

Cloud 데이터 처리 부칙(파트너)

본 Cloud 데이터 처리 부칙(부록 포함, 이하 '부칙')은 Google과 '파트너' 간의 '계약'(아래에 정의됨)에 포함됩니다. 본 '부칙'의 이전 명칭은 Google Cloud Platform의 '데이터 처리 및 보안 약관', 'Looker(원본)' 또는 Google 'SecOps 서비스'의 '데이터 처리 부칙' 또는 '데이터 처리 및 보안 약관'입니다.

일반 약관

1. 개요

본 '부칙'은 '파트너 데이터'의 처리 및 보안과 관련된 당사자들의 의무를 설명하며, 여기에는 관련 개인정보 보호, 데이터 보안, 데이터 보호법에 따른 의무가 포함됩니다. 본 '부칙'은 '부칙 시행일'(아래에 정의됨)부터 효력이 발생하며, '파트너 데이터'의 처리 및 보안과 관련하여 이전에 적용되었던 모든 약관을 대체합니다. 본 '부칙'에서 사용되고 있지만 정의되지 않은 작은따옴표로 표기된 용어는 '계약'에서 명시된 의미를 지닙니다.

2. 정의

2.1 본 '부칙'에서 정의된 용어는 다음과 같습니다.

- '부칙 시행일'은 '파트너'가 본 '부칙'을 수락한 날짜, 또는 당사자들이 본 '부칙'에 합의한 날짜를 의미합니다.
- '추가 보안 제어'는 '파트너'가 재량으로 선택 및 결정하여 사용할 수 있는 보안 리소스, 구성요소, 기능, 제어를 의미하며, 여기에는 '관리 콘솔', 암호화, 로깅 및 모니터링, ID 및 액세스 관리, 보안 스캔, 방화벽이 포함됩니다.
- '계약'은 Google이 '파트너'에게 해당 '서비스'를 제공하기로 동의한 계약을 의미합니다.
- '관련 개인정보 보호법'은 '파트너 개인정보' 처리에 적용되는 모든 국가, 연방, 유럽연합, 주, 지역 또는 기타 범위에 해당하는 개인정보 보호, 데이터 보안 또는 데이터 보호 관련 법 또는 규정을 의미합니다.
- '감사 서비스'는 <https://cloud.google.com/security/compliance/services-in-scope>에 관련된 인증 또는 보고서의 범위에 속하는 것으로 표시된 해당 시점의 '서비스'를 의미합니다. Google은 '계약'에 따라 '서비스'가 중단된 경우가 아닌 한 이 URL에 안내된 어떠한 '서비스'도 삭제할 수 없습니다.
- '규정 준수 인증'은 7.4항(규정 준수 인증 및 SOC 보고서)에 명시된 의미를 지닙니다.
- '데이터 사고'는 Google이 관리하거나 다른 방식으로 제어하는 시스템에 저장된 '파트너 데이터'의 우발적 또는 불법적 파기, 손실, 변경, 무단 공개 또는 이러한 데이터에 대한 액세스로 이어지는 Google 보안 침해를 의미합니다.

- 'EMEA'는 유럽, 중동, 아프리카를 의미합니다.
- 'EU GDPR'은 2016년 4월 27일에 제정된 개인정보 처리 관련 자연인 보호 및 해당 정보의 자유로운 이동에 관한 유럽의회 및 유럽이사회 규정(EU) 제2016/679호를 의미하며, 지침 제95/46/EC호를 폐지 및 대체합니다.
- '유럽 데이터 보호법'은 해당되는 경우에 따라 (a) GDPR 또는 (b) 스위스 FADP를 의미합니다.
- '유럽 법률'은 해당되는 경우에 따라 (a) EU 또는 EU 회원국 법률('파트너 개인정보' 처리에 EU GDPR이 적용되는 경우), (b) 영국 또는 영국 일부 지역의 법률('파트너 개인정보' 처리에 영국 GDPR이 적용되는 경우), 또는 (c) 스위스 법률('파트너 개인정보' 처리에 스위스 FADP가 적용되는 경우)을 의미합니다.
- 'GDPR'은 해당되는 경우에 따라 (a) EU GDPR 또는 (b) 영국 GDPR을 의미합니다.
- 'Google의 제3자 감사자'는 Google이 임명하여 자격을 부여받은 독립적인 제3자 감사자이며, Google은 해당 감사자의 당시 신분을 '파트너'에게 공개합니다.
- '지침'은 5.2항(파트너의 지침 준수)에 명시된 의미를 지닙니다.
- '알림 이메일 주소'는 '관리 콘솔' 또는 '주문 양식'에서 '파트너'가 Google의 특정 알림을 받기 위해 고용한 이메일 주소를 의미합니다.
- '파트너 최종 이용자'는 '계약'에 명시된 의미를 지니며, 의미가 명시되지 않은 경우 '계약'에서 '최종 이용자'에 대해 명시한 의미를 지닙니다.
- '파트너 개인정보'는 '파트너 데이터'에 포함된 개인정보를 의미하며, 여기에는 '관련 개인정보 보호법'에 정의된 특수한 범주의 개인정보 또는 민감한 정보가 포함됩니다.
- '보안 문서'는 '규정 준수 인증' 및 'SOC 보고서'를 의미합니다.
- '보안 조치'는 7.1.1항(Google의 보안 조치)에 명시된 의미를 지닙니다.
- '서비스'는 부록 4(특정 제품)에 설명된 관련 서비스를 의미합니다.
- 'SOC 보고서'는 7.4항(규정 준수 인증 및 SOC 보고서)에 명시된 의미를 지닙니다.
- '보조 프로세서'는 본 '부칙'에 따라 또 다른 프로세서로서 '파트너 데이터'를 처리하여 일부 '서비스' 및 TSS를 제공하도록 승인된 제3자를 의미합니다.
- '감독 당국'은 해당되는 경우에 따라 (a) EU GDPR에 정의된 '감독 당국' 또는 (b) 영국 GDPR이나 스위스 FADP에 정의된 '사무국'을 의미합니다.
- '스위스 FADP'는 해당되는 경우에 따라 1992년 6월 19일 스위스 연방 데이터 보호법(1993년 6월 14일 연방 데이터 보호법 조례 포함) 또는 개정된 2020년 9월 25일 스위스 연방 데이터 보호법(2022년 8월 31일 연방 데이터 보호법 조례 포함)을 의미합니다.

- '계약 기간'은 '부칙 시행일'부터 Google의 '서비스' 제공이 종료되는 날까지의 기간을 의미하며, 해당되는 경우 '서비스' 제공이 보류될 수 있는 기간과 Google이 전환을 목적으로 '서비스'를 계속해서 제공할 수 있는 종료 후 기간도 여기에 포함됩니다.
- '영국 GDPR'은 영국의 2018년 유럽연합(탈퇴)법과 해당 법에 따른 관련 2차 법률에 의거하여 개정되고 영국 법에 통합된 'EU GDPR'을 의미합니다.

2.2 본 '부칙'에서 사용되는 용어인 '개인정보', '정보주체', '처리', '컨트롤러', '프로세서'는 '관련 개인정보 보호법'에 명시된 의미를 지니며, 명시된 의미가 없거나 관련법이 없는 경우 'EU GDPR'에 명시된 의미를 지닙니다.

2.3 '정보주체', '컨트롤러', '프로세서' 용어에는 '관련 개인정보 보호법'에 따라 각각 '소비자', '사업자', '서비스 제공업체'의 의미가 포함됩니다.

3. 기간

'계약'의 종료 또는 만료 여부와 관계없이, 본 '부칙'은 Google이 본 '부칙'에 설명된 대로 모든 '파트너 데이터'를 삭제할 때까지 유효하며, 해당 데이터가 삭제됨과 동시에 자동으로 만료됩니다.

4. 역할 및 법적 규정 준수

4.1 당사자들의 역할. Google은 '파트너 개인정보'의 프로세서이고, '파트너'는 해당되는 경우에 따라 컨트롤러 또는 프로세서입니다.

4.2 처리 요약. '파트너 개인정보' 처리의 주제 및 세부정보는 부록 1(데이터 처리의 주제 및 세부정보)에 설명되어 있습니다.

4.3 법적 규정 준수. 각 당사자는 '관련 개인정보 보호법'에 따라 '파트너 개인정보' 처리와 관련된 의무를 준수합니다.

4.4 추가 법률 조항. '파트너 개인정보' 처리에 부록 3(특정 개인정보 보호법)에 설명된 '관련 개인정보 보호법'이 적용되는 경우, 부록 3의 해당 조항이 이 '일반 약관'에 추가로 적용되며 14.1항(우선 적용)에 설명된 대로 우선 적용됩니다.

5. 데이터 처리

5.1 프로세서 파트너. '파트너'가 프로세서인 경우 다음을 따릅니다.

a. '파트너'는 관련 '고객' 및 컨트롤러가 다음을 승인했음을 지속적으로 보증합니다.

i. '지침'

ii. '파트너'가 Google을 또 하나의 프로세서로 고용한다는 사실

iii. 11항(보조 프로세서)에 설명된 대로 Google이 보조 프로세서를 고용한다는 사실

b. '파트너'는 Google에서 7.2.1항(사고 알림), 9.2.1항(요청에 대한 책임) 또는 11.4항(보조 프로세서에 대한 이의 제기 권한)에 따라 제공한 모든 통지를 관련 '고객' 및 컨트롤러에게 지체 없이 신속하게 전달합니다.

c. '파트너'는 Google에서 본 '부칙'에 따라 제공한 Google 데이터 센터의 위치 또는 보조 프로세서의 이름, 위치, 활동에 관한 기타 정보를 관련 '고객' 및 컨트롤러에게 제공할 수 있습니다.

5.2 파트너의 지침 준수. Google은 '파트너'의 지침을 바탕으로 '계약'(본 '부칙' 포함)에 따라 '파트너 데이터'를 다음과 같은 목적으로만 처리합니다.

a. '서비스' 및 TSS 제공, 보호, 모니터링 목적

b. 다음을 통해 추가로 명시된 사항을 따릅니다.

i. '파트너'의 '서비스'('관리 콘솔'을 통한 이용 포함) 및 TSS를 이용하는 방식

ii. '파트너'가 제공한 기타 서면 지침 중 Google이 본 '부칙'에 부합하는 것으로 인정하는 지침

('지침'으로 통칭)

Google은 '유럽 데이터 보호법' 적용하에서 '유럽 법률'에 의해 금지되지 않는 경우, 또는 기타 '관련 개인정보 보호법' 적용하에서 관련 법률에 의해 금지되지 않는 경우 이 '지침'을 준수합니다.

6. 데이터 삭제

6.1 파트너에 의한 삭제. Google은 '서비스'의 기능에 부합하는 방식으로 '계약 기간' 동안 '파트너'가 '파트너 데이터'를 삭제하도록 허용합니다. '파트너'가 '계약 기간' 동안 '서비스'를 이용해 '파트너 데이터'를 삭제하고 '파트너'가 해당 '파트너 데이터'를 복구할 수 없는 경우, 이러한 이용은 Google이 Google 시스템에서 관련 '파트너 데이터'를 삭제해야 한다는 '지침'으로 간주됩니다. Google은 '유럽 데이터 보호법' 적용하에서 '유럽 법률'에 따라 데이터를 보관해야 하는 경우 또는 기타 '관련 개인정보 보호법' 적용하에서 관련 법률에 따라 데이터를 보관해야 하는 경우가 아닌 한 합리적으로 실행 가능한 범위에서 최대 180일 안에 신속하게 이 '지침'을 준수합니다.

6.2 계약 기간 종료 시 반환 또는 삭제. '파트너'가 '계약 기간' 종료 후에도 '파트너 데이터'를 보관하기를 원할 경우, 9.1항(액세스, 정정, 제한적 처리, 이동성)에 따라 '파트너'는 Google에 '계약 기간' 안에 해당 데이터를 반환하도록 지시할 수 있습니다. '파트너'는 '계약 기간' 종료 시 Google에 Google 시스템에 남아 있는 모든 '파트너 데이터'(기존 사본 포함)를 삭제하도록 지시합니다. '계약 기간' 종료일로부터 최대 30일간의 복구 기간이 지나면 Google은 '유럽 데이터 보호법' 적용하에서 '유럽 법률'에 따라 데이터를 보관해야 하는 경우 또는 기타 '관련 개인정보 보호법' 적용하에서 관련 법률에 따라 데이터를 보관해야 하는 경우가 아닌 한 합리적으로 실행 가능한 범위에서 최대 180일 안에 신속하게 이 '지침'을 준수합니다.

7. 데이터 보안

7.1 Google의 보안 조치, 제어 및 지원.

7.1.1 Google의 보안 조치. Google은 부록 2(보안 조치)('보안 조치')에 명시된 바와 같이 우발적 또는 불법적 파괴, 손실, 변경 또는 무단 공개나 액세스로부터 '파트너 데이터'를 보호하는 기술적, 조직적, 물리적 조치를 이행하고 유지합니다. '보안 조치'로는 '파트너 데이터'를 암호화하거나, Google 시스템 및 서비스의 기밀성, 무결성, 가용성, 복원력을 지속적으로 유지하며, 사고 이후 '파트너 데이터'에 대한 액세스를 적시에 복구하고, 정기적으로 효율성을 테스트하는 조치 등이 있습니다. Google은 '서비스'의 보안이 심각하게 저하되지 않는 범위에서 이러한 '보안 조치'를 경우에 따라 업데이트할 수 있습니다.

7.1.2 액세스 및 규정 준수. Google에서는 다음을 수행합니다.

a. '지침'을 준수하는 데 반드시 필요한 경우에만 Google의 직원, 계약업체, '보조 프로세서'에게 '파트너 데이터'에 액세스할 수 있는 권한을 부여합니다.

b. 성과 범위에 적용되는 범위에서 직원, 계약업체, '보조 프로세서'의 '보안 조치' 준수를 위해 적절한 조치를 취합니다.

c. '파트너 데이터'를 처리할 권한이 있는 모든 사람이 비밀유지 의무를 이행하도록 합니다.

7.1.3 추가 보안 제어. Google은 다음과 같은 경우에 '추가 보안 제어'를 시행합니다.

a. '파트너'가 '파트너 데이터' 보호를 위한 조치를 취할 수 있도록 허용해야 하는 경우

b. '파트너'에게 '파트너 데이터' 보호, 액세스, 사용에 관한 정보를 제공해야 하는 경우

7.1.4 Google의 보안 지원. Google은 ('파트너 개인정보' 처리의 성격과 Google에 제공되는 정보를 고려하여) 다음과 같은 조치를 통해 '파트너'(또는 '파트너'가 프로세서인 경우 관련 컨트롤러)가 '관련 개인정보 보호법'에 따라 보안 및 개인정보 유출과 관련된 의무를 준수하도록 지원합니다.

a. 7.1.1항(Google의 보안 조치)에 따라 '보안 조치'를 이행하고 유지합니다.

b. 7.1.3항(추가 보안 제어)에 따라 '추가 보안 제어'를 제공합니다.

c. 7.2항(데이터 사고)의 조항을 준수합니다.

d. 7.5.1항(보안 문서 검토)에 따라 '보안 문서'를 제공하고 '계약'(본 '부칙' 포함)에 포함된 정보를 제공합니다.

e. '파트너'(또는 관련 컨트롤러)가 해당 의무를 준수하는 데 위의 하위 섹션 (a)~(d)로 충분하지 않은 경우, '파트너'의 요청에 따라 '파트너'에게 합당한 수준의 협조와 지원을 추가로 제공합니다.

7.2 데이터 사고.

7.2.1 사고 알림. Google은 '데이터 사고'를 인지한 후 지체 없이 신속하게 '파트너'에게 알리며, 피해를 최소화하고 '파트너 데이터'를 보호하기 위한 합당한 조치를 즉시 취합니다.

7.2.2 데이터 사고 세부정보. Google은 '데이터 사고' 알림을 통해 '데이터 사고'의 성격(영향을 받은 '파트너' 리소스 포함), Google이 '데이터 사고'를 해결하고 그로 인한 잠재적 위험을 완화하기 위해 취한 조치 또는 그 계획, '데이터 사고'를 해결할 수 있도록 Google이 '파트너'에게 권장하는 조치(있는 경우), 더 자세한 정보를 얻을 수 있는 담당자 연락처를 제공합니다. 이러한 모든 정보를 한 번에 제공할 수 없는 상황인 경우, Google의 초기 알림에는 해당 시점에 제공할 수 있는 정보가 포함되며 추가 정보는 준비가 되는 대로 지체 없이 제공됩니다.

7.2.3 Google의 파트너 데이터 평가 금지. Google은 '파트너 데이터'에 특정한 현지 법규가 적용되는 정보가 있는지 평가할 의무가 없습니다.

7.2.4 Google의 과실 인정 금지. Google이 본 7.2항(데이터 사고)에 따라 '데이터 사고'를 알리거나 이에 대응한다고 해서 Google이 '데이터 사고'에 대한 과실이나 책임을 인정하는 것은 아닙니다.

7.3 파트너의 보안 책임 및 평가.

7.3.1 파트너의 보안 책임. 7.1항(Google의 보안 조치, 제어 및 지원) 및 7.2항(데이터 사고)과 '계약'에 따라 Google과 '파트너' 간에 있어 Google의 의무를 침해하지 않는 범위 내에서, '파트너'는 '파트너' 및 그 '고객'의 '서비스' 사용과 Google 시스템 또는 Google의 '보조 프로세서' 시스템 외부에 있는 '파트너' 및 그 '고객'의 '파트너 데이터' 사본의 보관에 대한 책임이 있습니다. 여기에는 다음이 포함됩니다.

- a. '서비스' 및 '추가 보안 제어'를 사용하여 '파트너 데이터'에 발생할 수 있는 위험에 적합한 수준의 보안을 보장해야 합니다.
- b. '파트너' 및 '파트너'의 '고객'이 '서비스'에 액세스하기 위해 사용하는 계정 사용자 인증 정보, 시스템, 기기를 보호해야 합니다.
- c. 적절하게 '파트너 데이터'를 백업해야 합니다.

7.3.2 파트너의 보안 평가. '파트너'는 '서비스', '보안 조치', '추가 보안 제어', 7항(데이터 보안)에 따른 Google의 책무가 '파트너 데이터'에 발생할 수 있는 위험에 적합한 수준의 보안을 제공한다는 데 동의합니다(최첨단 기술, 시행 비용 및 '파트너 데이터' 처리의 성격, 범위, 맥락, 목적과 개인에 대한 위험 고려).

7.4 규정 준수 인증 및 SOC 보고서. Google은 '보안 조치'의 지속적인 효과를 검증하기 위해 '감사 서비스'에 대해 최소한으로 다음 사항을 유지합니다.

- a. 부록 4(특정 제품)('규정 준수 인증')에 설명된 ISO 27001 인증서 및 기타 추가 인증
- b. Google의 '제3자 감사자'가 작성하고 12개월마다 최소 1회 이상 시행되는 감사를 바탕으로 매년 업데이트되는 SOC 2 및 SOC 3 보고서('SOC 보고서').

Google은 언제든지 표준을 추가할 수 있습니다. Google은 '규정 준수 인증' 또는 'SOC 보고서'를 이에 상응하거나 강화된 인증 또는 보고서로 대체할 수 있습니다.

7.5 규정 준수 검토 및 감사.

7.5.1 보안 문서 검토. Google이 본 '부칙'에 따른 의무를 준수하고 있음을 입증하기 위해 Google은 '파트너'가 검토할 수 있도록 '보안 문서'를 제공하며, '파트너'가 프로세서인 경우 7.5.3항(검토 및 감사를 위한 추가 비즈니스 약관)에 따라 관련 '고객' 및 컨트롤러가 'SOC 보고서'에 액세스할 수 있는 권한을 '파트너'가 요청하도록 허용합니다.

7.5.2 파트너의 감사 권리.

a. 파트너 감사. Google은 '관련 개인정보 보호법'상 필요한 경우 7.5.3항(검토 및 감사를 위한 추가 비즈니스 약관)에 따라 '파트너' 또는 '파트너'가 임명한 독립적인 감사자가 감사(점검 포함)를 시행하여 Google이 본 '부칙'에 따른 의무를 준수하고 있는지 확인하도록 허용합니다. 감사 기간 동안 Google은 7.5항(규정 준수 검토 및 감사)에 명시된 대로 '파트너' 또는 '파트너'의 감사자와 합당한 수준에서 협력합니다.

b. 파트너의 독자적인 검토. '파트너'는 감사를 통해 '보안 문서'(Google의 '제3자 감사자'가 시행한 감사 결과가 반영됨)를 검토하여 Google이 본 '부칙'에 따른 의무를 준수하고 있는지 확인할 수 있습니다.

7.5.3 검토 및 감사를 위한 추가 비즈니스 약관.

- a. '파트너'는 Google의 'Cloud 데이터 보호팀'에 다음을 요청해야 합니다.

i. 7.5.1항(보안 문서 검토)에 따른 관련 컨트롤러에 대한 'SOC 보고서' 액세스

ii. 7.5.2(a)항(파트너 감사)에 따른 감사

b. 7.5.3(a)항의 '파트너' 요청에 따라, Google 및 '파트너'는 다음 사항에 대해 논의하고 합의해야 합니다.

i. 7.5.1항(보안 문서 검토)에 따른 관련 컨트롤러의 'SOC 보고서' 액세스에 적용되는 보안 및 비밀유지 제어

ii. 7.5.2(a)항(파트너 감사)에 따른 감사의 합당한 시작일, 범위, 기간과 감사에 적용되는 보안 및 비밀유지 제어

c. Google은 7.5.2(a)항(파트너 감사)에 따른 모든 감사에 대해 비용(Google의 합당한 비용 기준)을 청구할 수 있습니다. Google은 이러한 감사 이전에 관련 비용과 계산 근거에 대한 세부정보를 '파트너'에게 제공합니다. '파트너'는 '파트너'가 임명한 감사자가 감사 시행을 위해 청구하는 모든 비용을 부담해야 합니다.

d. 감사자가 Google의 합리적 판단에 따라 자격 또는 독립성이 적합하지 않거나, Google의 경쟁업체거나, 그밖에 명백히 부적합한 경우 Google은 7.5.2(a)항(파트너 감사)에 따라 감사를 시행할 목적으로 '파트너'가 임명한 감사자에 대해 서면으로 거부 의사를 표시할 수 있습니다. Google이 이러한 거부 의사를 표시하는 경우 '파트너'는 다른 감사자를 임명하거나 직접 감사를 시행해야 합니다.

e. 부록 3(특정 개인정보 보호법) 또는 부록 4(특정 제품)에 따라 관련 컨트롤러나 감사에 대한 SOC 보고서 액세스를 요청하는 모든 '파트너'에게는 본 7.5.3항(검토 및 감사를 위한 추가 비즈니스 약관)이 함께 적용됩니다.

8. 영향 평가 및 협의

Google은 (처리의 성격과 Google에 제공되는 정보를 고려하여) 다음과 같은 조치를 통해 '파트너'(또는 '파트너'가 프로세서인 경우 관련 컨트롤러)가 '관련 개인정보 보호법'에 따라 데이터 보호 평가, 위험 평가, 사전 규제 협의 또는 이에 상응하는 절차와 관련된 의무를 준수하도록 지원합니다.

a. 7.1.3항(추가 보안 제어)에 따라 '추가 보안 제어'를 제공하고 7.5.1항(보안 문서 검토)에 따라 '보안 문서'를 제공합니다.

b. '계약'(본 '부칙' 포함)에 포함된 정보를 제공합니다.

c. '파트너'(또는 관련 컨트롤러)가 해당 의무를 준수하는 데 위의 하위 섹션 (a)와 (b)로 충분하지 않은 경우, '파트너'의 요청에 따라 '파트너'에게 합당한 수준의 협조와 지원을 추가로 제공합니다.

9. 액세스 등, 정보주체 권리, 데이터 내보내기

9.1 액세스, 정정, 제한적 처리, 이동성. '계약 기간' 중 Google은 6.1항(파트너에 의한 삭제)에 명시된 Google에서 제공한 삭제 기능을 사용하는 등 '서비스'의 기능과 일치하는 방식으로 '파트너'의 '파트너 데이터'에 대한 액세스, 정정, 제한적 처리 및 내보내기를 허용합니다. '파트너'가 부정확하거나 오래된 '파트너 개인정보'를 인지한 경우, '파트너'는 '관련 개인정보 보호법'에 따라 필요 시 이러한 기능을 사용해 해당 데이터를 정정하거나 삭제할 책임이 있습니다.

9.2 정보주체 요청.

9.2.1 요청에 대한 책임. '계약 기간' 동안 Google의 'Cloud 데이터 보호팀'이 정보주체로부터 받은 요청이 '파트너 개인정보'와 관련이 있고 '파트너'를 식별할 수 있는 경우, Google은 다음과 같이 조치합니다.

- a. 정보주체에게 해당 요청을 '파트너'에게 제출하도록 안내합니다.
- b. '파트너'에게 즉시 알립니다.
- c. '파트너'의 승인 없이 해당 정보주체의 요청에 응답하지 않습니다.

'파트너'는 필요한 경우 '서비스'의 기능을 사용해 이러한 요청에 응답해야 합니다.

9.2.2 Google의 정보주체 요청 지원. Google은 ('파트너 개인정보' 처리의 성격을 고려하여) 다음과 같은 조치를 통해 '파트너'(또는 '파트너'가 프로세서인 경우 관련 컨트롤러)가 '관련 개인정보 보호법'에 따라 정보주체의 권리 행사 요청에 응답할 의무를 이행할 수 있도록 지원합니다.

- a. 7.1.3항(추가 보안 제어)에 따라 '추가 보안 제어'를 제공합니다.
- b. 9.1항(액세스, 정정, 제한적 처리, 이동성) 및 9.2.1항(요청에 대한 책임)을 준수합니다.
- c. '파트너'(또는 관련 컨트롤러)가 해당 의무를 준수하는 데 위의 하위 섹션 (a)와 (b)로 충분하지 않은 경우, '파트너'의 요청에 따라 '파트너'에게 합당한 수준의 협조와 지원을 추가로 제공합니다.

10. 데이터 처리 위치

10.1 데이터 저장 및 처리 시설. '서비스별 약관'에 따른 Google의 데이터 위치 약정과 부록 3(특정 개인정보 보호법)에 따른 데이터 전송 약정에 따라, 해당하는 경우 '파트너 데이터'는 Google 또는 Google의 '보조 프로세서'가 시설을 관리하는 국가에서 처리될 수 있습니다.

10.2 데이터 센터 정보. Google 데이터 센터의 위치는 부록 4(특정 제품)에 설명되어 있습니다.

11. 보조 프로세서

11.1 보조 프로세서 고용에 대한 동의. '파트너'는 '부칙 시행일'을 기준으로 11.2항(보조 프로세서에 관한 정보)에 설명된 바와 같이 공개된 법인을 Google이 '보조 프로세서'로 고용할 수 있는 권한을 특별히 부여합니다. 또한 11.4항(보조 프로세서에 대한 이의 제기 권한)을 침해하지 않는 범위 내에서 '파트너'는 Google이 다른 제3자를 '보조 프로세서'('신규 보조 프로세서')로 고용할 수 있는 권한을 일반적으로 부여합니다.

11.2 보조 프로세서에 관한 정보. '보조 프로세서'의 이름, 위치, 활동은 부록 4(특정 제품)에 설명되어 있습니다.

11.3 보조 프로세서 고용 요건. Google은 '보조 프로세서'를 고용할 때 다음 작업을 수행합니다.

- a. 서면 계약을 통해 다음 사항을 보장합니다.
 - i. '보조 프로세서'는 하도급된 의무를 수행하는 데 필요한 범위 내에서만 '파트너 데이터'에 액세스하고 이를 사용하며, '계약'(본 '부칙' 포함)에 따라 이를 수행합니다.
 - ii. '관련 개인정보 보호법'에 따라 필요한 경우 본 '부칙'에 명시된 데이터 보호 의무가 '보조 프로세서'에게 부과됩니다(부록 3(특정 개인정보 보호법)에 자세한 설명이 있을 수 있음).

b. '보조 프로세서'에 하도급된 모든 의무에 대해서, 그리고 '보조 프로세서'의 모든 작위와 부작위에 대해서 전적으로 책임을 집니다.

11.4 보조 프로세서에 대한 이의 제기 권한.

a. '계약 기간' 동안 Google이 '신규 보조 프로세서'를 고용하는 경우, Google은 해당 '신규 보조 프로세서'가 '파트너 데이터' 처리를 시작하기 최소 30일 전에 '파트너'에게 이러한 고용 사실('신규 보조 프로세서'의 이름, 위치, 활동 포함)을 알립니다.

b. '파트너'는 '신규 보조 프로세서' 고용에 대한 통지를 받은 후 90일 이내에 다음에 따라 '계약'을 즉시 편의상 해지하여 이의를 제기할 수 있습니다.

i. 해당 '계약'의 편의에 의한 해지 조항에 따라 계약을 해지합니다.

ii. 관련 조항이 없는 경우 Google에 통지하여 계약을 해지합니다.

12. Cloud 데이터 보호팀, 처리 기록

12.1 Cloud 데이터 보호팀. Google의 'Cloud 데이터 보호팀'은 '계약'에 따라 '파트너 데이터' 처리와 관련된 '파트너' 문의에 신속하고 합당한 지원을 제공하며, '계약'의 '통지' 조항 또는 부록 4(특정 제품)에 명시된 대로 'Cloud 데이터 보호팀'에 연락을 취할 수 있습니다.

12.2 Google의 처리 기록. Google은 '관련 개인정보 보호법'에 따라 Google의 처리 활동과 관련된 문서를 보관합니다. '관련 개인정보 보호법'에 따라 Google이 '파트너' 또는 '파트너'의 '고객'과 관련된 특정 정보의 기록을 수집 및 유지해야 하는 경우, '파트너'는 '관리 콘솔' 또는 부록 4(특정 제품)에 명시된 기타 방법을 사용해 해당 정보를 제공하고 해당 정보의 정확성과 최신성을 유지해야 합니다. Google은 '관련 개인정보 보호법'에 따라 필요한 경우 '감독 당국'을 비롯하여 관할 규제 기관에 해당 정보를 제공해야 할 수 있습니다.

12.3 컨트롤러 요청. '계약 기간' 동안 Google의 'Cloud 데이터 보호팀'이 '파트너 개인정보'의 컨트롤러라고 주장하는 제3자로부터 어떤 요청이나 지침을 받게 되는 경우, Google은 해당 제3자를 '파트너'에게 연락하도록 안내합니다.

13. 통지

본 '부칙'에 따른 통지(모든 '데이터 사고' 관련 알림 포함)는 '알림 이메일 주소'로 전달됩니다. '파트너'는 '관리 콘솔'을 사용하거나 기타 방법으로 Google에 '알림 이메일 주소'가 최신 상태이고 유효하다는 사실을 알릴 책임이 있습니다.

14. 해석

14.1 우선 적용. 상충하는 경우 다음에 따라 적용됩니다.

a. 부록 3(특정 개인정보 보호법)과 '부칙'의 나머지 부분(부록 4(특정 제품) 포함) 간에 상충하는 내용이 있는 경우 부록 3이 우선합니다.

b. 부록 4(특정 제품)와 '부칙'의 나머지 부분(부록 3 제외) 간에 상충하는 내용이 있는 경우 부록 4가 우선합니다.

c. 본 '부칙'과 '계약'의 나머지 부분 간에 상충하는 내용이 있는 경우 본 '부칙'이 우선합니다.

14.2 조항 언급. 달리 명시되지 않는 한, 본 '부칙'의 모든 부록에 있는 조항 언급은 본 '부칙'의 '일반 약관' 조항을 의미합니다.

14.3 고객. 의심의 소지를 없애기 위해, '고객'은 본 '부칙'의 제3의 수혜자가 아님을 밝힙니다.

부록 1: 주제 및 데이터 처리 세부정보

주제

'파트너'에 대한 Google의 '서비스' 및 TSS 제공

처리 기간

'계약 기간'과 '계약 기간'의 종료 시점부터 본 '부칙'에 따라 Google이 '파트너 데이터'를 모두 삭제할 때까지의 기간입니다.

처리 성격 및 목적

Google은 본 '부칙'에 따라 '서비스'와 TSS를 '파트너'에게 제공할 목적으로 '파트너 개인정보'를 처리합니다.

데이터 범주

'파트너' 또는 '파트너'의 '고객', 또는 '파트너 최종 사용자'가(또는 '파트너'의 지시로) '서비스'를 통해 Google에 제공하는 개인 관련 데이터가 포함됩니다.

정보주체

'파트너' 또는 '파트너'의 '고객', 또는 '파트너 최종 사용자'가(또는 '파트너'의 지시로) '서비스'를 통해 Google에 제공하는 데이터의 주체인 개인이 정보주체에 포함됩니다.

부록 2: 보안 조치

Google은 '부칙 시행일'을 기준으로 부록 2에 명시된 '보안 조치'를 이행하고 유지합니다.

1. 데이터 센터와 네트워크 보안

(a) 데이터 센터.

인프라. Google은 데이터 센터를 지리적으로 분산하여 유지합니다. Google은 모든 프로덕션 데이터를 물리적으로 안전한 데이터 센터에 저장합니다.

중복화. 인프라 시스템은 단일 장애점을 제거하고, 예상되는 환경 위험의 영향을 최소화하도록 설계되었습니다. 이중 회로, 스위치, 네트워크 또는 기타 필요한 기기는 이러한 중복화를 제공하는 데 효과적입니다. '서비스'는 Google이 특정 유형의 예방적/교정적 유지보수를 중단 없이 수행할 수 있도록 설계되었습니다. 모든 환경 장비와 시설은 문서화된 예방적 유지보수 절차가 있으며, 이 문서에는 제조업체

또는 내부 사양에 따른 유지보수 시행 프로세스와 주기가 자세하게 설명되어 있습니다. 데이터 센터 장비의 예방적/교정적 유지보수는 문서화된 절차에 따라 표준 변경 프로세스를 통해 예약됩니다.

전력. 데이터 센터 전력 시스템은 중복화되어 1일 24시간 및 주 7일 지속적인 운영에 영향을 미치지 않고 유지할 수 있도록 설계되었습니다. 대부분의 경우 기본 전력원과 대체 전력원은 데이터 센터에서 중요한 인프라 구성요소에 각각 동일한 용량으로 제공됩니다. 백업 전력은 무정전 전원공급(UPS) 배터리를 비롯한 다양한 메커니즘으로 제공됩니다. 특히 UPS 배터리는 전력회사 브라운아웃, 블랙아웃, 과도 전압, 부족 전압, 허용오차를 벗어나는 주파수 조건 시에도 안정적인 전력 보호를 일관적으로 공급합니다. 백업 전력은 전력회사 전원이 중단될 경우를 대비해 백업 발전기 시스템이 가동될 때까지 최대 10분 동안 일시적으로 데이터 센터에 최대 용량의 전력을 공급하도록 설계되었습니다. 백업 발전기는 몇 초 안에 자동으로 가동되며, 일반적으로 며칠 동안 데이터 센터를 최대 용량으로 가동하는 데 충분한 비상 전력을 공급할 수 있습니다.

서버 운영체제. Google 서버는 적용 환경에 맞게 맞춤설정된 Linux 기반 운영체제를 사용합니다. 데이터는 데이터 보안 및 중복화를 강화할 수 있도록 독점 알고리즘을 사용해 저장됩니다.

코드 품질. Google은 코드 검토 프로세스를 도입하여 '서비스'를 제공하는 데 사용되는 코드의 보안을 강화하고 프로덕션 환경에서 보안 제품을 개선합니다.

비즈니스 연속성. Google은 비즈니스 연속성 계획/재해 복구 프로그램을 설계했으며 이를 정기적으로 계획하고 테스트합니다.

(b) 네트워크 및 전송.

데이터 전송. 데이터 센터는 일반적으로 고속 비공개 링크를 통해 연결되어 데이터 센터 간에 안전하고 빠른 데이터 전송을 제공합니다. 또한 전자적 전송 또는 이동 과정에서 혹은 데이터 저장 미디어에 기록되는 과정에서 승인 없이 데이터를 읽거나, 복사하거나, 변경하거나, 삭제하지 못하도록 설계되었습니다.

Google은 인터넷 표준 프로토콜을 통해 데이터를 전송합니다.

외부 공격 표면. Google은 여러 계층으로 이루어진 네트워크 기기 및 침입 감지를 도입하여 외부 공격 표면을 차단합니다. Google은 잠재적 공격 벡터를 고려하여 목적에 따라 설계된 적절한 기술을 외부 대응 시스템에 적용합니다.

침입 감지. 침입 감지는 지속적인 공격 활동에 대한 인사이트와 사고 대응에 적합한 정보를 제공하는 데 목적이 있습니다. Google 침입 감지에는 (i) 예방 조치를 통해 Google에서 공격에 노출되는 표면의 규모와 구성요소를 엄격하게 제어하고, (ii) 데이터 진입점에서 지능적인 감지 제어를 도입하고, (iii) 특정 위험 상황을 자동으로 해결하는 기술을 도입하는 것이 포함됩니다.

사고 대응. Google은 다양한 통신 채널을 모니터링하여 보안 사고를 탐지하고, Google의 보안 요원이 알려진 사고에 신속히 대응합니다.

암호화 기술. Google은 HTTPS 암호화(SSL 또는 TLS 연결이라고도 함)를 지원합니다. Google 서버는 RSA와 ECDSA로 서명된 일회성 타원 곡선 디피-헬만(Diffie-Hellman) 암호화 키 교환을 지원합니다. 이러한 PFS(Perfect Forward Secrecy) 기법은 트래픽을 보호할 뿐만 아니라 키 유출 또는 암호 해독으로 인한 침투의 영향을 최소화하는 데도 효과적입니다.

2. 접근 및 현장 통제

(a) 현장 통제.

데이터 센터 현장 보안 운영팀. Google의 데이터 센터는 현장 보안 운영팀을 유지하면서 1일 24시간, 주 7일 동안 데이터 센터의 물리적 보안 운영을 맡고 있습니다. 현장 보안 운영 담당자는 폐쇄 회로 TV(CCTV) 카메라를 비롯한 모든 경보 시스템을 모니터링합니다. 또한 데이터 센터 내부와 외부를 정기적으로 순찰합니다.

데이터 센터 접근 절차. Google은 데이터 센터에 대한 물리적 접근을 허용하는 공식 접근 절차를 유지합니다. 데이터 센터는 현장 보안 운영팀에 연결된 경보 시스템을 갖춘 전자식 카드 키를 사용해야 접근이 가능한 시설 내에 있습니다. 데이터 센터에 입장하는 개인은 모두 자신의 신분을 밝혀야 할 뿐만 아니라 현장 보안 운영팀에게 신분증을 제시해야 합니다. 직원과 계약업체, 방문자는 승인을 거쳐야만 데이터 센터에 입장할 수 있습니다. 이러한 시설에 대한 전자식 카드 키 접근 역시 승인된 직원과 계약업체에게만 허용됩니다. 데이터 센터에 대한 전자식 카드 키 접근은 이메일을 통해서 요청해야 하며, 요청자의 관리자와 데이터 센터 책임자의 승인이 필요합니다. 그 밖에 일시적인 데이터 센터 접근이 필요한 개인은 (i) 방문하려는 특정 데이터 센터 및 내부 구역을 관리하는 데이터 센터 관리자에게 사전 승인을 받아야 하고, (ii) 입장할 때 현장 보안 운영팀에게 서명해야 하고, (iii) 본인의 승인 여부를 알 수 있도록 승인된 데이터 센터 접근 기록을 참조해야 합니다.

데이터 센터 현장 보안 기기. Google의 데이터 센터에는 시스템 경보와 연동된 이중 인증 접근 통제 시스템이 적용되어 있습니다. 접근 통제 시스템은 개인이 경계 출입구, 하역장, 기타 주요 구역에 접근할 때 전자식 카드 키를 모니터링하고 기록합니다. 승인받지 않은 활동과 잘못된 접근 시도는 접근 통제 시스템에 기록되고, 필요한 경우 조사가 진행됩니다. 비즈니스 운영과 데이터 센터를 통틀어 접근 승인은 개인의 직무 및 구역에 따라 제한됩니다. 데이터 센터의 방화문에는 경보기가 장착되어 있습니다. 데이터 센터 내부와 외부에서는 CCTV 카메라가 작동합니다. 카메라는 무엇보다 경계, 데이터 센터 건물 출입구, 하역장 등 전략적으로 중요한 구역을 촬영할 수 있는 위치에 설치되어 있습니다. 현장 보안 운영 요원은 CCTV 모니터링, 녹화, 제어 장비를 관리합니다. 이러한 CCTV 장비는 데이터 센터 곳곳의 보안 케이블을 통해 연결됩니다. 카메라는 현장에서 디지털 동영상 레코더를 통해 1일 24시간, 주 7일 녹화됩니다. 감시 기록물은 활동에 따라 최대 30일까지 보관됩니다.

(b) 접근 통제.

인프라 보안 요원. Google은 요원에 대한 보안 정책을 마련하고 유지하는 동시에 교육 과정의 일환으로 요원에게 보안 교육을 받도록 요구하고 있습니다. Google의 인프라 보안 요원은 Google의 보안 인프라를 지속적으로 모니터링하고, '서비스'를 검토하고, 보안 사고에 대응해야 하는 책임이 있습니다.

접근 통제 및 권한 관리. '파트너'의 '관리자'와 '파트너 최종 이용자'가 '서비스'를 사용하려면 중앙 인증 시스템이나 싱글 사인온(SSO) 시스템을 통해 본인 인증을 거쳐야 합니다.

내부 데이터 액세스 프로세스 및 정책 - 액세스 정책. Google의 내부 데이터 액세스 프로세스와 정책은 승인되지 않은 개인 및 시스템이 '파트너 데이터'를 처리하는 데 사용되는 시스템에 액세스하지 못하도록 설계되어 있습니다. Google은 (i) 승인된 개인이 액세스가 허용된 데이터에만 액세스할 수 있도록 허용하고, (ii) 처리 및 사용 도중에, 그리고 기록 후에도 승인 없이는 '파트너 데이터'를 읽거나, 복사하거나, 변경하거나, 삭제할 수 없도록 시스템을 설계합니다. 또한 이러한 시스템은 부적절한 액세스를 탐지하도록 설계됩니다. Google은 중앙 집중식 액세스 관리 시스템을 도입하여 프로덕션 서버에 대한 직원 액세스를 제어하는 동시에 소수의 인증된 직원에게만 액세스 권한을 부여합니다. Google의 인증 및 승인 시스템은 SSH 인증서와 보안 키를 사용하며, Google에 안전하고 유연한 액세스 메커니즘을 제공하도록 설계되어 있습니다. 이러한

메커니즘은 사이트 호스트, 로그, 데이터 및 구성 정보에 대해서만 승인된 액세스 권한을 부여하도록 설계되어 있습니다. Google은 고유한 사용자 ID, 안전한 비밀번호, 2단계 인증 및 엄격하게 모니터링된 액세스 목록의 사용을 요구하는 방식으로 승인되지 않은 계정 사용의 가능성을 최소화합니다. 액세스 권한 부여 또는 변경은 승인된 직원의 담당 업무, 승인된 작업을 수행하는 데 필요한 직무 요건, 그리고 알 권리를 기준으로 결정됩니다. 액세스 권한 부여 또는 변경은 또한 Google의 내부 데이터 액세스 정책 및 교육 내용을 따라야 합니다. 승인은 모든 변경사항에 대한 감사 레코드를 유지보수하는 워크플로 도구에서 관리됩니다. 책임 소재를 밝히기 위한 감사 추적을 생성하기 위해 시스템에 대한 액세스 기록이 로깅됩니다. 인증(워크스테이션 로그인 등)을 위해 비밀번호를 도입한 경우에는 최소한 업계 표준 관행에 따라 비밀번호 정책을 마련합니다. 이러한 표준으로는 비밀번호 재사용에 대한 제한과 충분한 비밀번호 안전성 등이 있습니다. 매우 민감한 정보(신용카드 데이터 등)에 대한 액세스의 경우 Google은 하드웨어 토큰을 사용합니다.

3. 데이터

(a) 데이터 저장, 격리 및 로깅. Google은 데이터를 Google 소유 서버의 멀티 테넌트 환경에 저장합니다. 상충되는 내용의 '지침'(예: 데이터 위치 선택)이 없는 한, Google은 지리적으로 분산된 여러 데이터 센터에 '파트너 데이터'를 복제합니다. Google은 또한 '파트너 데이터'를 논리적으로 격리합니다. '파트너'에게는 특정 데이터 공유 정책에 대한 제어 권한이 부여됩니다. '파트너'는 '서비스'의 기능에 따라 이러한 정책을 사용해 '파트너 최종 사용자'에게 특정 목적으로 적용되는 제품 공유 설정을 결정할 수 있습니다. '파트너'는 Google이 '서비스'를 통해 제공하는 로깅 기능 사용 여부를 선택할 수 있습니다.

(b) 사용 중단 디스크 및 디스크 삭제 정책. 데이터가 저장된 디스크가 성능 문제, 오류 또는 하드웨어 장애를 일으킬 경우 사용이 중단될 수 있습니다('사용 중단 디스크'). 모든 '사용 중단 디스크'는 재사용 또는 파기를 목적으로 Google의 시설을 떠나기 전에 일련의 데이터 파기 프로세스('디스크 삭제 정책')를 거치게 됩니다. '사용 중단 디스크'는 여러 단계의 프로세스를 거쳐 삭제되며, 최소 2곳 이상의 독립적인 검증 기관이 삭제 완료 여부를 확인합니다. 삭제 결과는 추적을 위해 '사용 중단 디스크'의 일련번호로 로깅됩니다. 마지막으로, 삭제된 '사용 중단 디스크'는 재사용 및 재배포를 위해 인벤토리에 등록됩니다. 하드웨어 장애로 인해 '사용 중단 디스크'를 삭제하지 못할 경우에는 파기가 가능할 때까지 안전하게 보관합니다. Google은 각 시설을 정기적으로 감사하여 '디스크 삭제 정책'을 준수하는지 모니터링합니다.

4. 직원 보안

Google 직원은 기밀성, 비즈니스 윤리, 적합한 사용, 직업 표준에 대한 회사의 가이드라인에 부합하는 방식으로 행동해야 합니다. Google은 관련 지역 노동법과 법규에 따라 법적으로 허용되는 범위에서 합당한 신원 조사를 실시합니다.

Google 직원은 기밀유지 협약을 이행하고, Google의 기밀유지 및 개인정보처리방침의 수신을 확인하고 준수 사실을 인정해야 합니다. 직원에게는 보안 교육이 제공됩니다. '파트너 데이터'를 취급하는 직원은 자신의 역할에 따라 추가 요건(예: 인증)을 충족해야 합니다. Google 직원은 '파트너 데이터'를 승인 없이 처리하지 않습니다.

5. 보조 프로세서 보안

Google은 '보조 프로세서' 온보딩에 앞서 '보조 프로세서'의 보안 및 개인정보 보호 관행에 대해 감사를 실시하여 '보조 프로세서'가 부여받은 데이터 액세스 권한과 제공하기로 한 서비스 범위에 대해 적절한 수준의 보안 및 개인정보 보호를 제공하도록 보장합니다. Google이 '보조 프로세서'에 의해 발생하는 위험을

평가하고 나면 '보조 프로세서'는 11.3항(보조 프로세서 고용 요건)에 명시된 요건에 따라 적절한 보안, 비밀유지, 개인정보 보호 약정을 체결해야 합니다.

부록 3: 특정 개인정보 보호법

본 부록 3의 각 하위 섹션에 포함된 조항은 '파트너 개인정보' 처리에 관련 법이 적용되는 경우에만 적용됩니다.

유럽 데이터 보호법

1. 추가 정의.

- '적정 데이터 보호 국가'란 다음을 의미합니다.

(a) EU GDPR에 따라 처리되는 데이터의 경우: 유럽 경제 지역 또는 EU GDPR에 따라 적절한 보호를 보장하는 것으로 인정되는 국가 또는 지역

(b) 영국 GDPR에 따라 처리되는 데이터의 경우: 영국 또는 영국 GDPR 및 2018년 데이터 보호법에 따라 적절한 보호를 보장하는 것으로 인정되는 국가 또는 지역

(c) 스위스 FADP에 따라 처리되는 데이터의 경우: 스위스, 또는 다음에 해당하는 국가나 지역: (i) 해당되는 경우, 스위스 연방 데이터 보호법 및 개인정보감독기구가 공표한, 법률에 따라 적절한 보호를 보장하는 국가 목록에 포함된 국가 또는 지역, 또는 (ii) 스위스 FADP에 따라 스위스 연방 의회에서 적절한 보호를 보장하는 것으로 인정되는 국가 또는 지역.

각 경우에서 선택적 데이터 보호 프레임워크를 기준으로 하는 국가 또는 지역은 제외됩니다.

- '대체 전송 솔루션'은 SCC가 아닌 '유럽 데이터 보호법'에 따라 제3의 국가에 개인정보를 합법적으로 전송할 수 있는 솔루션을 가리킵니다. 참여 기관이 적절한 보호를 제공하는 것으로 인정되는 데이터 보호 프레임워크를 예로 들 수 있습니다.
- '파트너 SCC'는 해당되는 경우에 따라 SCC(컨트롤러-프로세서), SCC(프로세서-프로세서), 또는 SCC(프로세서-컨트롤러)를 의미합니다.
- 'SCC'는 해당되는 경우에 따라 '파트너 SCC' 또는 SCC(프로세서-프로세서, 수출자 Google)를 의미합니다.
- 'SCC(컨트롤러-프로세서)'는 <https://cloud.google.com/terms/sccs/eu-c2p>의 조항을 의미합니다.
- 'SCC(프로세서-컨트롤러)'는 <https://cloud.google.com/terms/sccs/eu-p2c>의 조항을 의미합니다.
- 'SCC(프로세서-프로세서)'는 <https://cloud.google.com/terms/sccs/eu-p2p>의 조항을 의미합니다.
- 'SCC(프로세서-프로세서, 수출자 Google)'는 <https://cloud.google.com/terms/sccs/eu-p2p-google-exporter>의 조항을 의미합니다.

2. 지침 알림. 5.2항(파트너의 지침 준수)에 따른 Google의 의무 또는 '계약'에 따른 각 당사자의 기타 권리나 의무를 침해하지 않는 범위 내에서, Google은 자체 판단에 따라 다음과 같은 경우 '파트너'에게 즉시 통지합니다.

a. 유럽 법률에 따라 Google이 '지침'을 준수할 수 없는 경우

b. '지침'이 '유럽 데이터 보호법'을 준수하지 않는 경우

c. 그 밖에 Google이 '지침'을 따를 수 없게 될 경우. '유럽 법률'이 이러한 사실에 대한 통지를 금지하지 않는 한 '파트너'에게 해당 사실을 통지합니다.

'파트너'가 프로세서인 경우, '파트너'는 본 조항에 따라 Google이 제공한 모든 통지를 관련 컨트롤러에게 즉시 전달합니다.

3. 파트너의 감사 권리. Google은 7.5.2(a)항(파트너 감사)에 명시된 바와 같이 '파트너' 또는 '파트너'가 임명한 독립적인 감사자가 감사(점검 포함)를 시행하는 것을 허용합니다. 이러한 감사 과정에서 Google은 본 '부칙'에 따른 의무 준수를 입증하는 데 필요한 모든 정보를 제공하고, 7.5항(규정 준수 검토 및 감사) 및 본 조항에 명시된 대로 감사에 참여합니다.

4. 데이터 전송.

4.1 제한된 전송. 당사자들은 '유럽 데이터 보호법'이 '파트너 개인정보'를 '적정 데이터 보호 국가'에서 처리하거나 해당 국가로 전송하기 위해 SCC 또는 '대체 전송 솔루션'을 요구하지 않는다는 사실을 확인합니다. '파트너 개인정보'가 여타 다른 국가로 전송되고 이러한 전송에 '유럽 데이터 보호법'이 적용되는 경우(청구서 수신 주소가 EMEA 외 지역인 경우 '유럽 데이터 보호법' 약관의 4.2항(EMEA 외 파트너에 의한 인증)에 따라 '파트너'의 인증을 받은 경우)(‘제한된 전송’)에는 다음 사항이 적용됩니다.

a. Google이 '제한된 전송'에 대한 '대체 전송 솔루션'을 채택한 경우: Google은 '파트너'에게 관련 솔루션에 대해 알리고 이러한 '제한된 전송'이 해당 솔루션에 따라 이루어지도록 보장합니다.

b. Google이 '제한된 전송'에 대한 '대체 전송 솔루션'을 채택하지 않았거나, Google이 더 이상 '제한된 전송'에 대한 '대체 전송 솔루션'을 채택하지 않는다는 사실을 '파트너'에게 알린 경우(다른 '대체 전송 솔루션'을 채택하지 않음) 다음을 따릅니다.

i. Google의 주소가 '적정 데이터 보호 국가'에 속하는 경우 다음 조항이 적용됩니다.

A. Google이 '보조 프로세서'로 전송하는 이러한 '제한된 전송'에 대해 SCC(프로세서-프로세서, 수출자 Google)가 적용됩니다.

B. 또한 '파트너'의 청구서 수신 주소가 '적정 데이터 보호 국가'에 속하지 않는 경우, Google과 '파트너' 간의 이러한 '제한된 전송'에 대해 SCC(프로세서-컨트롤러)가 적용됩니다('파트너'가 컨트롤러인지 프로세서인지 여부와 관계없음).

ii. Google의 주소가 '적정 데이터 보호 국가'에 속하지 않는 경우, Google과 '파트너' 간의 이러한 '제한된 전송'에 대해 SCC(컨트롤러-프로세서) 또는 SCC(프로세서-프로세서)가 적용됩니다('파트너'가 '컨트롤러'인지 '프로세서'인지에 따라 다름).

4.2 EMEA 외 파트너에 의한 인증. '파트너'의 청구서 수신 주소가 EMEA에 속하지 않고 '파트너 개인정보' 처리가 '유럽 데이터 보호법'을 따르는 경우, 본 '부칙'의 부록 4(특정 제품)에 달리 명시되지 않는 한 '파트너'는 관련 '서비스'의 '관리 콘솔'을 통해 인증을 진행하고 관할 '감독 당국'을 파악합니다.

4.3 제한된 전송에 관한 정보. Google은 '파트너'에게 '제한된 전송', '추가 보안 제어' 및 기타 추가적인 보호 조치와 관련된 정보를 다음과 같이 제공합니다.

a. 7.5.1항(보안 문서 검토)에 명시된 내용에 따라 정보를 제공합니다.

b. 부록 4(특정 제품)에 명시된 추가 위치에 따른 정보를 제공합니다.

c. <https://cloud.google.com/terms/alternative-transfer-solution>에 명시된 Google의 '대체 전송 솔루션' 채택과 관련된 정보를 제공합니다.

4.4 SCC 감사. '파트너 SCC'가 '유럽 데이터 보호법'의 4.1항(제한된 전송)에 명시된 대로 적용되는 경우, Google은 7.5.3항(검토 및 감사를 위한 추가 비즈니스 약관)에 따라 '파트너'(또는 '파트너'가 임명한 독립적인 감사자)가 해당 SCC에 명시된 대로 감사를 진행하는 것을 허용하며, 감사 중에 해당 SCC에서 요구하는 모든 정보를 제공합니다.

4.5 SCC 통지. '파트너'는 관련 컨트롤러에게 SCC에 대한 모든 통지를 신속하고 지체없이 전달해야 합니다.

4.6 데이터 전송 위험으로 인한 계약 해지. '파트너'가 '서비스'의 현재 사용 또는 의도된 사용에 근거하여 전송된 '파트너 개인정보'에 대한 적절한 보호 조치가 제공되지 않는다고 판단할 경우, '파트너'는 '계약'의 편의에 의한 해지 조항에 따라 또는 이러한 조항이 없는 경우 Google에 통지하여 '계약'을 즉시 해지할 수 있습니다.

4.7 SCC 수정 금지. 본 '계약'(본 '부칙' 포함)의 어떠한 내용도 SCC를 변경 또는 부정하거나, '유럽 데이터 보호법'에 따른 정보주체의 기본적인 권리 또는 자유를 침해하려는 의도가 없습니다.

4.8 SCC 우선 적용. '파트너 SCC'(본 '부칙'에 인용으로 포함됨)와 '계약'(본 '부칙' 포함)의 나머지 부분 간에 충돌이나 불일치가 있는 경우, '파트너 SCC'가 우선합니다.

5. 보조 프로세서 고용 요건. '유럽 데이터 보호법'에 따라 Google은 GDPR의 28조 3항에 명시된 바에 따라, 해당되는 경우, 본 '부칙'에 명시된 데이터 보호 의무가 Google이 고용한 모든 '보조 프로세서'에게 부과되도록 서면 계약을 통해 보장해야 합니다.

CCPA

1. 추가 정의.

- 'CCPA'란 2018년 캘리포니아 소비자 개인정보 보호법과 그 개정사항을 의미하며, 여기에는 2020년 캘리포니아 개인정보 보호 권리법에 의한 개정사항과 모든 시행 규정을 포함합니다.
- '파트너 개인정보'에는 '개인정보'가 포함됩니다.
- '비즈니스', '비즈니스 목적', '소비자', '개인정보', '처리', '영업', '판매', '서비스 제공자', '공유'와 같은 용어는 CCPA에서 정의한 의미를 지닙니다.

2. 금지사항. 5.2항(파트너 지침 준수)에 따른 Google의 의무를 침해하지 않는 범위 내에서, CCPA에 따른 '파트너 개인정보' 처리에 관해 Google은 CCPA에서 달리 허용되지 않는 한 다음을 수행하지 않습니다.

a. '파트너 개인정보'를 판매하거나 공유

b. 다음과 같은 경우에 '파트너 개인정보'를 보관, 사용 또는 공개

i. CCPA에 따라 '파트너'를 대신하는 비즈니스 목적이 아니거나 '서비스' 및 TSS 수행과 관련된 구체적인 목적이 아닌 경우

ii. Google과 '파트너' 간의 직접적인 비즈니스 관계가 아닌 경우

c. Google이 제3자로부터 또는 제3자를 대신하여 수신한 '개인정보' 또는 Google이 소비자와 직접 상호작용하여 수집한 '개인정보'를 '파트너 개인정보'와 결합 또는 업데이트

3. 규정 준수. 5.2항(파트너 지침 준수)에 따른 Google의 의무 또는 '계약'에 따른 각 당사자의 여타 권리 또는 의무를 침해하지 않는 범위 내에서, Google은 Google이 CCPA에 따른 의무를 이행할 수 없다고 판단되는 경우, 관련 법에서 금지하지 않는 한 '파트너'에게 이러한 사실을 통지합니다.

4. 파트너 개입. Google이 본 하위 섹션의 3항(규정 준수) 또는 7.2.1항(사고 알림)의 경우를 포함하여 '파트너'에게 '파트너 개인정보'가 무단으로 사용된 사실을 통지하는 경우, '파트너'는 이러한 무단 사용을 중지하거나 해결하기 위한 합리적이고 적절한 조치를 다음과 같은 방식으로 취할 수 있습니다.

a. 해당되는 경우 7.2.2항(데이터 사고 세부정보)에 따라 Google이 권장하는 조치를 취합니다.

b. 7.5.2(a)항(파트너 감사) 또는 9.1항(액세스, 정정, 제한적 처리, 이동성)에 따른 권리를 행사합니다.

튀르키예

1. 추가 정의.

- '튀르키예 데이터 보호법'은 2016년 4월 7일에 제정된 개인정보 보호에 대한 튀르키예 법률 제6698호를 의미합니다.
- '튀르키예 개인정보 보호 당국'은 'Kişisel Verileri Koruma Kurumu'를 가리킵니다.
- '튀르키예 SCC'는 '튀르키예 데이터 보호법'에 따른 표준 계약 조항을 의미합니다.

2. 데이터 전송.

2.1 추가 약관. '파트너'의 청구서 수신 주소가 튀르키예에 있고 Google이 '튀르키예 데이터 보호법'에 따라 '파트너 개인정보'의 전송과 관련하여 '파트너'가 수락할 수 있는 선택적 추가 약관(튀르키예 SCC 포함)을 제공하는 경우, 이러한 약관은 아래의 2.2항(관할 당국에 대한 알림)에 따라 '튀르키예 개인정보 보호 당국'에 통지된 날짜를 기준으로 '파트너'가 이러한 통지 사실을 Google에 입증한 바에 따라 본 '부칙'을 보완하는 효력을 가집니다.

2.2 관할 당국에 대한 알림. '파트너'가 본 2항(데이터 전송)에 따라 튀르키예 SCC를 체결한 경우, '파트너'는 '튀르키예 데이터 보호법'에 따라 '튀르키예 개인정보 보호 당국'에 튀르키예 SCC 사용에 대해 튀르키예 SCC에 서명하여 영업일 기준 5일 이내에 통지해야 합니다.

2.3 SCC 감사. 본 2항(데이터 전송)에 따라 '파트너'가 튀르키예 SCC를 체결한 경우, Google은 7.5.3항(검토 및 감사를 위한 추가 비즈니스 약관)에 따라 '파트너'(또는 '파트너'가 임명한 독립적인 감사자)가 해당 SCC에 명시된 대로 감사를 수행할 수 있도록 허용하며, 감사 중에 해당 SCC에서 요구하는 모든 정보를 제공합니다.

2.4 데이터 전송 위험으로 인한 계약 해지. '파트너'가 '서비스'의 현재 사용 또는 의도된 사용에 근거하여 전송된 '파트너 개인정보'에 대한 적절한 보호 조치가 제공되지 않는다고 판단할 경우, '파트너'는 '계약'의 편의에 의한 해지 조항에 따라 또는 이러한 조항이 없는 경우 Google에 통지하여 관련 '계약'을 즉시 해지할 수 있습니다.

2.5 튀르키예 SCC 수정 금지 본 '계약'(본 '부칙' 포함)의 어떠한 내용도 튀르키예 SCC를 변경 또는 부정하거나, '튀르키예 데이터 보호법'에 따른 정보주체의 기본적인 권리 또는 자유를 침해하려는 의도가 없습니다.

2.6 SCC 우선 적용. '튀르키예 SCC'('파트너'가 해당 SCC를 체결한 경우 본 '부칙'에 인용으로 포함됨)와 '계약'(본 '부칙' 포함)의 나머지 부분 간에 충돌이나 불일치가 있는 경우, '튀르키예 SCC'가 우선합니다.

이스라엘

1. 추가 정의.

- '이스라엘 개인정보 보호법'은 1981년 제정된 '이스라엘 개인정보 보호법'과 이에 따라 공포된 모든 규정을 의미합니다.

2. 대응하는 용어. 본 '부칙'에서 사용되는 '컨트롤러', '개인정보', '처리', '프로세서'에 대응하는 용어는 '이스라엘 개인정보 보호법'에 명시된 의미를 지닙니다.

3. 파트너의 감사 권리. Google은 7.5.2(a)항(파트너 감사)에 명시된 바와 같이 '파트너' 또는 '파트너'가 임명한 독립적인 감사자가 감사(점검 포함)를 시행하는 것을 허용합니다.

부록 4: 특정 제품

본 부록 4의 각 하위 섹션에 포함된 조항은 해당 '서비스'에 의한 '파트너 데이터' 처리에 대해서만 적용됩니다.

Google Cloud Platform

1. 추가 정의.

- '계정'은 '계약'에 정의되어 있지 않은 경우 '파트너'의 Google Cloud Platform 계정을 의미합니다.
- 'Google Cloud Platform'은 <https://cloud.google.com/terms/services>에 명시된 Google Cloud Platform 서비스를 의미하며, '서드 파티 서비스'는 제외됩니다.
- '서드 파티 서비스'는 '계약'에 달리 정의되지 않은 경우 (a) Google Cloud Platform 또는 '소프트웨어'에 통합되어 있지 않은 서드 파티 서비스, 소프트웨어, 제품 및 기타 서비스, (b) '계약'의

'서비스별 약관'에 포함된 '서드 파티 약관' 조항에서 의미하는 서비스, (c) 서드 파티 운영체제를 의미합니다.

2. 규정 준수 인증. Google Cloud Platform '감사 서비스'에 대한 '규정 준수 인증'에는 ISO 27017 및 ISO 27018 인증서와 PCI DSS 준수 증명도 포함됩니다.

3. 데이터 센터 위치. Google Cloud Platform 데이터 센터의 위치는 <https://cloud.google.com/about/locations/>에 명시되어 있습니다.

4. 보조 프로세서에 관한 정보. Google Cloud Platform '보조 프로세서'의 이름, 위치, 활동에 관한 정보는 <https://cloud.google.com/terms/subprocessors>에 명시되어 있습니다.

5. Cloud 데이터 보호팀. Google Cloud Platform의 데이터 보호팀에는 <https://support.google.com/cloud/contact/dpo> 페이지를 통해 문의할 수 있습니다.

6. 제한된 전송에 관한 정보. '제한된 전송', '추가 보안 제어' 및 기타 추가적인 보호 조치와 관련된 더 많은 정보는 <https://cloud.google.com/privacy>에서 확인할 수 있습니다.

7. 서비스별 약관.

베어메탈 솔루션(Google Cloud Platform)

베어메탈 솔루션은 기반 인프라 리소스에 대한 비가상화 액세스를 제공하며, 설계상 고유한 특성이 있습니다.

1. 개정안. 본 '부칙'은 베어메탈 솔루션에 대해 다음과 같이 개정됩니다.

- 'Google의 제3자 감사자'의 정의가 다음과 같이 대체됩니다.
 - 'Google의 제3자 감사자'는 Google 또는 베어메탈 솔루션 '보조 프로세서'가 임명하고 자격을 갖춘 독립적인 제3자 감사자를 의미하며, Google은 '파트너'의 요청이 있는 경우 해당 감사자의 당시 신분을 '파트너'에게 공개합니다.
- 다음 조항이 삭제됩니다.
 - 7.1.1항(Google의 보안 조치)에서 '파트너 데이터 암호화' 문구
 - 부록 2(보안 조치)의 1(a)항에서 제목이 '서버 운영체제' 및 '비즈니스 연속성'인 하위 섹션
 - 부록 2의 1(b)항에서 제목이 '외부 공격 표면', '침입 감지', '암호화 기술'인 하위 섹션
 - 부록 2의 3(a)항에 포함된 다음 문장을 삭제합니다.
 - Google은 데이터를 Google 소유 서버의 멀티 테넌트 환경에 저장합니다. 상충되는 내용의 '파트너' 지침(예: 데이터 위치 선택)이 없는 한, Google에서는 '파트너 데이터'를 여러 지역으로 분산된 데이터 센터에 복제합니다.

2. 규정 준수 인증 및 SOC 보고서. Google 또는 Google의 '보조 프로세서'는 '보안 조치'의 지속적인 효과를 검증할 수 있도록 베어메탈 솔루션에 대해 최소한 다음 사항(또는 이에 상응하거나 강화된 대안)을 유지합니다.

a. ISO 27001 인증서 및 PCI DSS 준수 증명('BMS 규정 준수 인증')

b. 12개월마다 최소 1회 수행되는 감사를 바탕으로 매년 업데이트되는 SOC 1 및 SOC 2 보고서('BMS SOC 보고서')

3. 보안 문서 검토. Google이 본 '부칙'에 따른 의무를 준수하고 있음을 입증하기 위해 Google은 '파트너'가 검토할 수 있도록 'BMS 규정 준수 인증' 및 'SOC 보고서'를 제공하며, '파트너'가 프로세서인 경우 7.5.3항(검토 및 감사를 위한 추가 비즈니스 약관)에 따라 관련 컨트롤러가 'BMS SOC 보고서'에 액세스할 수 있는 권한을 '파트너'가 요청하도록 허용합니다.

4. 파트너 의무. '파트너'는 베어메탈 솔루션과 관련된 Google의 명시적 의무를 제한하지 않으면서, '파트너 데이터'와 베어메탈 솔루션에 저장되어 있거나 베어메탈 솔루션을 통해 처리된 여타 콘텐츠의 보안을 보전하고 유지하기 위한 합당한 조치를 취합니다.

5. 면책 조항. '계약'(본 '부칙' 포함)에 어떠한 상충되는 내용이 있더라도, Google은 베어메탈 솔루션과 관련하여 다음에 해당하는 경우 책임을 지지 않습니다.

a. 액세스 제어, 암호화, 방화벽, 바이러스 백신 프로그램, 위협 탐지, 보안 스캔 등의 비물리적 보안

b. 로깅 및 모니터링

c. 비하드웨어 유지보수 또는 지원

d. 중복 또는 고가용성 구성을 포함한 데이터 백업

e. 비즈니스 연속성 및 재해 복구 정책 또는 절차

'파트너'가 베어메탈 솔루션과 함께 사용하거나, 베어메탈 솔루션에 업로드하거나 호스팅하는 '운영체제', '파트너 데이터', 소프트웨어, 애플리케이션에 대한 보안(베어메탈 솔루션 서버에 대한 물리적 보안 제외), 로깅, 모니터링, 유지보수, 지원, 백업에 대한 책임은 전적으로 '파트너'에게 있습니다.

Cloud NGFW(Google Cloud Platform)

'Cloud NGFW Enterprise'('CNE')라는 이름의 Cloud NGFW 버전은 사이버 보안 위험을 완화하도록 설계되었으며, 이에 따라 고유한 특성이 있습니다.

1. 개정안. 본 '부칙'은 'CNE'에 대해 다음과 같이 개정됩니다.

- 6.1항(파트너에 의한 삭제) 및 6.2항(계약 기간 종료 시 반환 또는 삭제)은 Google 또는 '보조 프로세서'가 TSS 목적으로 제출되고 'CNE'에 의해 보안 위협으로 고용된 파일 또는 네트워크 트래픽 패킷 캡처(해당 파일 또는 네트워크 트래픽 패킷 캡처에 '파트너 개인정보'가 포함되지 않은 경우)를 보관하는 것을 막지 않습니다.

Google Distributed Cloud Edge(Google Cloud Platform)

Google Distributed Cloud Edge('GDCE')는 Google 데이터 센터에 배포되지 않으며, 설계상 고유한 특성이 있습니다.

1. 개정안. 본 '부칙'은 'GDCE'에 대해 다음과 같이 개정됩니다.

- 'Google의 시스템'에 대한 언급이 '장비'로 대체됩니다.
- 6.2항(계약 기간 종료 시 반환 또는 삭제)이 다음 항목으로 대체됩니다.
 - 6.2 계약 기간 종료 시점에 반환 또는 삭제. '파트너'는 '계약 기간' 종료 시점에 관련 법에 따라 '장비'에 남아 있는 모든 '파트너 데이터'(기존 사본 포함)를 삭제하도록 지시합니다. '파트너'가 '계약 기간' 종료 후에도 '파트너 데이터'를 보관하기를 원할 경우, '파트너'는 '계약 기간'이 종료되기 전에 해당 데이터를 내보내거나 복사할 수 있습니다. Google은 합리적으로 실행 가능한 범위 내에서 가능한 한 신속하게, 그리고 최대 180일 기간 내에 본 6.2항의 '지침'을 이행합니다. 단, '유럽 데이터 보호법' 적용하에 '유럽 법률'에 따른 보관이 요구되거나, 기타 '관련 개인정보 보호법' 적용하에 관련 법률에 따른 보관이 요구되는 경우는 예외로 합니다.
- 10.1항(데이터 저장 및 처리 시설)의 끝부분에 "또는 '고객 위치'가 자리한 곳"이라는 표현이 추가됩니다.
- 부록 2(보안 조치)의 1항(데이터 센터 및 네트워크 보안)이 다음과 같이 대체됩니다.
 - 1. 로컬 머신 및 네트워크 보안

로컬 머신. '파트너 데이터'는 '고객 위치'에 배포되는 '장비'에만 저장됩니다.

서버 운영체제. Google 서버는 적용 환경에 맞게 맞춤설정된 Linux 기반 운영체제를 사용합니다. Google은 코드 검토 프로세스를 도입하여 'GDCE'를 제공하는 데 사용되는 코드의 보안을 강화하고 'GDCE' 프로덕션 환경에서 보안 제품을 개선합니다.

암호화 기술. Google은 HTTPS 암호화(SSL 또는 TLS 연결이라고도 함)를 제공하고 전송 중 데이터 암호화를 허용합니다. Google 서버는 RSA와 ECDSA로 서명된 일회성 타원 곡선 디피-헬만(Diffie-Hellman) 암호화 키 교환을 지원합니다. 이러한 PFS(Perfect Forward Secrecy) 기법은 트래픽을 보호할 뿐만 아니라 키 유출 또는 암호 해독으로 인한 침투의 영향을 최소화하는 데도 효과적입니다. Google은 또한 최소한 AES128 또는 이와 유사한 암호화 방식을 사용하여 저장 데이터 암호화를 지원합니다. 'GDCE'에는 CMEK 통합 기능이 있습니다. 자세한 내용은 <https://cloud.google.com/kms/docs/cmek>에서 확인할 수 있습니다.

Cloud VPN 연결. Google은 '파트너'가 IPsec VPN 연결을 통해 Cloud VPN을 사용하여 '장비'와 '파트너'의 '가상 프라이빗 클라우드' 간에 강력하고 암호화된 상호 연결을 설정하고 구성하는 것을 허용합니다.

결합 스토리지. '파트너'의 데이터 스토리지는 서버에 결합되어 있습니다. 디스크가 도난당하거나 저장 중 복사되는 경우, 해당 디스크의 내용을 서버 외부에서 복구할 수 없습니다.

- 부록 2(보안 조치)의 2항(액세스 및 사이트 제어)과 3항(데이터)이 삭제됩니다.

2. 적용 불가능한 조항. '계약'(본 '부칙' 포함)에 규정된 Google의 의무 또는 관련 보안 문서(백서 포함)에 명시된 내용 중 Google의 Google 데이터 센터 운영을 전제로 하는 내용은 'GDCE'에 적용되지 않습니다.

Google 관리형 멀티 클라우드(Google Cloud Platform)

'Google 관리형 멀티 클라우드 서비스'는 서드 파티 인프라를 필요로 하며, 설계상 고유한 특성이 있습니다.

1. 추가 정의.

- 'Google 관리형 MCS 데이터 처리 수정안'은 <https://cloud.google.com/terms/mcs-data-processing-terms>의 조항을 의미합니다.

2. 멀티 클라우드 데이터 처리 약관. 'Google 관리형 MCS 데이터 처리 수정안'은 Google Cloud Platform의 'Google 관리형 멀티 클라우드 서비스'에 대해 본 '부칙'을 보완하고 개정합니다.

Google Cloud VMware Engine(Google Cloud Platform)

Google은 '파트너'의 VMware 환경에 대한 액세스 권한이 없거나 '파트너'의 VMware 환경에서 개인정보를 암호화하지 못할 수 있습니다.

NetApp Volumes(Google Cloud Platform)

1. 개정안. 본 '부칙'은 NetApp Volumes에 대해 다음과 같이 개정됩니다.

- 'Google의 제3자 감사자'의 정의가 다음과 같이 대체됩니다.
 - 'Google의 제3자 감사자'는 Google 또는 NetApp Volumes '보조 프로세서'가 임명하고 자격을 갖춘 독립적인 제3자 감사자를 의미하며, Google은 '파트너'의 요청이 있는 경우 해당 감사자의 당시 신분을 '파트너'에게 공개합니다.
- 부록 2(보안 조치)의 3(a)항(데이터 저장, 격리 및 로깅)이 다음과 같이 대체됩니다.
 - (a) 데이터 저장, 격리 및 로깅. Google은 NetApp, Inc.가 소유한 서버의 멀티 테넌트 환경에 데이터를 저장합니다. 상충되는 내용의 '지침'(예: 데이터 위치 선택)이 없는 한, Google은 지리적으로 분산된 여러 데이터 센터에 '파트너 데이터'를 복제합니다. Google은 또한 '파트너 데이터'를 논리적으로 격리합니다. '파트너'에게는 특정 데이터 공유 정책에 대한 제어 권한이 부여됩니다. '파트너'는 '서비스'의 기능에 따라 이러한 정책을 사용해 '파트너 최종 사용자'에게 특정 목적으로 적용되는 제품 공유 설정을 결정할 수 있습니다. '파트너'는 Google이 '서비스'를 통해 제공하는 로깅 기능 사용 여부를 선택할 수 있습니다.

2. 규정 준수 인증 및 SOC 보고서. Google 또는 Google의 '보조 프로세서'는 NetApp Volumes에 대해 최소한 다음 사항(또는 이에 상응하거나 강화된 대안)을 유지합니다.

a. ISO 27001 인증서 및 PCI DSS 준수 증명('NetApp 규정 준수 인증')

b. 12개월마다 최소 1회 수행되는 감사를 바탕으로 매년 업데이트되는 SOC 1 및 SOC 2 보고서('NetApp SOC 보고서')

3. 보안 문서 검토. Google이 본 '부칙'에 따른 의무를 준수하고 있음을 입증하기 위해 Google은 '파트너'가 검토할 수 있도록 'NetApp 규정 준수 인증' 및 'NetApp SOC 보고서'를 제공하며, '파트너'가 프로세서인 경우 7.5.3항(검토 및 감사를 위한 추가 비즈니스 약관)에 따라 관련 컨트롤러가 'NetApp SOC 보고서'에 액세스할 수 있는 권한을 '파트너'가 요청하도록 허용합니다.

Looker(원본)

1. 추가 정의.

- '관리 콘솔'은 각 인스턴스에 해당하는 모든 관리 콘솔을 의미합니다.
- 'Google 관리형 MCS 데이터 처리 수정안'은 해당되는 경우 <https://cloud.google.com/terms/mcs-data-processing-terms>의 조항을 의미합니다.
- 'Google 관리형 멀티 클라우드 서비스'는 해당되는 경우 서드 파티 클라우드 제공업체의 인프라에서 호스팅되는 고용된 Google 서비스, 제품, 기능을 의미합니다.
- 'Looker(원본)'는 비즈니스가 Google에서 '파트너'에게 '계약'에 따라 제공하는 여러 데이터 소스를 사용해 데이터를 분석하고 비즈니스 측정항목을 정의할 수 있도록 하는 통합 플랫폼(해당되는 경우 클라우드 기반 인프라 및 모든 관련 API를 비롯한 소프트웨어 구성요소를 포함)을 의미합니다. 'Looker(원본)'에서 '서드 파티 서비스'는 제외됩니다.
- '멀티 클라우드 서비스 서드 파티 제공업체'는 'Google 관리형 MCS 데이터 처리 수정안'에 명시된 의미를 지닙니다.
- '주문 양식'은 '계약'에 명시된 의미를 지니며, '파트너'가 리셀러 또는 온라인 마켓플레이스를 통해 구매했거나 무료 체험판 또는 평가 계약에 따라 Looker를 체험 또는 평가 목적으로만 사용하는 경우는 제외됩니다. 이때 '주문 양식'은 Google이 승인한 또 다른 서면 양식(이메일 또는 기타 허용되는 전자적 수단)을 의미할 수 있습니다.

2. 개정안. 본 '부칙'은 'Looker(원본)'에 대해 다음과 같이 개정됩니다.

- '알림 이메일 주소'의 정의는 다음과 같이 대체됩니다.
 - '알림 이메일 주소'는 Google로부터 특정 알림을 받기 위해 '주문 양식'에서 또는 Looker(해당하는 경우)를 통해 '파트너'가 고용한 이메일 주소를 의미합니다.
- 부록 3(특정 개인정보 보호법)에서 'SCC(컨트롤러-프로세서)', 'SCC(프로세서-컨트롤러)', 'SCC(프로세서-프로세서)', 'SCC(프로세서-프로세서, 수출자 Google)'의 정의가 다음과 같이 대체됩니다.
 - 'SCC(컨트롤러-프로세서)'는 <https://cloud.google.com/terms/looker/legal/sccs/eu-c2p>의 조항을 의미합니다.
 - 'SCC(프로세서-컨트롤러)'는 <https://cloud.google.com/terms/looker/legal/sccs/eu-p2c>의 조항을 의미합니다.
 - 'SCC(프로세서-프로세서)'는 <https://cloud.google.com/terms/looker/legal/sccs/eu-p2p>의 조항을 의미합니다.
 - 'SCC(프로세서-프로세서, 수출자 Google)'는 <https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group>의 조항을 의미합니다.
- 10.1항(데이터 저장 및 처리 시설)의 끝부분에 "또는 '멀티 클라우드 서비스 서드 파티 제공업체'가 시설을 유지하는 곳"이라는 표현이 추가됩니다.

3. 추가적인 파트너 보안 책임. '파트너'는 Google에서 관리 및 제어하는 시스템을 제외하고 'Looker(원본)'에 대한 '파트너'의 환경, 데이터베이스, 구성의 보안을 유지할 책임이 있습니다.

4. 규정 준수 인증 및 SOC 보고서. 'Looker(원본)' '감사 서비스'에 대한 '규정 준수 인증 및 SOC 보고서'는 관련 '서비스'가 사용되는 호스팅 환경에 따라 달라질 수 있습니다. 요청 시 Google은 특정 호스팅 환경에서 사용 가능한 '규정 준수 인증 및 SOC 보고서'의 세부정보를 제공합니다.

5. 데이터 센터 위치. 'Looker(원본)' 데이터 센터 위치는 해당하는 '주문 양식'에 설명되어 있으며, 그렇지 않은 경우 Google에서 별도로 명시합니다.

6. EMEA 외 파트너에 의한 인증 금지. '파트너'는 'Looker(원본)'에 대해 부록 3(특정 개인정보 보호법)의 '유럽 데이터 보호' 조항 4.2항(EMEA 외 파트너에 의한 인증)에 명시된 대로 '파트너'의 관할 '감독 당국'을 인증하거나 증명할 의무가 없습니다.

7. 제한된 전송에 관한 정보. 'Looker(원본)'에 대한 '제한된 전송', '추가 보안 제어', 기타 추가적인 보호 조치와 관련된 더 많은 정보는 <https://docs.looker.com>에서 확인할 수 있습니다.

8. 보조 프로세서에 관한 정보. 'Looker(원본)'에 대한 '보조 프로세서'의 이름, 위치, 활동에 관한 정보는 다음 페이지에 명시되어 있습니다.

a. <https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors>

b. <https://cloud.google.com/terms/subprocessors>.

9. Google 관리형 멀티 클라우드(Looker(원본))

'Google 관리형 멀티 클라우드 서비스'는 서드 파티 인프라를 필요로 하며, 설계상 고유한 특성이 있습니다.

9.1 멀티 클라우드 데이터 처리 약관. 'Google 관리형 MCS 데이터 처리 수정안'은 'Looker(원본)'의 'Google 관리형 멀티 클라우드 서비스'에 대해 본 '부칙'을 보완하고 수정합니다.

10. Cloud 데이터 보호팀. 'Looker(원본)'의 '데이터 보호팀'에는 <https://support.google.com/cloud/contact/dpo> 페이지를 통해 문의할 수 있습니다.

11. Google의 처리 기록. '관련 개인정보 보호법'에 따라 Google이 '파트너' 또는 '파트너'의 '고객'과 관련된 특정 정보의 기록을 수집 및 유지해야 하는 경우, '파트너'는 Google의 요청에 따라 해당 정보를 제공하고, 해당 정보의 정확성과 최신성을 유지하는 데 필요한 업데이트가 있을 경우 이를 Google에 알려야 합니다. 단, Google이 해당 정보를 다른 방식으로 제공 및 업데이트해 달라고 요청한 경우는 예외로 합니다.

12. 추가적인 애플리케이션 보안 조치. Google은 'Looker(원본)'에 대해 아래에 명시된 추가적인 '보안 조치'를 이행하고 유지합니다.

a. Google은 보안 아키텍처에 대해 최소한 업계 표준 관행을 따릅니다. Google 애플리케이션에 사용되는 프록시 서버는 IP 차단 목록 및 연결 비율 제한을 통해 공격을 필터링하는 단일 지점을 제공하여 Looker 액세스 보안에 도움이 됩니다.

b. '파트너' 관리자는 '파트너' 또는 '파트너 최종 이용자'가 요청한 기술 지원을 제공하기 위해 Google 직원의 애플리케이션 액세스를 제어합니다.

SecOps 서비스

1. 추가 정의.

- '계정'은 '계약'에 정의되어 있지 않으면 경우에 따라 '파트너'의 'SecOps 서비스' 또는 Google Cloud Platform 계정을 의미합니다.
- 'SecOps 서비스'는 <https://cloud.google.com/terms/secops/services>에 각각 명시된 바와 같이 Chronicle SIEM, Chronicle SOAR, Mandiant Solutions를 의미하며, 모든 '서드 파티 서비스'는 제외됩니다. 의심의 소지를 없애기 위해 'SecOps 서비스'에서 'Mandiant 관리형 서비스' 및 'Mandiant 컨설팅 서비스'는 제외됩니다.
- '서드 파티 서비스'는 '계약'에 달리 정의되지 않은 경우 (a) 'SecOps 서비스' 또는 '소프트웨어'에 통합되어 있지 않은 서드 파티 서비스, 소프트웨어, 제품 및 기타 서비스와 (b) 서드 파티 운영체제를 의미합니다.

2. 개정안. 본 '부칙'은 'SecOps 서비스'에 대해 다음과 같이 개정됩니다.

- '추가 보안 제어'의 정의가 다음과 같이 대체됩니다.
 - '추가 보안 제어'는 '파트너'가 재량으로 선택 및/또는 결정하여 사용할 수 있는 보안 리소스, 구성요소, 기능 및/또는 제어(있는 경우)를 의미하며, 여기에는 (있는 경우) 암호화, 로깅 및 모니터링, ID 및 액세스 관리, 보안 스캔이 포함됩니다.
- '감사 서비스'의 정의가 다음과 같이 대체됩니다.
 - '감사 서비스'는 <https://cloud.google.com/security/compliance/secops/services-in-scope> 페이지에서 관련된 인증 또는 보고서의 범위에 속하는 것으로 표시된 해당 시점의 'SecOps 서비스'를 의미합니다. Google은 '계약'에 따라 'SecOps 서비스'가 중단된 경우가 아닌 한 이 URL에 안내된 어떠한 'SecOps 서비스'도 삭제할 수 없습니다.
- 부록 3(특정 개인정보 보호법)에서 'SCC(컨트롤러-프로세서)', 'SCC(프로세서-컨트롤러)', 'SCC(프로세서-프로세서)', 'SCC(프로세서-프로세서, 수출자 Google)'의 정의가 다음과 같이 대체됩니다.
 - 'SCC(컨트롤러-프로세서)'는 <https://cloud.google.com/terms/secops/scs/eu-c2p>의 조항을 의미합니다.
 - 'SCC(프로세서-컨트롤러)'는 <https://cloud.google.com/terms/secops/scs/eu-p2c>의 조항을 의미합니다.
 - 'SCC(프로세서-프로세서)'는 <https://cloud.google.com/terms/secops/scs/eu-p2p>의 조항을 의미합니다.
 - 'SCC(프로세서-프로세서, 수출자 Google)'는 <https://cloud.google.com/terms/scs/secops/eu-p2p-google-exporter>의 조항을 의미합니다.

- 본 '부칙'의 7.4항(규정 준수 인증 및 SOC 보고서)은 다음과 같이 수정됩니다.
 - 7.4 규정 준수 인증 및 SOC 보고서. Google은 '보안 조치'('규정 준수 인증' 및 'SOC 보고서')의 지속적인 효과를 검증하기 위해 '감사 서비스'에 대해 최소한 <https://cloud.google.com/security/compliance/secops/services-in-scope>에 명시된 인증 및 보고서를 유지합니다.

Google은 언제든지 표준을 추가할 수 있습니다. Google은 '규정 준수 인증' 또는 'SOC 보고서'를 이에 상응하거나 강화된 인증 또는 보고서로 대체할 수 있습니다.

3. 데이터 센터 위치. 'SecOps 서비스' 데이터 센터의 위치는 <https://cloud.google.com/terms/secops/data-residency>에 명시되어 있습니다.

4. EMEA 외 파트너에 의한 인증 금지. '파트너'는 'SecOps 서비스'에 대해 부록 3(특정 개인정보 보호법)의 '유럽 데이터 보호' 조항 4.2항(EMEA 외 파트너에 의한 인증)에 명시된 대로 '파트너'의 관할 '감독 당국'을 인증하거나 증명할 의무가 없습니다.

5. 보조 프로세서에 관한 정보. 'SecOps 서비스'에 대한 '보조 프로세서'의 이름, 위치, 활동에 관한 정보는 <https://cloud.google.com/terms/secops/subprocessors>에 명시되어 있습니다.

6. Cloud 데이터 보호팀. 'SecOps 서비스'의 데이터 보호팀에는 <https://support.google.com/cloud/contact/dpo> 페이지(및/또는 Google에서 경우에 따라 제공하는 기타 수단)를 통해 문의할 수 있습니다.

7. Google의 처리 기록. '관련 개인정보 보호법'에 따라 Google이 '파트너'와 관련된 특정 정보의 기록을 수집 및 유지해야 하는 경우, '파트너'는 Google의 요청에 따라 해당 정보를 제공하고, 해당 정보의 정확성과 최신성을 유지하는 데 필요한 업데이트가 있을 경우 이를 Google에 알려야 합니다. 단, Google이 해당 정보를 다른 방식으로 제공 및 업데이트해 달라고 요청한 경우는 예외로 합니다.

데이터 처리 및 보안 약관(파트너)의 이전 버전

[2022년 6월 30일](#) [2021년 9월 24일](#) [2020년 8월 20일](#) [2020년 8월 10일](#) [2020년 7월 17일](#) [2019년 10월 1일](#)
[2019년 2월 28일](#) [2018년 5월 25일](#) [2018년 3월 13일](#)

SecOps 서비스 데이터 처리 및 보안 약관(파트너)의 이전 버전

[2023년 2월 6일](#) [2022년 10월 31일](#) [2021년 9월 27일](#)

이전 버전(최종 수정일: 2024년 10월 30일)

[2024년 10월 15일](#) [2024년 9월 26일](#) [2024년 9월 9일](#) [2024년 4월 9일](#) [2023년 11월 8일](#) [2023년 8월 15일](#)
[2022년 9월 20일](#)