Microsoft 조달

공급자 보안 및 개인정보보호 보증(SSPA) 프로그램 가이드

버전 11

2025년 4월

목차

Microsoft

SSPA 프로그램 개요

공급자 보안 및 개인정보보호 보증(Supplier Security and Privacy Assurance, "**SSPA**") 프로그램은 당사의 공급자가 개인정보보호 및 보안, 책임 있는 AI 원칙을 따르도록 보장하기 위한 Microsoft 조달팀, 기업 외부 및 법무팀, 기업 보안팀, 책임 있는 AI 사무국 간의 파트너십입니다. 이 기업 프로그램은 Microsoft.com/Procurement의 SSPA 페이지에서 제공되는 Microsoft 공급자 데이터 보호 요건(Data Protection Requirements, DPR)의 형태로 Microsoft의 기본 데이터 처리 지침을 전달하기 위해 마련되었습니다.

공급자는 수행하기로 계약한 상품 및/또는 서비스에 맞게 데이터 처리 프로필을 선택할 수 있습니다. 이러한 선택을 할 경우 Microsoft 규정준수를 보증하기 위해 상응하는 요건이 유발됩니다.

등록된 모든 공급자는 매년 DPR 규정준수에 대한 자체 증명을 완료합니다. 데이터 처리 프로필에 따라 전체 DPR 부과 또는 하위 요건 적용 여부가 결정됩니다. Microsoft에서 위험도가 더 높은 것으로 간주되는 데이터를 처리하는 공급자는 규정준수에 대한 독립적인 검증 등 추가적인 요건을 충족해야 할 수도 있습니다(독립 평가 참조). 공급자는 공급자와의 업무를 담당하는 Microsoft 그룹이 SSPA와 개별적으로 결정하고 전달하는 조직 수준의 추가적인 요건을 준수해야 할 수 있습니다.

중요: 규정준수 활동은 SSPA 상태가 녹색(준수) 또는 빨간색(미준수)인지를 결정하고 데이터 처리를 승인합니다(하기의 데이터 처리 프로필 참조). Microsoft 구매 도구는 업무 진행을 허용하기 전 SSPA 상태가 녹색(SSPA 범위에 속하는 각 공급자에 대해)이고 필수 승인을 받았는지 확인합니다.

SSPA 데이터 처리 프로필

Microsoft 공급자는 SSPA 데이터 처리 프로필을 제어할 수 있습니다. 데이터 처리 프로필에서 선택된 승인은 SSPA가 Microsoft와 체결하는 계약의 위험 수준을 평가하도록 지원합니다. SSPA 규정준수 요건은 데이터 처리 프로필 및 관련 승인에 따라 달라지며 공급자가 어떤 계약에 참여할 자격이 있는지 결정하도록 이끕니다. 승인을 얻기 위해 완료해야 하는 선택 및 규정준수 활동을 주의 깊게 고려하는 것이 중요합니다.

Microsoft 비즈니스 그룹은 데이터 처리 활동이 공급자가 받은 승인과 일치하는 경우에만 공급자와 계약을 체결할 수 있습니다.

공급자는 연중 언제든 진행 중인 작업이 없는 경우 데이터 처리 프로필을 업데이트할 수 있습니다. 변경 사항이 발생하면 해당하는 규정준수 활동(과업)을 발행하고 새로운 승인 사항이 데이터 처리 프로필에 반영되기 전에 완료해야 합니다. 새로 부과된 요건을 완료할 때까지 기존에 완료된 승인이 계속 적용됩니다. 새로 실행된 작업을 허용된 기간인 90일 이내에 완료하지 않으면 SSPA 상태가 빨간색(미준수)으로 바뀌고 계정이 Microsoft 지급 계정 시스템에서 비활성화될 위험이 있습니다.

규정준수 요건을 강화하거나 완화할 수 있는 조합도 있습니다. 이 조합은 부록 A에 나와 있으며 프로필을 작성하면 Microsoft 공급자 규정준수 포털에서 실행할 수 있습니다. SSPA 팀 검토를 요청하여 시나리오가 이 프레임워크에 잘 맞는지 항상 확인할 수 있습니다.

SSPA 데이터 처리 프로필 테이블

#	프로필	요건	독립 보증 옵션
1	**범위**: 개인, 기밀 **처리 위치**: Microsoft 또는 고객 **처리 역할**: 처리자 또는 컨트롤러 **데이터 클래스**: 기밀 또는 고급 기밀 **결제 카드**: 해당 안 됨 **SaaS**: 해당 안 됨 **하도급업자 이용**: 해당 없음 또는 예 **웹 사이트 호스팅**: 해당 없음 또는 예 **의료 서비스**: 해당 없음 또는 예	DPR 준수 자체 증명	
2	**범위**: 기밀 **처리 위치**: 공급자 **처리 역할**: 해당 안 됨 **데이터 클래스**: 기밀 **결제 카드**: 해당 안 됨 **SaaS**: 해당 안 됨 **하도급업자 이용**: 해당 안 됨 **웹 사이트 호스팅**: 해당 안 됨	DPR 준수 자체 증명	

	의료 서비스: 해당 안 됨		
3	**범위**: 기밀 **처리 위치**: 공급자 **처리 역할**: 해당 안 됨 **데이터 클래스**: 고급 기밀 **결제 카드**: 해당 안 됨 **SaaS**: 해당 안 됨 **하도급업자 이용**: 해당 안 됨 **웹 사이트 호스팅**: 해당 안 됨 **의료 서비스**: 해당 안 됨	DPR 규정준수 자체 증명 **및** 독립 규정준수 보증	독립 보증 옵션: 1. DPR에 대한 독립 평가 완료, **또는** 2. ISO 27001 제출
4	**범위**: 개인, 기밀 **처리 위치**: 공급자 **처리 역할**: 처리자 **데이터 클래스**: 고급 기밀 **결제 카드**: 해당 안 됨 **SaaS**: 해당 안 됨 **하도급업자 이용**: 해당 안 됨 **웹 사이트 호스팅**: 해당 안 됨 **의료 서비스**: 해당 안 됨	DPR 규정준수 자체 증명 **및** 독립 규정준수 보증	독립 보증 옵션: 1. DPR에 대한 독립 평가 완료, **또는** 2. DPR 섹션 A-I 및 ISO 27001에 대한 독립 평가, **또는** 3. ISO 27701 및 ISO 27001 제출
5	**범위**: 개인, 기밀 **처리 위치**: 공급자 **처리 역할**: 처리자 **데이터 클래스**: 기밀 **결제 카드**: 해당 안 됨 **SaaS**: 해당 안 됨 **하도급업자 이용**: 해당 안 됨 **웹 사이트 호스팅**: 해당 안 됨 **의료 서비스**: 해당 안 됨	DPR 규정준수 자체 증명	
6	**범위**: 개인, 기밀 **처리 위치**: 공급자 **처리 역할**: 컨트롤러 **데이터 클래스**: 고급 기밀 또는 기밀 **결제 카드**: 해당 안 됨	DPR 규정준수 자체 증명	

	SaaS: 해당 안 됨 **하도급업자 이용**: 해당 없음 또는 예 **웹 사이트 호스팅**: 해당 안 됨 **의료 서비스**: 해당 없음 또는 예		
7	**범위**: 개인, 기밀 **처리 위치**: 모든 위치 **처리 역할**: 하위 처리자(Microsoft가 이 역할을 결정. 프로필에는 '하위 처리자 승인: 예'로 표시) **데이터 클래스**: 고급 기밀 또는 기밀 **결제 카드**: 해당 안 됨 **SaaS**: 해당 안 됨 **하도급업자 이용**: 해당 안 됨 **웹 사이트 호스팅**: 해당 안 됨 **의료 서비스**: 해당 안 됨	DPR 규정준수 자체 증명 **및** 독립 규정준수 보증	독립 보증 옵션: 1. DPR에 대한 독립 평가 완료, **또는** 2. DPR 섹션 A-I 및 ISO 27001에 대한 독립 평가, **또는** 3. ISO 27701 및 ISO 27001 제출
8	**범위**: 개인, 기밀 **처리 위치**: 공급자 **처리 역할**: 처리자 **데이터 클래스**: 고급 기밀 또는 기밀 **결제 카드**: 해당 안 됨 **하도급업자**: 예 또는 **SaaS**: 예 또는 **웹 사이트 호스팅**: 예 또는 **의료 서비스**: 예	DPR 규정준수 자체 증명 **및** 독립 규정준수 보증	독립 보증 옵션: 1. DPR에 대한 독립 평가 완료, **또는** 2. DPR 섹션 A-I 및 ISO 27001에 대한 독립 평가, **또는** 3. ISO 27701 또는 ISO 27001 제출 **또는** 4. HITRUST 보고서(해당되는 독립체 또는 미국 내 의료 서비스 제공자인 경우에만 해당)
	상기 모든 프로필 및 **결제 카드**	해당 되는 상기 요건 **및** 결제 카드 산업 보증	PCI DSS 인증서 제출

	상기 모든 프로필 및 서비스형 소프트웨어(SaaS)	상기 해당 요건 **및** 기능 서비스에 대해 계약상 요구되는 ISO 27001 인증서 제출	제공된 서비스의 기능 범위와 함께 ISO 27001 인증서 제출
	상기 모든 프로필 및 인공지능(AI) 시스템	AI 브랜치를 포함하여 DPR에 대한 규정준수 자체 증명 **및** 독립 규정준수 보증	독립 보증 옵션: 1. AI 브랜치를 포함하여 DPR에 대한 독립 평가 완료, **또는** 2. DPR 섹션 A-I, K 및 ISO 27001에 대한 독립 평가 3. DPR 섹션 K, ISO 27701 및 ISO 27001에 대한 독립 평가, **또는** 4. ISO 27701, ISO 27001 및 ISO 42001 제출* (*ISO 42001은 AI 시스템의 민감한 사용과 관련된 서비스 전달에 필요함)

범위

기밀

공급자의 수행이 Microsoft 기밀 데이터 처리 업무에만 관련된 경우 이 승인을 선택합니다.

이 승인을 선택하면 개인 데이터 처리 업무를 수행할 수 있는 자격이 없습니다.

개인, 기밀

공급자의 수행이 개인 데이터 및 Microsoft 기밀 데이터 처리와 관련된 경우 이 승인을 선택합니다.

귀사(공급자)가 개인 데이터 및/또는 Microsoft 기밀 데이터를 처리하는지 여부를 확인하려면 아래 도표의 사례 목록을 참조하십시오. 해당 목록은 사례일 뿐 전체 목록은 아니라는 점에 유의하시기 바랍니다.

참고: Microsoft 비즈니스 소유자는 처리하는 데이터의 기밀성을 고려하여 이 목록 이외의 등록을 요청할 수 있습니다.

데이터 유형별 개인 데이터

예시에는 다음이 포함되나 이에 국한되지는 않습니다.

민감한 데이터
아동 관련 데이터
유전자 데이터, 생체 데이터 또는 건강 데이터
인종 또는 민족 출신
정치적, 종교적 또는 철학적 신념, 의견 및 소속
노동조합 가입
자연인의 성생활 또는 성적 지향
이민 신분(비자, 취업 허가 등)
정부 식별자(여권, 운전면허증, 비자, 사회보장번호, 주민등록번호)
정확한 사용자 위치 데이터(300미터 이내)
개인 은행 계좌번호
신용카드 번호 및 유효기간, **또는** 계좌 접근을 허용하는 보안/액세스 코드 또는 비밀번호/자격 증명
최종 사용자 가명 정보(End-user Pseudonymized Information, EUPI) (Microsoft 제품 및 서비스의 사용자를 식별하기 위해 Microsoft에서 생성한 식별자) • 전역 고유 식별자(Globally Unique Identifier, GUID)

• 여권 사용자 ID 또는 고유 식별자(Passport User ID or Unique Identifier, PUID) • 해시드 최종 사용자 식별 정보(End-User Identifiable Information, EUII) • 세션 ID • 장치 ID • 진단 데이터 • 로그 데이터 • 지원 사례와 연결된 고객 데이터
고객 콘텐츠 데이터
문서, 사진, 동영상, 음악 등
제품 또는 서비스에 입력된 리뷰 및/또는 평점
설문조사 응답
브라우징 내역, 관심 사항 및 선호 사항
잉크 인자, 타이핑 및 발언(음성/오디오 및/또는 채팅/봇)
자격 증명 데이터(신원 확인에 사용되는 비밀번호, 비밀번호 힌트, 사용자 이름, 생체 데이터)
지원 사례와 연결된 고객 데이터
캡처 및 생성되는 데이터
부정확한 위치 데이터
IP 주소
장치 기본 설정 및 개인 설정
웹 사이트 서비스 이용, 웹 페이지 클릭 추적
소셜 미디어 데이터, 소셜 그래프 관계
피트니스 모니터와 같은 연결된 장치의 활동 데이터

이름, 주소, 전화번호, 이메일 주소, 생년월일, 피부양자 및 비상 연락처와 같은 연락처 데이터
사기 및 위험 평가, 배경 확인
보험, 연금, 수당 내역
지원자 이력서, 면접 기록/피드백
메타데이터 및 텔레메트리
계정 데이터
결제 수단 데이터
신용카드 번호 및 유효기간
은행 라우팅 정보
은행 계좌번호
신용 요청 또는 신용 한도
세금 서류 및 식별자
투자 또는 비용 데이터
법인카드
온라인 고객 데이터
Microsoft 온라인 기업 고객(Azure 테넌트, M365 테넌트 등)
Microsoft 소비자 고객(Xbox Live, OneDrive 소비자)
Microsoft 기업 고객(온프레미스 고객)
지원 데이터(고객이 발행한 티켓)
계정 데이터(결제 데이터, 전자 상거래)
설문 조사/이벤트 등록/교육
보호되는 건강 정보

국가 식별 번호(부족 번호 및 건강 정보 식별 번호 포함)
보호되는 건강 정보(PHI) 컨텍스트에 사용되는 인구 통계 데이터: • 생년월일 • 성별 • 민족 • 생체 데이터 • 안면 사진 • 주소(전체 또는 부분) • 연락처 정보 • 비상 연락처 데이터
민감한 사용(AI 시스템)
다음을 포함하여 법적 지위 또는 생활 기회에 영향을 미칠 수 있는 사용: • 사법 제도 위험 평가 및 채점 시스템 • 고등교육 입학 시스템 • 신용 평가 및 신청 시스템
다음을 포함한 신체적 또는 정신적 부상 위험: • 의학 진단 또는 치료 시스템 • 정신 건강 및 웰빙 시스템 • 장비 제어 및 예방 유지관리 시스템
다음을 포함한 인권에 대한 위협: • 선거에 영향을 미치기 위해 허위 정보 또는 정치적 선전을 생성할 수 있는 합성 미디어 시스템 • 종교적, 정치적 또는 사회적 표현을 기반으로 하는 경보 시스템 • 사회적 신용 평가

Microsoft 기밀 데이터

예시에는 다음이 포함되나 이에 국한되지는 않습니다.

고급 기밀
Microsoft 제품 또는 Microsoft 제품 구성 요소의 개발, 테스트 또는 제조에 관한 정보 또는 관련 정보 *모든 경로를 통해 상업적으로 판매되는 Microsoft 소프트웨어, 온라인 서비스 또는 하드웨어는 "**Microsoft 제품**" 으로 간주됩니다.* **참고:** 게이밍 제품 개발의 경우 Microsoft 비즈니스 소유자는 작업물에 고급 기밀 또는 기밀 데이터 분류가 있는지 여부를 나타낼 수 있습니다.
Microsoft 기기 사전공개 마케팅 정보
SEC 규칙이 적용되는 미고지 Microsoft 기업 재무 데이터

기밀
모든 수단으로 배포하기 위해 Microsoft를 대신하는 Microsoft 제품 라이선스 키
Microsoft 내부 영업군(Line of Business, LOB) 애플리케이션의 개발 또는 테스트에 관한 정보 또는 관련 정보
Office, SQL, Azure 등 Microsoft 소프트웨어 및 서비스용 Microsoft 사전공개 마케팅 자료
기기(처리 또는 절차 가이드, 구성 데이터 등)와 같은 Microsoft 서비스 또는 제품에 대한 문서의 작성, 설계, 전자 기록 또는 인쇄 기록

중요: Microsoft 비즈니스 소유자는 본 목록에 포함되지 않은 데이터에 대한 참여를 요구할 수 있습니다.

처리 위치

Microsoft 또는 고객

직원이 @microsoft.com 액세스 자격 증명을 사용하는 Microsoft 네트워크 환경 내에서 또는 Microsoft 고객 환경 내에서 공급자의 수행이 공급자의 데이터 처리와 관련된 경우 이 승인을 선택합니다.

다음과 같은 상황에서는 이 옵션을 선택해서는 안 됩니다.

- 공급자가 Microsoft가 지정한 해외 시설(Offshore Facility, OF)을 관리합니다.
- 공급자가 Microsoft에 리소스를 제공하며 경우에 따라 Microsoft 네트워크 내외에서 작업합니다. 네트워크 외부 작업을 위한 처리 위치는 "공급자"로 간주됩니다.

공급자

"Microsoft 또는 고객" 조건(상기 설명됨)이 적용되지 않는 경우 이 옵션을 선택하십시오.

데이터 처리 역할

컨트롤러

공급자가 진행하는 수행의 모든 측면이 컨트롤러 데이터 처리 역할의 정의에 부합하는 경우 이 승인을 선택합니다(DPR 참조).

이 승인을 선택하면 '처리자' 역할 지정으로 개인 데이터 처리 업무를 수행할 자격이 없습니다. 공급자가 Microsoft의 처리자 및 컨트롤러인 경우 '컨트롤러'를 선택하지 마시고 처리자를 선택하십시오.

처리자

처리자는 공급자가 Microsoft를 대신해 데이터를 처리할 때 가장 일반적인 처리 역할입니다. DPR에서 처리자의 정의를 검토하십시오.

하위 처리자

공급자는 내부 개인정보보호 팀의 사전 승인을 받아야 하기 때문에 자체적으로 Microsoft의 하위 처리자로서 신원을 규정할 수 없습니다. DPR에서 하위 처리자의 정의를 검토하십시오. 하위 처리자의 경우 데이터 보호 부록 및 독립 평가(아래 참조)를 비롯한 추가 계약 및 규정준수 요건이 적용됩니다. 공개된 Microsoft 하위 처리자 목록에 포함된 공급자는 규정준수에 대한 독립적인 검증을 제공해야 합니다.

결제 카드 처리

공급자가 처리하는 데이터에 Microsoft를 대신하여 신용카드 또는 기타 결제 카드 처리를 지원하는 데이터가 포함된 경우 이 승인을 선택합니다.

이 승인을 통해 공급자는 결제 카드 처리 업무에 참여할 수 있습니다.

PCI 인증 요건

결제 카드 산업데이터보안 표준(Payment Card Industry Data Security Standard, PCI DSS)은 보안 사고에 대한 예방, 감지 및 적절한 대응을 포함하는 강력한 결제 카드 데이터 보안 조치를 개발하기 위한 프레임워크입니다. 이 프레임워크는 자가 규제 산업 조직인 PCI 보안 표준 위원회(PCI Security Standards Council)에서 개발했습니다. PCI DSS 요건의 목적은 카드 소지자 데이터 처리에 보안상 위험을 초래하는 기술 및 처리 취약성을 파악하는 것입니다.

Microsoft는 이러한 표준을 준수해야 합니다. 공급자가 Microsoft를 대신하여 결제 카드 정보를 처리하는 경우 이러한 표준을 준수한다는 증거가 필요합니다. PCI 조직에서 설정한 요건을 이해하려면 PCI 보안 표준 위원회에 문의하십시오.

처리하는 거래량에 따라 공급자는 규정준수에 대해 공인 보안 평가자의 인증을 받아야 하거나 자체 평가 설문지 양식을 작성할 수 있습니다.

결제 카드 회사는 일반적으로 다음과 같이 평가 유형에 대한 최저 기준을 설정합니다.

- 레벨 1: 타사 평가자 PCI AOC 인증서 제공
- 레벨 2 또는 3: 공급자 담당자가 서명한 PCI DSS 자체 평가 설문지(Self-Assessment Questionnaire, SAQ) 제공

PCI 요건 적용 및 준수 인증서를 제출해 주십시오. Microsoft 고객 결제 데이터를 처리 또는 저장하는 공급자는 서비스 제공자로서 현재 PCI 티어 1 인증을 획득해야 합니다.

서비스형 소프트웨어(SaaS)

사용자는 서비스형 소프트웨어(SaaS)를 통해 인터넷으로 클라우드 기반 애플리케이션에 접속하고 해당 서비스를 이용할 수 있습니다. SSPA 규정준수 목적상, SaaS를 서비스형 플랫폼(Platform as a Service, PaaS) 및 서비스형 인프라(Infrastructure as a Service, IaaS)도 포함하여 광범위하게 확인해야 합니다. (SaaS에 대해 자세히 알아보려면 이 설명을 참조하십시오.)

Microsoft는 사용한 만큼 지불하는(pay-for-use) 일대다 모델에 사용되는 공용 코드를 기반으로 하는 소프트웨어 또는 사용 메트릭을 기반으로 하는 구독으로 **서비스형 소프트웨어(SaaS)**를 정의합니다. 클라우드 서비스 제공자는 클라우드 기반 소프트웨어를 개발 및 유지관리하고, 자동 소프트웨어 업데이트를 제공하며, 일대다 선불(pay-as-you-go) 기반으로 고객이 인터넷을 통해 소프트웨어를 사용할 수 있도록 합니다. 이 소프트웨어 전송 및 라이선싱 방법을 통해 소프트웨어를 구입하여 각각의 개별 컴퓨터에 설치하는 대신 구독을 통해 온라인으로 소프트웨어에 액세스할 수 있습니다.

참고: 개인 데이터 또는 Microsoft 기밀 데이터가 타사 플랫폼 또는 클라우드 인프라 제공자에서 호스팅되는 경우 대부분의 SaaS 공급자는 Microsoft 공급자 규정준수 포털에 하도급업자 승인을 추가해야 합니다.

데이터 처리 프로필에 기재된 SaaS의 정의에 부합하는 공급자는 유효한 ISO 27001 인증서를 제공해야 하니다. 데이터 센터 인증서를 제출하면 안 됩니다. Microsoft와의 계약에 명시된 소프트웨어 서비스에 적용되는 ISO 27001 인증서를 제출해 주십시오.

하도급업자 이용

공급자가 하도급업자를 이용하여 업무를 수행하는 경우 이 승인을 선택합니다.
"**하도급업자(Subcontractor)**"란 Microsoft와 직접 계약하지 않은 공급자 계열사를 포함하여 공급자의 업무 수행을 책임지는 계약과 관련해 공급자가 그 의무를 위임하는 제3자를 말합니다.

여기에는 프리랜서도 해당됩니다(DPR 참조).

Microsoft는 하도급업자 이용을 고위험 요소로 간주합니다. 개인 및/또는 Microsoft 기밀 데이터를 처리하는 하도급업자를 이용하는 공급자는 해당 하도급업자를 공개해야 합니다. 또한 공급자는 각 하도급업자가 해당 개인 데이터를 처리하게 될 국가도 공개해야 합니다.

웹 사이트 호스팅

공급자가 Microsoft를 대신하여 웹 사이트를 호스팅하고 웹 사이트 포털, 온라인 서비스 및/또는 모바일 애플리케이션을 제공할 때 이 프로필 옵션을 선택하십시오.

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.

의료 서비스

공급자가 보호되는 건강 정보를 처리해야 하는 경우 이 프로필 옵션을 선택합니다.

“**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.

인공지능(AI) 시스템

공급자가 이미지, 사운드, 동영상, 인사이트, 분석 및/또는 텍스트와 같이 완전히 새로운 콘텐츠를 생성하기 위해 인텔리전트 시스템을 훈련 및 구축하는 AI 기술을 비롯한 도구, 시스템 또는 플랫폼을 포함하여 AI 시스템과 관련하여 Microsoft에 서비스를 제공하는 경우, 이 프로필 옵션을 선택합니다. 이 조항은 AI 시스템의 게시자(소유, 관리, 통제 등)에게만 해당합니다. Microsoft와 진행하는 업무가 Microsoft Copilot 또는 타사 AI 활용(귀사에서 게시하지 않고 귀사가 하도급업자가 아닌 경우)으로만 국한되는 경우(DPR의 정의 참조), 프로필의 이 질문에 “아니요” 라고 답할 수 있습니다.

SSPA AI 시스템 승인에는 개인 및/또는 Microsoft 기밀 데이터의 처리와 관련된 문서와 사람, 조직 및 사회에 미치는 영향, 적절한 공급자 인증의 수락 등이 포함됩니다. 공급자는 Microsoft 공급자 데이터 보호 요건의 책임감 있는 AI 브랜치를 완료하고 조달을 진행하기 전에 필수적인 서명 계약 및/또는 Microsoft 내부 검토를 완료합니다. AI 시스템을 제공하는 모든 공급자는 독립 보증 옵션을 제공해야 합니다. ISO 42001은 DPR 섹션 K에 대한 규정준수를 검증하기 위해 제공될 수 있으며 AI 민감 사례에 대한 **필수** 요건입니다. DPR 섹션 K에 대한 독립 평가를 받는 공급자의 경우, 선호하는 평가 기관에 의해 독립 평가를 받아야 합니다(여기에서 제공되는 목록 참조).

SSPA가 승인한 독립 평가에 대해서만 이러한 승인이 부여될 수 있습니다.

SSPA 프로세스 개요

SSPA란 무엇인가요?

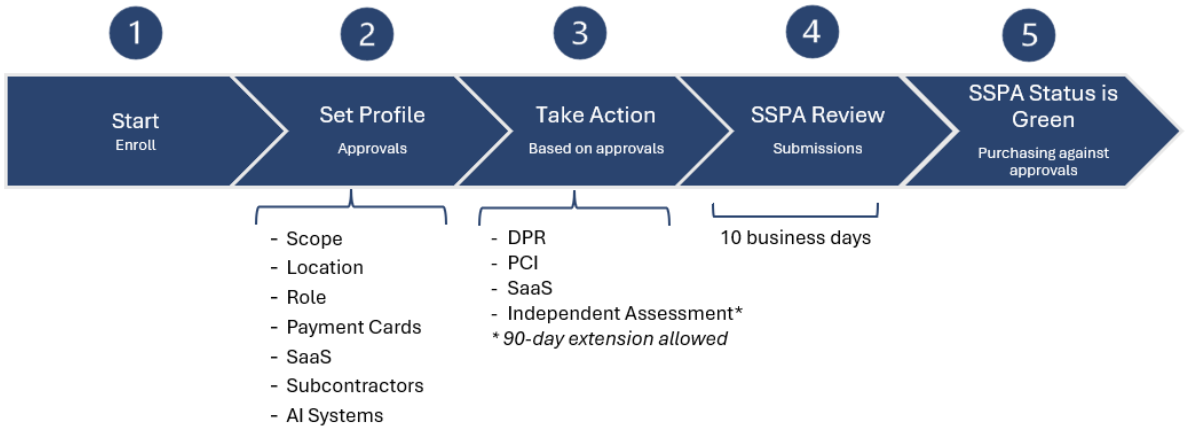
Microsoft는 개인정보보호를 기본적인 권리라고 생각합니다. 당사는 지구상의 모든 개인과 조직이 더 많은 것을 성취할 수 있도록 힘을 실어주겠다는 사명을 가지고 매일 고객의 신뢰를 얻고 유지하기 위해 노력합니다.

견고한 개인정보보호 및 보안 관행은 우리의 사명에 매우 중요하고 고객의 신뢰를 얻는 데 필수적이며 일부 관할구역에서는 법적으로 요구되기도 합니다. Microsoft의 개인정보보호 및 보안 정책에 포함된 기준은 기업으로서 당사의 가치를 반영하며, 이는 Microsoft를 대신하여 Microsoft 데이터를 처리하는 공급자(귀사 등)까지 확장됩니다.

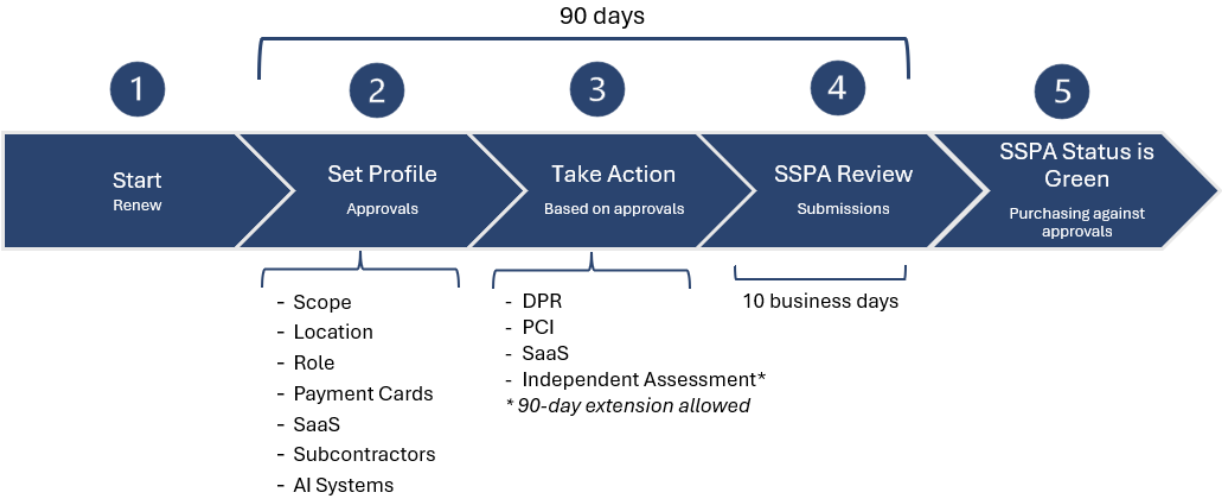
주요 SSPA 용어는 DPR에 정의되어 있습니다. 프로그램에 대해 자세히 알아보려면 자주 묻는 질문(FAQ)을 읽고 당사의 글로벌 팀 이메일 SSPAHelp@microsoft.com으로 문의하십시오.

DPR은 연간 요건입니다. 규정준수 활동은 SSPA 상태가 녹색(준수) 또는 빨간색(미준수)인지를 결정합니다. Microsoft 구매 도구는 업무 진행을 허용하기 전 SSPA 상태가 녹색(SSPA 범위에 속하는 각 공급자에 대해)이고 공급자가 필수 승인을 받았는지 확인합니다.

SSPA 처리 다이어그램 – 신규 공급자 등록



SSPA 처리 다이어그램 – 연간 공급자 갱신



보증 요건

데이터 처리 프로필에서 선택한 승인은 전반적인 Microsoft 업무의 위험 수준을 평가하는 데 도움이 됩니다. SSPA 규정준수 요건은 데이터 처리 프로필 및 관련 승인에 따라 다릅니다.

DPR 준수 자체 증명

SSPA에 등록된 모든 공급자는 요청 접수일 기준으로 90일 이내에 DPR 규정준수에 대한 자체 증명을 완료해야 합니다. 연간 단위로 증명을 요청하지만 데이터 처리 프로필이 연중에 업데이트되면 더 자주 요청할 수 있습니다. 90일 기간이 초과되면 공급자 계정이 빨간색(미준수) SSPA 상태로 바뀝니다. 새로운 범위의 구매 주문은 SSPA 상태가 녹색(준수)으로 바뀔 때까지 처리할 수 없습니다.

신규 등록 공급자는 업무가 시작되기 전에 SSPA 상태가 녹색(준수)이 되도록 부과된 요건을 완료해야 합니다.

중요: SSPA 팀은 이 작업을 확장할 권한이 없습니다.

공급자는 데이터 처리 프로필에 따라 부과된 모든 해당 DPR 요건에 응답해야 합니다. 부과된 요건 중 일부는 공급자가 Microsoft에 제공하는 제품 또는 서비스에 적용되지 않을 수 있습니다. 이는 SSPA 검토자가 검증할 수 있도록 자세한 설명과 함께 '적용되지 않음'으로 표시될 수 있습니다.

SSPA 팀은 부과된 요건에 대해 '적용되지 않음', '현지 법률과 충돌' 또는 '계약 사항 충돌'이 선택되었는지 DPR 제출을 검토합니다. SSPA 팀은 한 가지 이상의 선택 항목에 대한 설명을 요청할 수 있습니다. 현지 법률과 충돌 및 계약 사항 충돌은 이를 뒷받침하는 참조가 제공되고 충돌이 분명히 존재하는 경우에만 인정됩니다.

자체 증명을 완료하도록 승인을 받은 대리인은 각 요건에 확신을 가지고 응할 수 있도록 해당 주제 전문가로부터 충분한 정보를 얻어야 합니다. 또한 SSPA 양식에 자신의 성명을 추가함으로써 DPR을 읽고 이해했음을 증명합니다. 특히 DPR 섹션 J에 대해 승인받기 위해서는 별도의 보안 담당자가 필요하며 귀사와 관련된 보안 사건이 발생할 경우 지원하기 위해 호출될 수 있습니다. 공급자는 요건을 완료하는 데 도움이 되도록 온라인 도구에 다른 연락처를 추가할 수 있습니다.

권한을 위임받은 대리인(정의는 DPR 참조)은 다음을 이행해야 합니다.

1. 적용되는 요건 결정

2. 각 해당 요건에 대한 응답 게시
3. Microsoft 공급자 규정준수 포털에서 서명하고 증명 제출

중요: SSPA에서 자체 증명 지원을 위해 특정 데이터 보호 요건에 대한 통합 규정준수의 증거를 요청할 수 있습니다. 또한, 공급자는 연간 규정준수 주기 이외에 Microsoft 데이터 보호 요건에 명시된 바와 같이, 증거를 제공하도록 선택될 수 있습니다. 이 조항은 독립 평가 작업을 받지 않는 회사에 대해서만 적용됩니다.

독립 평가 요건

이 요건이 유발되는 데이터 처리 승인을 보려면 SSPA 데이터 처리 프로필 표의 승인별 요건을 참조하십시오.

공급자는 데이터 처리 프로필을 업데이트하여 승인을 변경할 수 있는 옵션을 가지고 있습니다. 그러나 공급자의 데이터 처리 역할이 "하위 처리자" 인 경우 이 승인을 변경할 수 없으며 매년 독립 평가를 수행해야 합니다.

규정준수에 대한 독립적인 검증을 요구하는 승인을 얻기 위해 공급자는 DPR에 대한 준수를 검증할 수 있는 독립적인 평가자를 선택해야 합니다. 평가자는 Microsoft에 규정준수 보증을 제공하기 위해 자문서를 작성해야 합니다. 자문서는 총체적이어야 하며, SSPA 팀의 검토를 위해 확인서를 Microsoft 공급자 규정준수 포털에 제출하기 전에 모든 미준수 문제를 해결하고 시정해야 합니다. **평가자는 여기에서 '기본 평가자(Preferred Assessors)' PDF에 첨부된 공인 자문서 템플릿을 다운로드할 수 있습니다.**

SSPA 데이터 처리 프로필 표에는 DPR 규정준수를 확인하기 위해 독립 평가자를 고용하지 않기로 하는 경우 허용되는 인증 대안이 기재되어 있습니다(해당되는 경우, SaaS 공급자, 웹 사이트 호스팅 공급자 또는 하도급업자가 있는 공급자 등). ISO 27701(개인정보보호), ISO 27001(보안) 및 AI 시스템에 대한 ISO 42001(DPR 섹션 K)은 DPR과 밀접한 매핑을 제공하는 토대가 됩니다. 보안 신뢰 기준을 포함한 SOC 2 보고서는 특정 자격이 명시되지 않은 경우 DPR 섹션 J(보안)에 대해 수락될 수 있습니다.

공급자가 HIPPA에 해당되는 독립체 또는 미국 내 의료 서비스 제공자인 경우 당사는 개인정보보호 및 보안 적용 범위에 대해 HITRUST 보고서를 인정합니다.

표준을 벗어나는 상황으로 인해 보증 추가 실사가 이루어지는 경우 SSPA에서 데이터 처리 프로필과 무관하게 독립 평가를 요구할 수 있습니다. 사례에는 부서의 개인정보보호 또는 보안 요청, 데이터 사건 시정 검증, SSPA 팀 비정기 검토 또는 자동화된 데이터 주체 권리 실행에 대한 요건이 포함됩니다.

요건에 접근하는 방법에 대한 지침:

1. 이 업무는 규정준수를 적절하게 평가할 수 있는 충분한 기술 교육을 받고 해당 주제와 관련된 지식을 갖춘 평가자가 수행해야 합니다.
2. 평가자는 국제회계사연맹(International Federation of Accountant, IFAC) 또는 미국공인회계사협회(American Institute of Certified Public Accountants, AICPA) 소속이거나 해당하는 경우 ISO 27001, ISO 27701 및 ISO 42001에 대한 자격을 갖춘 감사자이거나 국제 개인정보보호 전문가 협회(International Association of Privacy Professionals, IAPP) 또는 정보 시스템 감사 및 조정 협회(Information Systems Audit and Control Association, ISACA)가 발행한 자격증을 소지해야 합니다.
3. 평가자는 각 요건을 지원하는 데 필요한 증거가 포함된 최신 DPR을 사용해야 합니다. **공급자는 가장 최근에 승인된 DPR 증명 응답을 평가자에게 제공해야 합니다.**
4. 업무 범위는 요청을 받은 공급자 계정 번호에 대해 실행한 모든 범위 내 데이터 처리 활동에 국한됩니다. 공급자가 한 번에 둘 이상의 공급자 계정을 선택하는 경우 **증명서에는 평가에 포함된 공급자 계정 목록이 기재되어 있어야 합니다.**
5. SSPA에 제출된 증명서에는 공급자가 데이터 보호 요건을 충족할 수 없다는 서면 진술이 있어서는 안 됩니다. 이러한 문제는 증명서를 제출하기 전에 시정해야 합니다.

SSPA는 권장 평가자 목록을 제공합니다. 모두 SSPA 평가를 수행하는 데 정통한 회사들입니다. 해당 평가 비용은 공급자가 부담해야 하며, 데이터 처리의 규모와 범위에 따라 달라집니다.

추가 독립 보증이 필요한 프로필:

서비스형 소프트웨어(SaaS)

데이터 처리 프로필에 기재된 SaaS의 정의에 부합하는 공급자는 Microsoft 클라우드 서비스 계약이 요구하는 경우 유효한 ISO 27001 인증서를 제공해야 할 수 있습니다. 데이터 센터 인증서를

제출하면 안 됩니다. Microsoft와의 계약에 명시된 소프트웨어 서비스에 적용되는 ISO 27001 인증서를 제출해 주십시오.

SSPA 검토자는 제출 사항이 계약 의무에 부합하는지 확인합니다.

AI 시스템

서비스 전달에 민감한 사용이 포함될 경우, ISO 42001 인증이 요구됩니다. 또한, ISO 42001은 독립 평가 작업의 섹션 K를 위해 제출할 수 있습니다.

데이터 사고

공급자가 개인정보보호 또는 보안 데이터 사고에 대해 알게 되는 경우 DPR에 정의되고 자세히 설명된 바에 따라 Microsoft 측에 해당 사실을 알려야 합니다.

데이터 사고는 SupplierWeb 또는 이메일 SuppIR@microsoft.com으로 신고하십시오.

다음 정보가 반드시 포함되어야 합니다.

- 데이터 사고 발생일
- 공급자 이름
- 공급자 번호
- Microsoft 연락 담당
- 관련 PO(해당되거나 사용 가능한 경우)
- 데이터 사고 요약