾기 위한 적절한 노력을 기울이고, 적절한 검색이 수행되었음을 입증하는 충분한 기록을 보유합니다.	공급업체는 데이터 주체 권한 요청을 충족하기 위해 수행되는 단계를 보여 주는 기록을 유지 관리합니다. 문서에는 다음이 포함됩니다. ▪ 요청 날짜/시간 ▪ 요청에 응답하기 위해 수행된 작업 ▪ Microsoft가 알림을 받은 시기의 기록	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
21	데이터 주체 권한 요청이 있던 날짜와 시간, 이러한 요청에 응답하기 위해 공급업체가 취한 조치를 기록합니다. 요청이 있을 때 Microsoft에 데이터 주체 요청 관련 기록을 제공합니다.	공급업체는 액세스 요청 기록을 유지 관리하고 개인 데이터 변경 내용을 문서화합니다.	
	데이터 주체가 인증되고 공급업체가 Microsoft 개인 데이터가 요청되었음을 확인한 후에 공급업체는 다음을 수행해야 합니다.		
22	개인 데이터 사본을 요청하는 경우 인쇄, 전자, 구두 등 적절한 형식으로 Microsoft 개인 데이터를 데이터 주체에 제공합니다.	공급업체는 데이터 주체에게 이해할 수 있는 형식 및 데이터 주체와 공급업체에 편리한 양식으로 개인 데이터를 제공합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
23	Microsoft의 안내에 따라 요청이 거부되면 Microsoft가 이전에 제공한 관련 지침과 일치하는 서면 설명을 데이터 주체에게 제공합니다. *이 요구 사항과 관련된 도움을 받으려면 SSPAHelp@microsoft.com으로 문의하십시오.*	요청이 거부된 사례를 문서화하고 Microsoft 검토 및 승인에 대한 증빙을 유지합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 F: 데이터 주체(계속)		
24	공급업체는 데이터 주체에게 공개된 Microsoft 개인 데이터가 다른 개인을 식별하는 데 사용될 수 없도록 적절한 예방 조치를 취해야 합니다.	공급업체는 공개된 정보에서 다른 개인을 식별할 수 없도록 합리적인 예방 조치를 취했음을 증명해야 합니다(예: 데이터 주체에 대해 요청된 개인 데이터가 한 줄에만 나타나는 경우 전체 데이터 페이지를 복사할 수 없음).	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
25	데이터 주체 및 공급업체가 Microsoft 개인 데이터의 완전성 및 정확성에 대한 의견이 다른 경우 공급업체는 해당 문제를 Microsoft에 에스컬레이션하고 문제 해결에 필요할 경우 Microsoft와 협력해야 합니다. *이 요구 사항과 관련된 도움을 받으려면 SSPAHelp@microsoft.com으로 문의하십시오.*	공급업체는 의견 차이 사례를 문서화하고 문제를 Microsoft에 에스컬레이션합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 G: 제3자에 정보 공개		
	공급업체가 하도급업자에 Microsoft 개인 데이터 또는 기밀 데이터 처리를 의뢰하려는 경우 공급업체는 다음을 수행해야 합니다.		
26	서비스를 하청하거나 하도급업자 추가 또는 교체와 관련된 변경 내용을 수행하기 전에 Microsoft의 명시적 서면 승인을 받습니다. *이 요구 사항과 관련된 도움을 받으려면 SSPAHelp@microsoft.com 으로 문의하십시오.*	관련 계약(예: 작업 명세서, 부록, 구매 주문)에서 필요하거나 SSPA 데이터베이스에 캡처된 것으로 Microsoft에 알려진 회사만 Microsoft 개인 데이터를 처리하는지 확인합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
27	하도급업자가 하청 처리하는 Microsoft 개인 데이터 및 기밀 데이터의 특성과 범위를 문서화하여 업무 수행에 필요한 정보가 수집되도록 합니다.	공급업체는 하도급업자에게 공개되거나 전송된 Microsoft 개인 데이터 및 기밀 데이터 관련 문서를 유지 관리합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
28	하도급업자가 데이터 주체의 명시된 연락처 기본 설정에 따라 Microsoft 개인 데이터를 사용하도록 합니다.	Microsoft 데이터 주체의 기본 설정을 하도급업자가 활용하는 방법을 보여 줍니다. 하도급업자가 기본 설정 변경을 반영하는 시간을 포함하는 지원 문서를 제공합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
29	하도급업자가 Microsoft와 공급업체 간 계약을 이행하는 데 필요한 목적으로만 Microsoft 개인 데이터를 처리하도록 제한합니다.	공급업체는 하도급업자에게 제공되는 Microsoft 개인 데이터가 업무 수행에 필요함을 보여 주는 문서를 제공할 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
30	Microsoft 개인 데이터의 무단 또는 불법 처리 지시에 대한 불만 사항을 검토합니다.	공급업체는 하도급업자에 의한 Microsoft 개인 데이터의 무단 사용이나 공개와 관련된 불만을 해결하기 위한 시스템과 프로세스를 보여 줄 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
31	하도급업자가 업무 수행과 관련된 것 이외의 목적으로 Microsoft 개인 데이터 또는 기밀 데이터를 처리한 것이 확인되면 Microsoft에 즉시 알립니다.	공급업체는 하도급업자가 Microsoft 데이터의 오용을 보고할 수 있는 수단과 지침을 제공했습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 G: 제3자에 정보 공개(계속)		
32	Microsoft 개인 데이터 및 기밀 데이터를 하도급업자가 무단 또는 불법적으로 처리함으로써 야기되는 모든 실제 또는 잠재적 위해 요인을 완화하기 위한 조치를 즉시 취합니다.	공급업체는 하도급업자가 Microsoft 개인 데이터 및 기밀 데이터를 오용하는 경우와 관련된 계획과 절차가 있음을 보여 줄 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
	섹션 H: 품질		
33	공급업체는 Microsoft 개인 데이터가 처리된 목적에 맞게 정확하고 완전하고 적절하도록 모든 정보의 무결성을 유지 관리해야 합니다.	공급업체는 수집, 생성 및 업데이트될 때 Microsoft 개인 데이터의 유효성을 검사하는 절차가 있음을 보여 줄 수 있습니다. 공급업체는 지속적으로 정확성을 확인하고 필요한 경우 수정하는 모니터링 및 샘플링 절차가 있음을 보여 줄 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 I: 모니터링 및 시행		
34	공급업체에 Microsoft 개인 데이터 또는 기밀 데이터에 대한 공급업체 처리와 관련해서 데이터 침해 또는 보안 취약성이 확인되면 바로 Microsoft에 알려야 하는 사고 대응 계획이 있습니다. *사고를 보고하려면 SSPAHelp@microsoft.com 으로 문의하십시오.*	공급업체에 이 섹션에서 설명한 대로 고객(Microsoft)에게 알리는 단계를 포함하는 사고 대응 계획이 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
35	법률이나 규정이 명시적으로 요구하는 경우가 아니면 Microsoft의 승인 없이 Microsoft 개인 데이터 또는 기밀 데이터와 관련된 데이터 침해에 대한 보도 자료나 기타 공지 사항을 발표하지 않습니다.	공급업체는 이벤트가 발생할 경우 이 요구 사항을 이행할 것에 동의합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
36	수정 계획을 구현하고 Microsoft 개인 데이터 또는 기밀 데이터와 관련된 데이터 침해 및 취약성의 해결 상황을 모니터링하여 적절한 시기에 적합한 정정 작업이 수행되도록 합니다.	공급업체는 데이터 침해에 대응하여 종결하기 위해 수행할 절차를 문서화했습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
37	Microsoft 개인 데이터와 관련된 모든 데이터 보호 불만 사항에 대응하기 위한 공식적인 불만 처리 프로세스를 설정합니다.	공급업체에 Microsoft 개인 데이터와 관련된 불만 사항을 검토하는 수단이 있으며 불만 사항을 해결하는 문서화된 불만 처리 절차가 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안		
	공급업체는 적절한 업계 사례 및 법률의 요구 사항에 따라 Microsoft 개인 데이터 및 기밀 데이터를 보호하고 보관하기 위한 정책 및 절차를 포함하는 정보 보안 프로그램을 설정, 구현 및 유지 관리해야 합니다. 공급업체의 보안 프로그램은 아래의 요구 사항 38~56에 캡처된 표준을 충족해야 합니다.	규정 체계(예: HIPAA, GLBA) 또는 계약 요구 사항을 충족할 필요가 있는 경우에 보호 항목은 나열된 항목을 초과할 수 있습니다. 보안이 적용된 유효한 ISO 27001 또는 SOC 2 보고서로 섹션 J를 대체할 수 있습니다. 이 대체를 적용하려면 SSPAHelp@microsoft.com으로 문의하십시오. 참고: 이러한 인증/보고서의 범위를 설명하는 문서를 제공해야 합니다.	
38	다음을 포함하는 네트워크 보안 평가를 매년 수행합니다. ▪ 새로운 시스템 구성 요소, 네트워크 토폴로지, 방화벽 규칙 등 환경에 대한 주요 변경 내용을 검토합니다. ▪ 취약성 검사를 수행합니다. ▪ 변경 로그를 유지 관리합니다.	공급업체는 네트워크 평가, 변경 로그 및 검사 결과를 문서화했습니다. 필요한 변경 로그는 변경 내용을 추적하고, 변경 사유와 관련된 정보를 제공하고, 지정된 승인자의 이름과 직함을 포함해야 합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
39	공급업체는 모바일 장치에서 액세스하거나 사용하는 Microsoft 개인 데이터 또는 기밀 데이터를 보호하고 사용 제한하는 모바일 장치 정책을 정의, 전달 및 구현합니다.	공급업체는 모바일 장치를 사용하여 Microsoft 개인 데이터 또는 기밀 데이터를 처리하도록 요구하는 준수 모바일 장치 정책의 사용을 보여 줍니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안(계속)		
40	업무 수행을 지원하는 데 사용되는 모든 자산이 고려되고 식별된 소유자가 있어야 합니다. 공급업체는 이러한 정보 자산의 재고를 유지 관리하고, 자산의 허용 가능하고 허가된 사용을 설정하고, 자산을 수명 주기 동안 적절히 보호해야 하는 책임이 있습니다.	업무 수행을 지원하는 데 사용되는 장치 자산의 재고입니다. 이러한 자산의 재고는 다음과 같습니다. ▪ 장치의 위치 ▪ 자산에 있는 데이터의 데이터 분류 ▪ 고용 또는 비즈니스 계약 종료 시 자산 복구에 대한 기록 ▪ 더 이상 필요하지 않은 경우 데이터 저장 미디어 처리에 대한 기록	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안(계속)		
41	공급업체가 관리하는 Microsoft 개인 데이터 또는 기밀 데이터에 무단으로 액세스하지 못하게 하는 액세스 권한 관리 절차를 설정하고 유지 관리합니다.	공급업체는 다음을 포함하는 액세스 권한 관리 계획을 구현했음을 보여 줍니다. ▪ 액세스 제어 절차 ▪ 식별 절차 ▪ 실패한 시도 후 잠금 절차 ▪ 필요한 만큼 자주(90일에 1번 이상) 암호 재설정 ▪ 인증 자격 증명을 선택하기 위한 강력한 매개 변수 ▪ 고용 종료 시 48시간 이내에 사용자 계정 비활성화 공급업체는 최소 권한 원칙을 적용하여 Microsoft 개인 데이터 및 기밀 데이터에 대한 사용자 액세스 권한을 검토하는 프로세스를 설정했습니다. 프로세스에는 다음이 포함됩니다. ▪ 명확히 정의한 사용자 역할 ▪ 역할에 대한 액세스 승인을 검토하고 정당화하는 절차 ▪ Microsoft 데이터에 액세스할 수 있는 역할 내의 사용자에게 그룹/역할에 속하게 된 근거가 문서화되어 있는지 테스트	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안(계속)		
42	Microsoft 개인 데이터 또는 기밀 데이터를 처리하는 데 사용되는 시스템의 보안 패치를 우선 적용하는 패치 관리 절차를 정의 및 구현합니다. 이러한 절차에는 다음이 포함됩니다. ▪ 보안 패치를 우선 적용하도록 정의된 위험 접근 방법 ▪ 긴급 패치를 처리 및 구현하는 기능 ▪ 응용 프로그램 서버 및 데이터베이스 소프트웨어와 같은 운영 체제 및 서버 소프트웨어의 적용 가능성 ▪ 패치로 완화되는 위험 문서화 및 모든 예외 추적 ▪ 제작 회사가 더 이상 지원하지 않는 소프트웨어의 사용 중단에 대한 요구 사항	공급업체는 이 요구 사항을 충족하고 최소한 다음을 포함하는 패치 관리 절차가 구현되어 있음을 보여 줄 수 있습니다. ▪ 우선 순위 지정을 알리는 심각도 할당(심각도 정의가 문서화되어 있습니다.) ▪ 긴급 패치를 구현하는 문서화된 절차 ▪ 제작 회사에서 더 이상 지원하지 않는 운영 체제를 사용하지 않는다는 확인 ▪ 승인 및 예외를 추적하는 패치 관리 기록	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
43	잠재적으로 위험할 수 있는 바이러스 및 악성 소프트웨어 응용 프로그램으로부터 보호하기 위한 서버, 프로덕션 및 교육 데스크톱을 포함하여 Microsoft 개인 데이터 및 기밀 데이터를 처리하는 데 사용되는 네트워크에 연결된 모든 장비에 바이러스 백신 및 맬웨어 방지 보호 소프트웨어를 설치합니다. 맬웨어 방지 대상을 매일 또는 바이러스 백신/맬웨어 방지 보호 소프트웨어 공급업체의 안내에 따라 업데이트합니다. 참고: 이 내용은 Linux를 포함하여 모든 운영 체제에 적용됩니다.	바이러스 백신 및 맬웨어 방지 프로그램이 사용되고 있음을 보여 주는 기록이 있습니다. 참고: 이 요구 사항은 모든 운영 체제에 적용됩니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
44	Microsoft용 소프트웨어를 개발하는 공급업체는 설계에 의한 보안 원칙을 빌드 프로세스에 통합해야 합니다.	공급업체 기술 사양 문서에는 개발 주기의 보안 유효성 검사를 위한 검사점이 포함됩니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안(계속)		
45	데이터 손실 방지("**DLP**") 프로그램을 이용합니다. 데이터가 제대로 분류되고 레이블이 지정되고 보호되어야 하며, 공급업체는 Microsoft 개인 데이터 또는 기밀 데이터가 침입, 손실 및 기타 무단 활동을 위해 처리되는, 사용 중인 정보 시스템을 모니터링해야 합니다. DLP 프로그램은 최소한 다음을 수행합니다. ▪ Microsoft 개인 데이터 또는 기밀 데이터를 보존하는 경우 업계 표준 호스트, 네트워크 및 클라우드 기반 침입 검색 시스템("**IDS**")을 사용하도록 요구합니다. ▪ 데이터 손실을 모니터링하고 적극적으로 중지하도록 구성된 고급 침입 방지 시스템("**IPS**")을 구현하도록 요구합니다. ▪ 시스템이 침해된 경우 시스템을 분석하여 남아 있는 취약성도 해결되었는지 확인하도록 요구합니다. ▪ 시스템 손상 검색 도구를 모니터링하는 데 필요한 절차를 설명합니다. ▪ 데이터 침해 이벤트가 검색될 때 업무 수행에 필요한 사고 대응 및 관리 프로세스를 수립합니다.	취약성이나 데이터 침해가 검색될 때 바로 대응하는 절차와 함께 배포되는 IDS/IPS를 문서화했습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
46	사고 대응의 조사 결과를 상급 관리자와 Microsoft에 신속하게 전달합니다. *Microsoft에 알리려면 SSPAHelp@microsoft.com으로 문의하십시오.*	사고 대응 조사 결과를 Microsoft에 전달하기 위한 시스템과 프로세스가 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
47	시스템 관리자, 운영 직원, 경영진 및 제3자가 매년 보안 교육을 받아야 합니다.	다음을 포함하는 보안 교육 프로그램을 마련합니다. ▪ 사고 대응에 대한 매년 교육 ▪ 위기 상황에 유연하고 효율적으로 대응하는 시뮬레이션 이벤트 및 자동 메커니즘 악성 소프트웨어 다운로드와 관련된 위험과 같은 사고 방지 인식을 제고합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안(계속)		
48	공급업체는 Microsoft 개인 데이터 및 기밀 데이터가 무단 사용, 액세스, 공개, 변경 및 폐기되지 않도록 보호하는 백업 계획 프로세스를 마련해야 합니다.	공급업체는 조직이 중단 이벤트를 관리하고 경영진에서 승인한 정보 보안 연속성 목표에 따라 미리 결정된 수준으로 정보 보안을 유지하는 방법을 자세히 설명하는 문서화된 대응 및 복구 절차를 보여 줄 수 있습니다. 공급업체는 중요 데이터를 정기적으로 백업하고 안전하게 저장하며 효과적으로 복구하는 절차를 정의 및 구현했음을 보여 줄 수 있습니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
49	비즈니스 연속성 및 재해 복구 계획을 설정하고 테스트합니다.	재해 복구 계획에는 다음이 모두 포함되어야 합니다. ▪ 시스템이 공급업체 비즈니스 운영에 중요한지를 결정하기 위한 정의된 기준 ▪ 재해 복구 시 복구의 대상으로 지정해야 하는 정의된 기준에 따른 중요 시스템 목록 ▪ 시스템에 대해 모르는 엔지니어가 72시간 이내에 응용 프로그램 복구할 수 있도록 하는 각 중요 시스템에 대한 정의된 재해 복구 절차 ▪ 복구 목표를 충족할 수 있는지 확인하는 연간(또는 이보다 빈번한) 재해 복구 계획 테스트 및 검토	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안(계속)		
50	Microsoft 개인 데이터 또는 기밀 데이터에 대한 개별 액세스 권한을 부여하기 전에 개인의 ID를 인증합니다.	모든 사용자 ID가 고유하고 각 사용자에게 Azure Active Directory와 같은 업계 표준 인증 방법이 있는지 확인합니다. 높은 권한으로 액세스(관리자 또는 다른 유형의 강화된 권한)하려면 스마트 카드나 휴대폰 기반 인증자와 같은 2단계 인증을 사용해야 합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
51	공급업체는 네트워크에서 전송 중인 Microsoft 개인 데이터 및 기밀 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 있습니다. 이와 동일한 업계 표준도 사용될 수 있습니다. 공급업체는 암호화되지 않은 수단을 통해 전송되는 Microsoft 개인 데이터 또는 기밀 데이터 전달을 거부해야 합니다.	TLS 또는 기타 인증서를 만들고 배포하고 교체하는 프로세스를 정의하고 적용해야 합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
52	Microsoft 개인 데이터 또는 기밀 데이터를 액세스하거나 처리하는 모든 공급업체 장치(노트북, 워크스테이션 등)에는 디스크 기반 암호화를 적용해야 합니다.	Microsoft 개인 데이터 또는 기밀 데이터를 처리하는 데 사용되는 모든 클라이언트 장치에 대해 Bitlocker 또는 이와 동일한 업계 디스크 암호화 솔루션에 맞게 모든 장치를 암호화합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안(계속)		
53	다음을 포함하여 모든 Microsoft 개인 데이터 및/또는 기밀 데이터를 미사용 시(저장되었을 때) 암호화하기 위한 시스템과 절차(NIST 800-111 표준에 설명된 것과 같은 최신 업계 표준 사용)가 있어야 합니다. ▪ 자격 증명 데이터(예: 사용자 이름/암호) ▪ 결제 방식 데이터(예: 신용 카드 및 은행 계좌 번호) ▪ 이민 관련 개인 데이터 ▪ 의료 프로필 데이터(예: 의료 기록 번호, 인증 목적으로 사용되는 DNA, 지문, 눈 망막 및 홍채, 음성 패턴, 얼굴 패턴, 손 측정과 같은 생체 표식 또는 식별자) ▪ 정부에서 발급한 식별자 데이터(예: 사회 보장 번호 또는 운전면허번호) ▪ Microsoft 고객에게 속하는 데이터(예: SharePoint, O365 문서, OneDrive 고객) ▪ 공개되지 않은 Microsoft 제품과 관련된 자료 ▪ 생년월일 ▪ 어린이 프로필 정보 ▪ 실시간 지역 데이터 ▪ 실제 개인(비업무용) 주소 ▪ 개인(비업무용) 전화 번호 ▪ 종교 ▪ 정치적 견해 ▪ 성적 지향/기호 ▪ 본인 확인 질문의 대답(예: 2fa, 암호 재설정) o 어머니의 결혼 전 이름	이 행에 나열된 Microsoft 개인 데이터 및 기밀 데이터가 미사용 시 암호화되는지 확인합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
54	Microsoft를 대신하여 신용 카드를 처리할 때는 카드 발급자에 따라 적절한 신용 카드 처리 표준을 준수합니다.	Payment Card Industry Data Services Standard("**PCI-DSS**") 인증을 매년 제공하여 준수를 증명합니다. *PCI DSS 인증을 SSPA에 제출합니다. 질문이 있으면 SSPAHelp@microsoft.com으로 문의하십시오.*	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*

#	Microsoft 공급업체 데이터 보호 요구 사항	준수 증빙	응답
	섹션 J: 보안(계속)		
55	공급업체는 Microsoft의 물리적 자산을 액세스 제어 환경에 저장해야 합니다.	Microsoft 데이터의 디지털, 하드 카피, 보관 및 백업 복사본에 대한 물리적 액세스를 관리하기 위한 시스템과 프로세스가 있어야 합니다. Microsoft 데이터를 포함하는 물리적 미디어의 이동 및 폐기에 대한 관리 연속성을 추적해야 합니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*
56	개발 또는 테스트 환경에서 사용되는 모든 Microsoft 개인 데이터를 익명화해야 합니다.	Microsoft 개인 데이터는 개발 또는 테스트 환경에서 사용되면 안 됩니다. 대안이 없는 경우에는 데이터 주체 식별이나 개인 데이터 오용을 방지하기 위해 익명화되어야 합니다. 참고: 익명화된 데이터는 의사 익명화된 데이터와 다릅니다. 익명화된 데이터는 식별되었거나 식별 가능한 자연인과 관련이 없어 개인 데이터의 데이터 주체를 현재 또는 더 이상 식별할 수 없는 데이터입니다.	*<준수>* *<비준수>* *<적용되지 않음>* *<법률 상충>* *<계약 상충>*