

Lenovo NetFilter 개인정보 처리 계약(DPA)

본 Lenovo NetFilter 개인정보 처리 계약(개인정보 보호 및 보안 요건을 모두 다룸) 및 그 부속서("DPA")는 Lenovo가 제공하는 Lenovo NetFilter 서비스의 구매에 대한 Lenovo와 "고객" 간의 Lenovo 판매 계약서 또는 그 외 서면 또는 전자적 형태의 계약서("계약서")를 구성하며 여기에는 개인 데이터 처리에 관한 양 당사자의 합의 내용이 반영됩니다.

본 DPA는 여기의 주제 사안과 관련해 양 당사자 간에 체결된 계약서를 보충하며, "고객"이 "Lenovo NetFilter 서비스 약관"을 수락하는 시점("발효일")부터 효력이 발효됩니다.

본 DPA는 "계약서" 서명 및 "Lenovo NetFilter 서비스 약관" 수락과 동시에 법적 효력이 발생되며, 귀하("고객")는 Lenovo가 그 "지정 계열사"가 "컨트롤러"로서의 자격을 충족하는 "개인 데이터"를 처리하는 범위 내에서 "지정 계열사"의 이름으로 그를 대신해, 관련 교육 및 학생 개인정보 보호 및 보안 법률 및 규정을 포함한 관련 개인정보 보호, 보안 및 데이터 보호 "법률 및 규정"에서 요구하는 범위 내에서 "고객"을 대신해 본 DPA를 체결합니다. "고객"은 본 DPA가 모든 사용자에게 적용되며, 자신이 그러한 사용자를 대신해 본 DPA 체결에 필요한 권한을 보유하고 있음을 증명합니다.

당사는 새로운 법적 요건을 수용하기 위해, 또는 운영상 업데이트를 반영하는 데 필요한 데 따라 본 약관을 업데이트할 수 있습니다. 귀하가 현재 유효한 Lenovo NetFilter 구독을 보유하고 있는 경우 당사는 이메일 또는 제품 내 알림을 통해 알려드립니다.

DPA 실행:

- a) 본 DPA는 DPA 본문과 부속서 A, B, C, D 및 E 등 2개 부분으로 구성됩니다.
- b) 본 DPA는 부속서 D의 EU 표준 계약 조항(EU Standard Contractual Clauses)을 포함해, 정보수령자로서 Lenovo를 대신해 사전 서명되었습니다. (참고: 부속서 D는 일반적으로 EU(유럽연합), EEA(유럽경제지역), 영국 및/또는 그 외에 국경 간 데이터 전송과 관련해 적정성 또는 동등성이 그와 유사한 국가로부터의 개인 데이터 전송과 관련될 수 있는 처리 활동에 한해 적용됩니다).

의심의 여지 없이 확실히 하기 위해 귀하는 본 DPA 5페이지에 서명하셔야 합니다. 해당되는 경우 부속서 D가 참조로 적용됩니다.

데이터 보호

용어 정의: 이 조항에서 다음 용어들은 다음의 의미로 사용됩니다.

- a) "컨트롤러", "프로세서", "서브프로세서", "데이터 처리" 및 "처리"(및 "프로세스")는 EU 데이터 보호법 및 관련 데이터 보호법에서 그에 상응하는 용어에 대해 부여된 의미를 갖습니다.
- b) "관련 데이터 보호법"이란 개인정보 보호, 데이터 보안, 데이터 보호, 데이터 침해 및 기밀 유지와 관련한 모든 법률을 포함해 "공급자"가 NetFilter 서비스를 제공하는 모든 사법 관할권 내의 모든 관련 법률, 규칙, 규정, 명령 또는 그에 대한 모든 관련 개정 버전을 의미하며, 여기에는 2018 캘리포니아 소비자 개인정보 보호법(California Consumer Privacy Act of 2018, "CCPA")과 캘리포니아 개인정보 보호 권리법(California Privacy Rights Act, "CPRA"), EU의 일반 데이터 보호 규정(General Data Protection Regulation) 2016/279의 수시 개정, 교체 또는 대체 버전("GDPR"), 영국의 2018 데이터 보호법(Data Protection Act 2018) 개정 버전, 브라질 법률(The Law) 제13.709/18호 개정 버전("LGPD") 및 시행된(또는 시행 예정인) 규정 그리고 국가, 주 및/또는 지방 교육 및 학생 개인정보 보호 법률을 포함해 그러한 모든 관련 법률이 포함됩니다.
- c) "개인 데이터"는 학생, 부모 및 학교 직원을 한정 없이 포함해 신분 식별되었거나 식별 가능한 개인과 관련한 정보를 의미합니다.
- d) "데이터 주체"는 학생, 부모 및 학교 직원을 한정 없이 포함해 직접 또는 간접적으로 신분 식별이 가능한 개인을 의미합니다.
- e) "고객"은 "컨트롤러"를 의미합니다. 본 DPA의 목적상, "고객"이라는 용어는 "고객"과 "지정 계열사"를 포함합니다.
- f) "공급자"는 "프로세서" 역할을 하는 Lenovo를 의미합니다.
- g) "정보제공자"는 "계약"에 따라 ("컨트롤러" 자격으로) "개인 데이터"를 다른 "당사자"에게 전송하는 당사자를 의미합니다.
- h) "정보수령자"는 본 "계약"에 따라 다른 "당사자"("컨트롤러")로부터 ("프로세서" 또는 "서브프로세서" 자격으로) "고객 개인 데이터"를 받는 당사자를 의미합니다.

당사자들과의 관계: "컨트롤러"는 "공급자"가 "프로세서" 자격으로 "Lenovo 판매 계약서", "Lenovo NetFilter 서비스 약관" 및 "공급자"와 체결한 EULA의 적용 대상인 "개인 데이터"를 처리함을 인정합니다. 각 당사자는 "관련 데이터 보호법"에 따라 자신에게 적용되는 의무 사항을 준수해야 합니다.

목적 제한: "공급자"는 "프로세서" 자격으로, "관련 데이터 보호법"에서 달리 정하는 경우를 제외하고 부속서 A "처리 세부정보"에 문서화되어 있는 바와 같이 "컨트롤러"의 문서화된 지시 사항("허용된 목적")에 따라 "개인 데이터"를 처리합니다. "공급자"는 "컨트롤러"의 "처리" 지시 사항이 "관련 데이터 보호법"을 침해한다는 사실을 인지하는 경우 즉시 "컨트롤러"에게 알려야

합니다. "공급자"는 마케팅 목적을 포함해 어떠한 경우에도 자체 목적 또는 일체 제3자의 목적을 위해 "개인 데이터"를 처리해서는 안 됩니다. "공급자"는 오해의 여지를 피하기 위해 **Lenovo NetFilter**를 사용하여 얻은 개인 데이터를 활용하여 **Lenovo NetFilter** 사용자에게 마케팅 또는 기타 홍보 통신을 보내지 않습니다. 이는 **Stoneware** 또는 **Lenovo** 웹사이트와 같은 표준 채널 및 기타 판매 관련 채널의 맥락에서 발생하는 마케팅 또는 홍보 통신의 수신을 막지는 않습니다.

해외 전송: "공급자"는 "관련 데이터 보호법"에 따라 "개인 데이터"가 수집된 국가가 아닌 외국으로 "개인 데이터"를 전송할 수 있습니다. 의심의 여지 없이 명확히 하자면:

- a) 다음 조건을 충족하는 경우 유럽경제지역("EEA") 및 영국 밖으로의 "개인 데이터" 전송이 허용됩니다. (i) 해당 "개인 데이터" 전송의 수신인이 유럽집행위원회(European Commission), 영국 국무장관(Secretary of State) 및/또는 영국 개인정보감독기구(Information Commissioner's Office, ICO)가 "개인 데이터"에 대해 적절한 보호를 제공한다고 판단한 국가에 있는 경우, 그리고 (ii) 유럽집행위원회, 영국 국무장관 및/또는 영국 ICO가 채택하거나 승인한 표준 계약 조항을 이행한 수신인에게 전송하는 경우.

다음 조건을 충족하는 경우, "공급자"는 브라질 외부로 "개인 데이터"를 전송할 수 있습니다. (i) 해당 "개인 데이터"가 "국가 당국 기관"이 "개인 데이터"에 대해 적절한 보호를 제공한다고 판단한 국가에 있는 수신인에게 전송되는 경우, (ii) "국가 당국 기관"이 채택하거나 승인한 표준 계약 조항을 이행한 수신인에게 전송되는 경우 또는 (iii) 수신인이 브라질의 "데이터 보호법"에 따른 그 외 안전 장치를 제공하며, 그 시행 사실을 입증할 수 있고, 해당 해외 전송이 "컨트롤러"의 승인을 받는 경우.

- b) 일반적으로, 본 DPA를 수락하는 경우 고객은 **Lenovo, Inc.**가 **Lenovo**가 관련 "데이터 보호법"을 모두 준수하는 범위 내에서 국경 간 "개인 데이터"를 전송할 수 있다고 승인하게 됩니다. 이와 관련해 부속서 D "해외 데이터 전송"은 해당되는 경우 "컨트롤러"와 "공급자" 간에 적용됩니다.

처리의 기밀 유지: "공급자"는 "공급자"가 "개인 데이터"를 처리하도록 허가하는 자("공급자"의 직원, 대리인 및 하청업자 포함)("허가 받은 자")에 대해 (계약에 따른 의무 또는 법적 의무에 관계 없이) 엄격한 기밀 유지 의무 요건이 적용되도록 해야 하며, 그러한 기밀 유지 의무를 적용 받지 않는 자에 대해서는 일체 "개인 데이터" 처리를 허가해서는 안 됩니다. "공급자"는 모든 "허가 받은 자"는 "허용된 목적"을 위해 필요한 경우에 한해 "개인 데이터"를 처리하도록 해야 합니다. 나아가, "공급자"는 "개인 데이터"를 상업적으로 이용해서는 안 됩니다.

보안: "프로세서"는 (i) 우발적이거나 불법적인 파기, 그리고 (ii) "개인 데이터"의 손실, 변경, 무단 제공 또는 접근("보안 인시던트")으로부터 "개인 데이터"를 보호하기 위해 적절한 기술적 및 조직적 조치를 시행해야 합니다. 부속서 C에는 **Lenovo NetFilter** 기술적 및 조직적 조치(TOM)가 나와 있습니다.

하위 처리: "공급자"는 자신이 지명하는 모든 제3자 서브프로세서에는 본 "계약서"에서 정하는 것과 동일한 데이터 보호 기준이 적용되며, "공급자"는 본 DPA에서 정하는 요건의 적절한

효과가 발효되도록 관련 서브프로세서와 그에 따른 계약을 체결하는 데 동의합니다. "컨트롤러"는 "공급자"가 부속서 B에 열거되어 있는 서브프로세서 중 누구라도 이용할 수 있다는 데 동의합니다. 그럼에도 불구하고, "컨트롤러"는 "공급자"가 신규 서브프로세서에게 "개인 데이터" 처리를 의뢰하는 데(기존 서브프로세서를 대체하는 경우 포함) 동의합니다. 단, **다음의 조건이 충족되어야 합니다.** (i) "공급자"는 서브프로세서의 추가 또는 대체에 대해 업무일 기준으로 최소 30일 전에 통지(해당 서브프로세서가 수행하거나 수행할 처리에 대한 세부정보 포함)하며, 이는 그러한 추가 또는 대체에 대한 세부정보를 "컨트롤러"에게 제공하는 방법으로 이루어질 수 있습니다. (ii) "공급자"는 자신이 지명하는 모든 서브프로세서에 대해 본 DPA에서 정하는 것과 동일한 기준에 따라 "개인 데이터"를 보호하는 데이터 보호 약관을 부과합니다. "컨트롤러"가 "공급자"의 신규 제3자 서브프로세서의 지명에 동의하기를 거부하는 경우(동의는 부당하게 보류해서는 안 됩니다) "컨트롤러"가 그러한 변경에 대해 실질적이고 문서화된 거부 사유가 있다는 전제 하에, "공급자"가 해당 서브프로세서를 지명하지 않거나 "컨트롤러"가 "계약" 해지를 선택할 수 있습니다.

협조 및 "데이터 주체"의 권리: "공급자"는 "컨트롤러"가 다음에 대응할 수 있도록 "컨트롤러"에게 합리적이고 적시성 있는 지원을 제공해야 합니다. (i) "관련 데이터 보호법"에 따른 자신의 권리 행사에 대한 "데이터 주체"로부터의 요청(해당되는 바에 따라 "개인 데이터"에 대한 접근, 그 시정, 반대, 삭제 및 "개인 데이터" 이동성에 대한 권리 포함). (ii) "데이터 주체", 규제 당국 또는 기타 제3자로부터의 "개인 데이터"의 "처리"와 관련한 모든 다른 연락, 문의 또는 불만 사항. 오해의 여지 없이 명확히 하자면, "데이터 주체 요청"(Data Subject Request, DSR)은 [Stoneware DSR 개인정보 보호 웹 양식](#)에서 "컨트롤러"가 정식 요청서를 제출해 요청해야 합니다.

보안 인시던트: "공급자"는 "보안 인시던트"에 대해 인지하게 되는 즉시, 과도한 지연 없이 "컨트롤러"에게 그 사실을 알리고 "관련 데이터 보호법"에 따른 (그리고 해당 법에서 정하는 시간에 따른) "개인 데이터" 침해 보고 의무를 이행하기 위해 "컨트롤러"가 필요로 할 수 있는 모든 정보와 협조를 적시성 있게 제공해야 합니다. "공급자"는 추가적으로 "보안 인시던트"의 영향을 바로잡거나 완화하는 데 필요한 조치 및 행동을 취하며, "보안 인시던트"와 관련한 모든 진행 상황에 대해 계속해서 "컨트롤러"에게 알려야 합니다.

데이터의 삭제 또는 반환: "공급자"는 "Lenovo 판매 계약서"의 해지 또는 만료 즉시 "컨트롤러"의 요청에 따라 보유 또는 관리("처리"를 위해 제3자에게 하청 의뢰한 모든 "개인 데이터" 포함)하고 있던 모든 "개인 데이터"("개인 데이터"의 모든 사본 포함)를 파기 또는 반환해야 합니다. "컨트롤러"가 "공급자"에게 추가적인 지시를 하지 않는 경우 부속서 A에서 명시하는 바와 같이 "공급자"의 데이터 보관 일정이 적용됩니다. 이 요건은 "공급자"가 일체의 관련 "데이터 보호법"에 따라 "개인 데이터"의 일부 또는 전체를 보관해야 할 의무가 있는 경우에는 적용되지 않으며, 이 경우 "공급자"는 그러한 법에서 요구하는 경우를 제외하고 해당 "개인 데이터"를 분리해 일체의 추가적인 "처리"가 진행되지 않도록 보호해야 합니다.

감사: 본 "계약" 기간 중, 그리고 해지 또는 만료일로부터 3년간, "공급자"는 자체적으로 경비를 부담해 "컨트롤러"(또는 그 제3자 감사자)가 "공급자"의 준수 여부에 대한 감사를 실시하도록 허용해야 하며, "컨트롤러"(또는 그 제3자 감사자)가 그러한 감사를 수행하는 데 필요한 정보를 제공해야 합니다. 단, 그러한 감사 요청은 그 범위가 합당해야 하며 "컨트롤러"는 감사 의도에

대해 합당한 시점에 사전 고지해야 합니다. "컨트롤러"는 관할 데이터 보호 당국 기관의 지시에 따라 수행해야 하는 경우를 제외하고, 감사 권리를 달력월 기준 십이(12) 개월 기간 중 1회에 한해 행사해야 합니다.

이에 대한 증거로, Lenovo와 "고객"은 위에서 정한 날짜에 본 "계약"을 체결하였습니다.

Digital Signer:Kimberly		
Lenovo	Page	고객
서명: _____	Date:3/16/2023 16:11:34	서명: _____
이름: Kimberly Page	-04:00	이름: _____
직책: Strategic Operations Manager		직책: _____

부속서 A – 처리 세부정보

데이터 및 데이터 주체의 유형	보관 기간	성격, 목적 및 주제 사안
학생 인터페이스 관련 데이터: • 학생의 이름 • 학생의 성 • 학생의 이메일 주소 • IP 주소 • 방문 기록 및 키워드 검색 기록	사용자 삭제 요청 시 또는 유효한 라이선스 또는 시험 사용 버전을 보유하고 있지 않은 지 1년 경과 시점에 데이터는 아카이브 보관됩니다. 아카이브 보관된 데이터는 90일 후 삭제됩니다.	<i>데이터 액세스</i> (검색, 복사, 열람, 수정, 이동, 스캔 또는 기타 방법으로 "고객 데이터"에 액세스)
학교 직원 인터페이스 관련 데이터: • 직원의 이름 • 직원의 성 • 직원의 이메일 주소 • IP 주소 • 방문 기록 및 키워드 검색 기록	사용자 삭제 요청 시 또는 유효한 라이선스 또는 시험 사용 버전을 보유하고 있지 않은 지 1년 경과 시점에 데이터는 아카이브 보관됩니다. 아카이브 보관된 데이터는 90일 후 삭제됩니다.	<i>데이터 액세스</i> (검색, 복사, 열람, 수정, 이동, 스캔 또는 기타 방법으로 "고객 데이터"에 액세스)
클라이언트 인터페이스 관련 데이터: • 호스트 이름 • 사용자 이름 • IP 주소 • 웹 기록 검색 • 키워드 검색 • 웹 앱 사용 • 브라우저 • 장치 유형 • NetFilter 앱 사용 • 브라우저 데이터	사용자 삭제 요청 시 또는 유효한 라이선스 또는 시험 사용 버전을 보유하고 있지 않은 지 1년 경과 시점에 데이터는 아카이브 보관됩니다. 아카이브 보관된 데이터는 90일 후 삭제됩니다.	<i>데이터 액세스</i> (검색, 복사, 열람, 수정, 이동, 스캔 또는 기타 방법으로 "고객 데이터"에 액세스)
조직 관련 데이터 • 조직의 명칭 • 조직 도메인	사용자 삭제 요청 시 또는 유효한 라이선스 또는 시험 사용 버전을	<i>데이터 저장</i> (기록, 호스트, 로그 작성, 아카이브 또는 기타

	보유하고 있지 않은 지 1년 경과 시점에 데이터는 아카이브 보관됩니다. 아카이브 보관된 데이터는 90일 후 삭제됩니다.	방법으로 "고객 데이터"를 저장), <i>데이터 액세스</i>(검색, 복사, 열람, 수정, 이동, 스캔 또는 기타 방법으로 "고객 데이터"에 액세스), <i>데이터 분석</i>(설문조사, 테스트, 연구, 해석, 정리, 보고 또는 기타 방법으로 "고객 데이터"를 분석).
사용자 데이터 • 사용자의 이름 • 사용자의 성 • 사용자의 이메일 주소 • IP 주소 • 시스템 • 액세스/사용/허가 데이터 상자 • 데이터의 민감한/특수 범주: 데이터 로그, 웹 방문 기록, 기계 호스트 이름, 키워드 검색 기록	사용자 삭제 요청 시 또는 유효한 라이선스 또는 시험 사용 버전을 보유하고 있지 않은 지 1년 경과 시점에 데이터는 아카이브 보관됩니다. 아카이브 보관된 데이터는 90일 후 삭제됩니다.	<i>데이터 액세스</i>(검색, 복사, 열람, 수정, 이동, 스캔 또는 기타 방법으로 "고객 데이터"에 액세스)
라이선스 데이터(개인 데이터 제외)	이 데이터는 법적 의무를 준수하거나 당사 계약을 집행하는 등의 목적으로 필요한 기간 동안 계속 보관합니다. 여기에 개인 데이터는 포함되지 않습니다.	<i>데이터 저장</i>(기록, 호스트, 로그 작성, 아카이브 또는 기타 방법으로 "고객 데이터"를 저장), <i>데이터 액세스</i>(검색, 복사, 열람, 수정, 이동, 스캔 또는 기타 방법으로 "고객 데이터"에 액세스), <i>데이터 분석</i>(설문조사, 테스트, 연구, 해석, 정리, 보고 또는 기타 방법으로 "고객 데이터"를 분석).

처리 기간

처리 기간은 "계약" 기간과 일치합니다. 위와 같은 데이터 보관 정책이 적용됩니다.

데이터 주체의 범주

학생, 교사, 조직 연락처 및 일반 사용자

부속서 B - 서브프로세서

이름	데이터	저장 위치	목적
Amazon Web Services(AWS)	부속서 A의 설명에 따른 모든 사용자 데이터	미국, EU	애플리케이션 인프라에 대한 클라우드 서비스 공급자. 모든 데이터는 애플리케이션이 처리합니다.
UDS Web Interface	신분 관리 데이터	미국, EU	신분 관리 및 인증 허가.

부속서 C- 기술적 및 조직적 조치(TOM)

"공급자"는 "개인 데이터"의 보호 및 책임감 있는 사용에 대해 널리 사용되고 있는 업계 기준을 반영하는 물리적, 기술적, 절차적 및 관리적 통제 장치가 포함된 종합적인 서면 보안 프로그램을 실시했으며, 여기에는 다음과 같은 통제 장치가 포함되나 여기에 국한되지 않습니다.

기술적	범위	통제 장치
액세스	로그인 (시스템 및 애플리케이션).	NIST 기반 암호 정책 (관리자 레벨 액세스 및 인터페이스에 대한 다중 인증).
암호화	정지 상태 및 전송 중 데이터 저장.	AES 256-GCM(정지), TLS 1.2(전송 중) ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 (서버 선호 암호화 스위트).
정적 애플리케이션 보안 테스트	전체 서버 및 마이크로 서비스 이미지, 전체 바이너리 클라이언트 및 확장 프로그램/플러그인.	정기적 취약성 스캔 및 모니터링.
동적 애플리케이션 보안 테스트	외부 애플리케이션 API.	웹 애플리케이션 스캔, 침투 테스트 (SSRB가 정하는 일정에 따라 수시로 실시).
CIS 벤치마크 하드닝	클라우드 플랫폼 공급자, 서버 인스턴스.	클라우드 CIS 준수 점검, 클라우드 보안 모니터링, 정기 CIS L2 서버 벤치마크 평가.
소프트웨어 구성 분석	제3자 오픈소스 의존성.	정기적 취약성 감사, 리포지터리 모니터링 실시.
인프라 평가	클라우드 플랫폼 공급자.	전체 소프트웨어 정의 네트워크(SDN)에 대한 정기적 검토 (네트워크 분할, 방화벽 구성 및 잘못된 리소스 액세스 구성을 파악).
WAF(Web Application Firewall)	프로덕션 웹 애플리케이션.	WAF 보호 (흔히 발생하는 공격에 대한 코어 규칙).
Netsweeper 소유의 정적 코드 분석	독점 소유 코드.	상용 도구를 사용해 정기적으로 코드 분석 실시, 각 코드 릴리스별로 실시.
로그 수집	클라우드 플랫폼 공급자, 애플리케이션.	클라우드 플랫폼 API 트랜잭션(1년 이상 지난 로그는 삭제되고, Datadog를 통해 액세스 가능하며, 내부 사용자가 Lenovo Active Directory Integration for SAML 2.0 auth를 통해 사용할 수 있음), 에지 감지를 위한 WAF 로깅(로그는 인스턴스 내에만

		존재하며, 엔지니어링 팀에서 액세스 가능), 애플리케이션 목적을 위한 서버프로세서에 대해서는 부속서 B를 참고합니다.
laC(Infrastructure as Code)	클라우드 플랫폼 공급자.	laC(Infrastructure as Code)는 인프라 배포를 자동화하고 인프라의 불변성과 잘못된 구성을 개선하는 용도로 사용됩니다.

조직적	범위	통제 장치
인시던트(데이터 침해 포함) 대응	프로덕션 단계의 제품과 관련한 보안 이벤트.	NIST 800-61 및 Lenovo의 사내 PSIRT(Product Security Incident Response Team, 제품보안 인시던트대응팀) 프로세스에 따른 제품 인시던트 대응 계획.
신뢰하는 공급자 명단	프로덕션 단계에서 제품과 직접 통합되는 모든 서버프로세서.	통합 공급자에 대한 표준 보안 평가, "개인 데이터" 처리 공급자에 대한 DPA.
취약성 관리	서버 OS, 도커 컨테이너, 클라이언트, 프로덕션 단계의 제품.	전체 컴퓨팅 시스템에 걸쳐 취약성 파악을 돕는 다양한 도구를 적용하는 프로그램.
SSRB(Software Security Review Board) 및 CSRB(Cloud Security Review Board)	프로덕션 단계의 제품.	SSRB 검토는 모든 릴리스 과정에서 실시합니다. CSRB 검토는 모든 아키텍처 변경 과정에서 실시합니다. 검토 과정에서는 대상 제품에 대해 모든 기술적 및 조직적 조치를 평가합니다.
데이터 보관 정책	개인 식별 정보, 애플리케이션 데이터, 프로덕션 단계의 제품.	사용자의 삭제 요청 시, 또는 유효한 라이선스 또는 시험 사용 버전을 보유하고 있지 않은 지 1년 경과 시점, 또는 데이터가 더 이상 필요하지 않게 된 경우 일체의 임의 기간 후, 그리고 보안 영향이 전혀 없는 데이터인 경우.
보안 및 개인정보 보호에 대한 인식	전체 직원(개인정보 보안 기초 및 보안 필수 요소 과정)	OWASP Top 10 등 고급 보안 주제에 대한 전문 IT 및 제품 팀 대상 정기 교육.
지속적인 보안	프로덕션 단계의 제품.	기술적 조치의 정기적 적용.
오픈소스 준수 검토	프로덕션 단계의 제품.	적절한 라이선스 취득 및 유지를 보장하기 위해 평가를

		실시하고 배포된 소프트웨어에서 저작자 표시를 제공합니다.
재난 복구	프로덕션 단계의 제품	NIST-800-34를 가이드로 사용해 RTO 및 RPO를 최대화합니다.
백업 정책	데이터베이스, 코드, 로그.	데이터베이스 백업/복구의 경우 암호화 백업(정지 상태에서 암호화)을 사용합니다. 이 방식은 여러 가용 영역에서 가용성이 높으며 30분 이내에 복구 가능합니다. 이전 7일간의 백업이 보관 및 회전됩니다. 실행하는 경우 수동 스냅샷은 무제한 보관 가능합니다(1년 이상). 크론 작업을 실행해 데이터베이스를 암호화 및 백업하고 회전 방식으로 7일간 보관하는 추가 자동화(UDS) 솔루션도 사용할 수 있습니다. 'IaC(Infrastructure as Code)'(및 DB 생성)를 포함하는 애플리케이션 소스 코드는 무한정 백업되는 UDS 엔터프라이즈 버전에 있습니다. 프로덕션 로그는 DataDog에서 30일간 이용 가능합니다. UDS는 아직 콜드 아카이브에서 이러한 로그를 12개월로 연장하는 과정에 있습니다.

부속서 D – 해외 데이터 전송 동의서

본 부속서에서는 다음에 적용되는 데이터 보호 요건("관련 개인정보 보호법"에 따른 요건 포함)을 정합니다. (i) "정보제공자"("컨트롤러")가 "개인 데이터"를 "데이터 처리" 목적으로 "정보수령자(Lenovo), 그 계열사 및/또는 그 "서브프로세서"에게 전송할 때, 그리고 (ii) "정보수령자"가 "데이터 처리" 목적으로 "정보제공자"로부터 "개인 데이터"를 받을 때.

"정보수령자"는 다음 사항을 항상 보증하고 약속합니다.

- a) "관련 개인정보 보호법"에 따라 "전송된 데이터"를 처리하고 "정보제공자"가 "관련 개인정보 보호법"에 따른 의무 사항을 준수할 수 있도록 돕는 데 필요한 바에 따라 "정보제공자"에게 합당한 지원을 적시성 있게 제공합니다.
- b) 본 "계약"에 따른 의무 사항을 수행할 때 의도적으로 "정보제공자"가 "관련 개인정보 보호법"에 따른 그 의무 사항을 위반하게 만드는 방식으로 수행하지 않습니다.

1. EEA(유럽경제지역)

"공급자"의 서비스가 유럽경제지역("EEA") 또는 EU "데이터 보호법"의 적용 대상인 그 외 사법 관할권 내에서 "컨트롤러"에게 제공되는 경우 다음 조항이 적용됩니다.

(A) "EU 데이터 보호법"은 (a) "개인 데이터"의 "처리"와 관련한 자연인의 보호와 그러한 데이터의 자유로운 이동에 관한 유럽 의회 및 이사회의 Regulation 2016/679(일반 데이터 보호 규정)("GDPR"), (b) EU e-Privacy Directive(Directive 2002/58/EC) 및 (c) 모든 관련 국가 데이터 보호 법률을 의미합니다.

(B) "공급자"는 (a) "컨트롤러"의 지시 사항과는 다른 방식으로 "개인 데이터"의 "처리"를 요구하는 EU 데이터 보호법에 따른 요건, 또는 (b) "공급자"가 볼 때 "컨트롤러"의 지시 사항이 관련 EU 데이터 보호법을 침해 또는 위반할 수 있을 것으로 판단되는 경우 지체 없이 "컨트롤러"에게 그 사실을 알려야 합니다.

(C) **데이터 전송:** "공급자" 또는 그 "하청업체"의 소재지가 EEA 외부인 경우, "공급자"와 "컨트롤러"는 이로써 [유럽 의회 및 이사회의 Regulation \(EU\) 2016/679에 따른 개인 데이터의 제3국 전송 관련 표준 계약 조항에 대한 2021년 6월 4일자 Commission Implementing Decision \(EU\) 2021/914](#)의 MODULE TWO에서 정하고 있는 컨트롤러-프로세서 표준 계약 조항을 수시로 개정 또는 대체되는 바에 따라("C2P 표준 계약 조항") 집행하며, 이로써 본 부속서에 참조로 포함합니다. 양 당사자는 다음을 인정하고 동의합니다.

- a. "공급자"와 "컨트롤러"는 "C2P 표준 계약 조항"에 따른 각자의 의무 사항을 준수합니다.
- b. "C2P 표준 계약 조항"과 본 부속서 또는 기초 계약 간에 상충되거나 불일치하는 사항이 있는 경우 그러한 상충 범위 내에서 "C2P 표준 계약 조항"이 우선합니다. 그리고
- c. 아래 표의 내용을 이로써 양 당사자 간 "C2P 표준 계약 조항"에 포함시킵니다.

"컨트롤러"와 "공급자" 간 "C2P 표준 계약 조항"에 포함시킬 내용:

조항 9. 서브프로세서의 이용	옵션 2 "일반 서면 허가"를 선택합니다. 정보수령자는 "하위 처리" 조항에 따라 최소 30일 전에 정보를 제공해야 합니다.
조항 17. 준거법	이 "조항"들은 양 당사자의 기초 계약에서 정하는 준거법에 따라 해석하되, 단, 준거법이 제3자 수혜자 권리를 허용하는 EU 회원국의 것이 아닌 경우는 예외로 합니다. 이 경우 양 당사자는 이러한 "조항"을 아일랜드 법률에 따라 해석하는 데 동의합니다.
조항 18 (b). 재판 장소 및 사법 관할권의 선택	양 당사자는 이러한 "조항"에서 분쟁이 발생하는 경우 이를 아일랜드 법원에서 해결하는 데 동의합니다.

"C2P 표준 계약 조항"의 부속서 1, 제A부에 포함시킬 내용:

"정보제공자"의 이름	"컨트롤러", 그리고 그 공동 소유 또는 지배 대상 계열사
"정보제공자"의 주소	정보제공자가 작성
"정보제공자"의 연락 담당자 이름, 직책 및 연락처 정보	정보제공자가 작성
이 "조항"에 따라 전송되는 데이터와 관련한 "정보제공자"의 활동	정보제공자가 작성
"정보제공자"의 서명 및 날짜	정보제공자가 작성
"정보제공자"의 역할	"컨트롤러"
"정보수령자"의 이름	"공급자"(Lenovo) 및 그 "하청업체"
"정보수령자"의 주소	3400 E Coliseum Blvd, #310, Fort Wayne, IN 46805 United States of America
"정보수령자"의 연락 담당자 이름, 직책 및 연락처 정보	Kimberly Page, Strategic Operations Manager privacy@lanschool.com
이 "조항"에 따라 전송되는 데이터와 관련한 "정보수령자"의 활동	부속서 1의 제B부에서 정하는 바에 따라
"정보수령자"의 서명 및 날짜	정보수령자가 작성
"정보수령자"의 역할	"프로세서"

"C2P 표준 계약 조항"의 부속서 1, 제B부 및 제C부에 포함시킬 내용:

데이터 주체의 범주	위 부속서 A에서 정하는 바에 따라
개인 데이터의 범주	위 부속서 A에서 정하는 바에 따라
민감한 데이터	위 부속서 A에서 정하는 바에 따라
전송의 빈도	LSA 라이선스가 유효한 기간 중 지속적인 빈도
처리의 성격	위 부속서 A에서 정하는 바에 따라
처리의 목적	위 부속서 A에서 정하는 바에 따라
개인 데이터를 보관하는 기간	위 부속서 A에서 정하는 바에 따라
서브프로세서가 수행하는 처리의 주제 사안, 성격 및 지속 기간	위 부속서 B에서 정하는 바에 따라
"정보제공자"의 Regulation (EU) 2016/679 ty 준수를 보장하는 책임을 맡고 있는 "관할 감독 당국 기관"	관할 감독 당국 기관 역할을 할 감독 당국 기관은 EU 내에 "정보제공자"가 설립된 EU 회원국의 당국 기관이 됩니다. "정보제공자"(즉, 계약을 체결한 법인체)가 EU 내에서 설립되지 않은 경우, "관할 감독 당국 기관"은 Regulation (EU) 2016/679 Article 27(1)의 의미 내에서 "정보제공자"의 EU 사무소가 설립된 EU 회원국의 당국 기관이 됩니다. "정보제공자"가 EU 내에서 설립되지 않았지만 EU 사무소를 지명할 필요가 없는 경우, "관할 감독 당국 기관"은 상품 또는 서비스 제공과 관련해 이 "조항들"에 따라 개인 데이터가 전송되거나 그 행동이 모니터링 대상인 데이터 주체가 위치해 있는 EU 회원국의 당국 기관이 됩니다.

"C2P 표준 계약 조항"의 부속서 2에 포함시킬 내용:

처리의 성격, 범위, 맥락 및 목적 그리고 자연인의 권리 및 자유에 부과되는 위험을 감안해 적절한 수준의 보안을 보장하기 위해 정보수령자(들)이(관련 인증을 포함해) 실시하는 기술적 및 조직적 조치에 대한 설명.	위 부속서 C에서 정하는 바에 따라
---	---------------------

"C2P 표준 계약 조항"의 부속서 3에 포함시킬 내용:

허가 받은 서브프로세서 명단	위 부속서 B에서 정하는 바에 따라
-----------------	---------------------

2. 영국

"공급자"의 서비스가 영국 내에 있는 "컨트롤러"에게 제공되거나, "개인 데이터"의 성격에 따라 2018년 EU (탈퇴)법(EU (Withdrawal) Act 2018)("영국 GDPR") 및 2018 데이터 보호법(Data Protection Act 2018)("DPA 2018")의 적용이 촉발되는 경우 다음과 같은 조항이 추가 적용됩니다.

- (A) 영국의 국무장관이 "개인 데이터"에 대해 적절한 보호를 하는 것으로 간주("적합성 결정")하는 국가에 있는 수신인에게 "개인 데이터"를 전송하는 것은 승인을 받은 영국 "표준 계약 조항"의 필요 없이 본 "계약(들)"에 따라 허용됩니다.
- (B) EEA 국가들은 영국에서 EEA로의 "개인 데이터" 전송 목적상 "적합성 결정" 대상으로 간주됩니다.
- (C) "적합성 결정" 부재 시, "컨트롤러"와 "공급자"는 유럽위원회의 국제 데이터 전송에 대한 표준 계약 조항에 승인된 영국 국제 데이터 전송 부속서를 이행하기로 합의합니다(<https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>).

제1부: 표 / 표 1: 당사자

유럽집행위원회 표준 계약 조항에 대한 국제 데이터 전송 부속서의 "제1부: 표"에 통합될 정보:		
시작일	상기한 바와 같이	
당사자들	제공자(제한된 전송을 보내는 자)	수령자(제한된 전송을 받는 자)
당사자 세부 정보	전체 법적 이름, 기본 주소(회사에서 주소를 등록한 경우): 본 조항 제2 표의 정보에 따름. 1. 부속서 D의 EEA(유럽경제지역) 공식등록번호(있는 경우) (기업 번호 또는 유사한 식별자): 판매 계약에 따라 식별된 고객에 따라	전체 법적 이름, 기본 주소(회사에서 주소를 등록한 경우): 본 조항 제2 표의 정보에 따름. 1. 부속서 D의 EEA(유럽경제지역) 공식등록번호(있는 경우) (기업 번호 또는 유사한 식별자): 35-2097171 인디애나 주 등록
주요 연락처	성명(선택 사항), 직함, 이메일을 포함한 연락처 세부 정보: 본 조항 제2 표의 정보에 따름. 1. 부속서 D의 EEA(유럽경제지역)	성명(선택 사항), 직함, 이메일을 포함한 연락처 세부 정보: 본 조항 제2 표의 정보에 따름. 1. 부속서 D의 EEA(유럽경제지역)

표 2: 선택된 SCC, 모듈 및 선택된 조항

부속서 유럽 SCC	위의 부속서 D, 조항 1을 참조하십시오.
------------	-------------------------

표 3: 부록 정보

부속서 1A: 조항에 명시된 당사자의 목록. 1. 부속서 D의 EEA(유럽경제지역)
부속서 1B: 전송 설명: 위의 부속서 A에 명시된 바와 같이
부속서 II: 데이터의 보안을 보장하기 위한 기술적 및 조직적 조치를 포함한 기술적 및 조직적 조치: 전송 설명: 위의 부속서 C에 명시된 바와 같이
부속서 III: 서브프로세서 목록(모듈 2 및 3에만 해당): 전송 설명: 위의 부속서 B에 명시된 바와 같이

표 4: 승인된 부속서 변경 시 이 부속서는 종료됨

승인된 부속서 변경 시 이 부속서는 종료됨	19조에 명시된 대로 본 부속서를 종료할 수 있는 당사자: ☒ 수령자 ☐ 제공자 ☐ 어떤 당사자도 할 수 없음
-------------------------	--

유럽집행위원회 표준 계약 조항에 대한 국제 데이터 전송 부속서의 "제2부: 필수 조항"에 통합될 정보:

제2부: 승인된 부속서의 필수 조항은 ICO가 발행하고 2018 데이터 보호법 s119A에 따라 2022년 2월 2일에 의회에 제출한 부록 B.1.0 템플릿으로, 해당 필수 조항의 18조에 따라 개정되었습니다.

3. 스위스

스위스의 관련 당국 기관이 "스위스 모델 조항"을 발표할 때까지는 상기 섹션 1 "EEA(유럽경제지역)"에 따라 집행된 "C2P 모델 조항"이 참조로 적용됩니다. 유럽집행위원회 또는 스위스 정부가 "스위스-미국 개인정보 보호 실드(Swiss-US Privacy Shield)"에 대한 승계 솔루션에 동의하는 경우, 상기 섹션 2 "영국"에 따른 조항이 참조로 적용됩니다.

4. 브라질

브라질의 관련 당국 기관이 상응하는 "브라질 모델 조항"을 발표할 때까지는 상기 섹션 1 "EEA(유럽경제지역)"에 따라 집행된 "C2P 모델 조항"이 참조로 적용됩니다.

5. 남아프리카 공화국

"공급자"의 서비스가 남아프리카 공화국 또는 POPIA(개인정보 보호법)의 적용 대상인 그 외 사법 관할권 내에서 "컨트롤러"에게 제공되는 경우 다음 조항이 추가 적용됩니다.

- (A) "데이터 주체"란 이름, 고유한 숫자, 위치 데이터, 온라인 식별자, 또는 해당 자연인의 신체적, 심리학적, 유전적, 정신적, 경제적, 문화적 또는 사회적 신분에 특정적인 하나 이상의 요인으로 식별 가능한 자연인, 그리고 식별 가능한 법인 또는 법인체를 의미합니다.

부속서 E – 추가 조항

1. 캘리포니아 소비자 개인정보 보호법(California Consumer Privacy Act, "CCPA").

Lenovo는 사업체입니다. 또한, "공급자"는 "고객"의 "서비스 공급자"로 "고객"을 대신해 "개인 데이터"를 처리합니다.

- a. "공급자"는 "개인 데이터" 또는 "독점 소유 정보"를 판매해서는 안 됩니다. "판매"란 금전적 대가 또는 그 외 값비싼 대가를 받고 정보를 판매, 대여, 공개, 유포, 가용화, 양도, 또는 그 외 방법으로 전달하는 것을 의미합니다.
- b. "공급자"는 (a) Lenovo를 위한 "계약"에 명시되어 있거나 CCPA 및 그 시행 규정에서 달리 허용되는 바에 따라 서비스를 수행하는 구체적인 목적이 아닌 일체 다른 목적으로, (b) 해당 기업과의 계약에 명시되어 있는 서비스를 제공하는 목적 외에 다른 상업적 목적으로, 또는 (c) 해당 자와 Lenovo 간의 직접적인 사업거래 관계를 벗어나 "개인 데이터"를 보관, 사용 또는 공개해서는 안 됩니다.
- c. 이 DPA는 "공급자"가 캘리포니아의 제한을 포함하여 사업 및 서비스 제공자에 적용되는 CCPA 요건을 이해하고 있음을 인증하는 역할을 합니다. Civ. Code § 1798.140(w)(2)(A)의 제한 사항을 포함해 기업 및 서비스 공급자들에게 적용되는 CCPA 요건을 이해하고 있으며 그러한 요건을 준수할 것임을 증명하는 역할을 합니다.