Dell Technologies 데이터 처리 명세서

1. 범위.

본 Dell Technologies 데이터 처리 명세서(이하 "명세서")는 공급업체 오퍼링의 제공에 대한 귀하(이하 "고객")와 Dell Technologies(이하 "Dell Technologies" 또는 "공급업체") 간에 체결된 계약을 보완하며, 공급업체가 해당 계약에 따라 의무를 이행하기 위해 개인 데이터를 처리하는 경우에 적용됩니다.

1.1. 충돌. 본 계약과 상반되는 조항에도 불구하고, 개인 데이터 처리와 관련하여 본 계약과 본 명세서의 내용이 상충하거나 불일치하는 경우 본 명세서가 우선 적용됩니다.

1.2. 고객의 역할. 고객은 본 명세서에 따라 개인 데이터의 "통제권자"로 간주됩니다. 단, 고객이 "처리자"인 경우는 제외하며, 이 경우 Dell Technologies가 하위 처리자입니다.

1.3 부록. 다음 부록(부록 I: 처리에 대한 설명, 부록 II: 기술적 및 조직적 보안 조치 및 부록 III: 데이터 전송 조건)은 본 명세서에 통합됩니다.

2. 정의.

본 명세서 내 대문자로 표기된 용어의 뜻은 본 계약에서 정의하는 의미를 가집니다. 다음 용어는 아래에 명시된 의미를 가집니다.

2.1. **"통제권자"**는 단독으로 또는 타인과 공동으로 개인 데이터 처리의 목적 및 수단을 결정하는 주체를 의미합니다.

2.2. **"데이터 보호 요구 사항"**은 GDPR 및 관련 관할권에 따른 데이터 보호 및 개인 정보 보호와 관련된 모든 관련 법률, 규정 및 기타 법적 요구 사항을 의미합니다.

2.3. **"EC SCC"**는 위원회 결정 2021/914의 명세서에 명시된 규정 (EU) 제2016/679호에 따라 제3국으로 개인 데이터를 전송하기 위한 유럽연합 집행위원회의 표준 계약 조항을 의미합니다. 이는 본 명세서의 최종 업데이트 당시 유효한 이행 결정 - 2021/914 - EN - EUR-Lex(Europa.eu)에서 확인할 수 있으며 참조를 위해 여기에 통합되었습니다.

2.4. **"GDPR"**은 2016년 4월 27일에 유럽의회 및 유럽연합이사회에서 제정한 개인 데이터 처리 관련 자연인의 보호 및 정보의 자유로운 이동에 관한 규정 (EU) 제2016/679호로, 지침 제95/46/EC호(일반 정보 보호 규정)를 대체하는 규정을 의미합니다.

2.5. **"개인 데이터"**는 개인 정보, 개인 식별 정보 또는 데이터 보호 요구 사항에 정의된 유사한 용어를 의미합니다.

2.6. **"개인 데이터 침해"**는 본 명세서에 따라 처리된 개인 데이터의 우발적 또는 불법적인 파괴, 손실, 변경, 무단 공개 또는 액세스를 유발하는 보안 위반을 의미합니다.

2.7. **"처리자"**는 통제권자를 대리하여 개인 데이터를 처리하는 주체를 의미합니다.

2.8. **"하위 처리자"**는 처리자가 공급업체 오퍼링의 제공을 위해 고용한 모든 처리자를 의미합니다.

3. 당사자들의 의무.

3.1. 설명 및 지침.

A. 고객과 공급업체는 (i) 고객이 개인 데이터의 처리자이고 Dell Technologies가 하위 처리자인 경우 또는 (ii) 본 명세서에 달리 명시된 경우를 제외하고 고객이 개인 데이터의 통제권자이고 공급업체가 해당 데이터의 처리자라는 데 동의합니다. 공급업체가 개인 데이터의 처리자 또는 하위 처리자인 경우 공급업체는 고객이 제공한 문서로 된 지침에 따라서만 개인 데이터를 처리해야 합니다. 단, 처리자에게 적용되는 데이터 보호 요구 사항에서 달리 규정하는 경우는 예외로 합니다. 이 경우 처리자는 처리 전에 통제권자에게 법적 요구 사항을 통지해야 하나, 관련 법률이 공익을 위해 중요한 이유로 이를 금지하는 경우는 예외로 합니다.

B. 처리자는 통제권자가 제공한 지침이 데이터 보호 요구 사항에 위반된다고 판단하는 경우 즉시 통제권자에게 통지해야 합니다.

C. 본 명세서의 부록 I은 개인 데이터의 범주를 포함하여 처리 작업에 대한 세부 정보를 제공합니다. 통제권자를 대신하여 개인 데이터를 처리하는 목적 및 기간.

3.2. 목적 제한.

A 처리자는 통제권자로부터 추가 지침을 받는 경우를 제외하고 본 명세서와 부록 I에 명시된 구체적인 처리 목적에 따라서만 개인 데이터를 처리합니다.

B. 통제권자가 지시하거나, 본 명세서에서 명시하거나, 데이터 보호 요구 사항에서 달리 허용하는 경우를 제외하고, 처리자는 본 계약에 따라 수신된 개인 데이터를 공개하거나 그에 대한 액세스 권한을 제공하거나, 다른 사람 또는 법인으로부터 또는 이들을 대신하여 수신한 개인 데이터와 결합해서는 안 됩니다.

3.3. 처리의 보안.

A. 처리자는 개인 데이터의 보안을 보장하기 위해 최소한 부록 II에 명시된 기술적 및 조직적 조치를 이행해야 합니다. 적절한 보안 수준을 평가할 때 당사자들은 최신 기술, 실행 비용, 처리의 성격, 범위, 상황 및 목적, 데이터 주체에 수반되는 위험을 적절히 고려해야 합니다.

B. 처리자는 개인 데이터를 처리할 권한이 있는 사람이 기밀을 유지하기 위해 노력했거나 적절한 법적 기밀 유지 의무를 준수하는지 확인합니다.

3.4. 문서화 및 규정 준수. 합당한 사전 서면 요청이 있는 경우, 본 계약 및 본 명세서에 따라 처리자는 본 명세서에 명시된 의무의 준수를 입증하고 통제권자 또는 통제권자가 위임한 다른 감사자가 실시하는 조사를 포함하여 감사에 합당하게 필요한 모든 정보를 통제권자에게 제공합니다.

3.5. 하위 프로세서의 사용

A. 처리자는 합의된 목록에서 하위 처리자의 고용에 대한 통제권자의 일반 승인을 받습니다. 처리자는 하위 처리자의 추가 또는 교체를 통해 발생한 해당 목록의 의도된 변경 사항을 통제권자에 통지하여, 통제권자에게 관련 하위 처리자의 업무 개시 전에 이러한 변경 사항에 이의를 제기할 수 있는 충분한 시간을 제공합니다. 공급업체가 처리자인 경우 공급업체의 하위 처리자 목록 및 모든 업데이트는 www.dell.com/subprocessors에서 확인할 수 있습니다. 고객이 데이터 보호를 이유로 하위 처리자의 추가 또는 제거에 합법적으로 이의를 제기했고 공급업체가 고객의 이의 제기를 합리적으로 수용할 수 없는 경우, 당사자들은 문제 해결을 위해 고객의 우려 사항을 성실하게 논의해야 합니다.

B. 처리자가 (통제권자를 대신하여) 특정 처리 활동을 수행하기 위해 하위 처리자를 고용하는 경우, 처리자는 본 명세서에 따라 데이터 처리자에게 부여된 것과 동일한 데이터 보호 의무를 하위 처리자에게 실질적으로 m부여하는 계약을 체결한 뒤 그러한 활동을 수행합니다. 처리자는 하위 처리자가 본 명세서 및 데이터 보호 요구 사항에 따른 처리자의 의무를 준수하는지 확인합니다. 처리자는 하위 처리자가 위에 규정된 데이터 보호 의무를 이행하지 못한 경우, 해당 하위 처리자의 의무를 이행해야 할 책임을 고객에 대해 집니다.

3.6. 해외 전송.

A. 처리자의 제3국 또는 국외 기관으로 개인 데이터 전송은 처리자에게 적용되는 데이터 보호 요구 사항에 달리 규정되지 않는 한 본 명세서에 따라 통제권자의 문서로 된 지침에 따라서만 수행됩니다. 이러한 경우 처리자는 처리 전에 해당 법적 요구 사항을 통제권자에 알려야 하나, 해당 법률에서 공익을 위해 중요한 이유로 해당 정보를 금지하는 경우는 예외로 합니다.

B. 고객은 공급업체가 미국 또는 공급업체 또는 그 하위 처리자가 운영되는 다른 국가로 개인 데이터를 전송하고, 계약에서 공급업체 오퍼링을 제공할 수 있도록 개인 데이터를 저장 및 처리함을 허용합니다. 공급업체 오퍼링의 제공이 유럽 경제 지역("EEA"), 영국 또는 스위스에서 EEA, 영국 또는 스위스 이외의 국가로 개인 데이터의 전송을 수반하는 경우(데이터 보호 요구 사항에 따른 적정성 결정 대상이 아닐 것), 공급업체는부록 III에 명시된 해당 EC SCC 또는 관련 데이터 보호 요구 사항에 따른 다른 적정한 데이터 전송 메커니즘 및 보호 조치를 사용한다는 데 동의합니다.

3.7. 통제권자에 대한 지원.

A. 처리자는 데이터 주체로부터 받은 모든 요청을 통제권자에게 즉시 통지하고 통제권자가 처리의 성격을 고려하여 응답할 의무를 이행할 수 있도록 지원합니다. 통제권자가 승인하지 않는 한 처리자는 요청에 응답하지 않습니다.

B. 처리자는 데이터 처리의 성격과 처리자가 사용할 수 있는 정보를 고려하여 통제권자가 다음 의무를 준수하도록 합당한 지원을 제공합니다.

(1) 데이터 보호 요구 사항에 규정된 데이터 보호 영향 평가 및 관련 감독 기관과의 협의를 수행할 의무

(2) 최신 기술, 실행 비용, 처리의 성격, 범위, 상황 및 목적과 함께 자연인의 권리와 자유에 미치는 위험의 다양한 가능성 및 심각성을 고려하여, 통제권자와 처리자가 해당 위험에 대비하기에 적정한 보안 수준을 보장하기 위해 부록 II에 명시된 대로 적정한 기술적 및 조직적 조치를 이행할 의무

3.8. 개인 데이터 침해 통지. 개인 데이터 침해가 발생하는 경우 처리자는 개인 데이터 침해의 발생을 알게 되는 즉시 통제권자에게 통지합니다. 처리자는 처리의 성격과 처리자가 사용할 수 있는 정보를 고려하여 해당하는 경우 통제권자가 데이터 보호 요구 사항에 따른 의무를 준수할 수 있도록 통제권자와 협력하고 지원합니다.

3.9. 해지. 본 계약이 해지된 후 처리자는 통제권자의 서면 요청에 따라 통제권자를 대신하여 처리된 모든 개인 데이터를 삭제합니다. 단, 데이터 보호 요구 사항에 따라 개인 데이터의 보관이 필요한 경우는 예외로 합니다. 개인 데이터가 삭제될 때까지 처리자는 본 명세서의 준수를 계속 보장합니다.

3.10. 독립 통제권자 조건. 공급업체가 통제권자인 경우, 본 명세서에 명시된 조건이 통제권자인 공급업체에 적용됩니다.

A. 관련 데이터 보호 요구 사항에서 허용하는 최대 범위 내에서, 공급업체가 통제권자인 경우 공급업체와 고객은 개인 데이터의 각 독립 통제권자이며, 따라서 해당 개인 데이터의 처리 목적과 수단을 독립적으로 결정합니다.

B. 각 당사자는 관련 데이터 보호 요구 사항에 따라 개인 데이터 처리가 합법적이고 공정하며 투명하도록 보장할 개별적인 책임을 집니다.

C. 각 당사자는 (i) 우발적 또는 불법적인 파괴, (ii) 손실, 변경, 무단 공개 또는 액세스로부터 자신의 소유 또는 관리 중인 개인 데이터를 보호하기 위한 적절한 기술적 및 조직적 조치를 이행하고 유지하며, 처리로 인해 나타나는 위험과 보호할 개인 데이터의 성격에 적합한 보안 수준을 제공합니다.

부록 I: 처리에 대한 설명

1. 개인 데이터가 처리되는 데이터 주체의 범주. 고객의 최종 사용자, 직원, 계약업체, 공급업체 및 공급업체 오퍼링과 관련된 기타 제3자.

2. 처리된 개인 데이터의 범주. 고객이 제출할 수 있는 개인 데이터의 유형은 다음과 같습니다.

A. 고객 세부 정보: 이름, 주소, 이메일 주소, 전화, 팩스, 기타 연락처 세부 정보, 긴급 연락처 세부 정보, 관련 현지 시간대 정보, 인보이스 발행 및 신용 관련 데이터.

B. IT 시스템 및 운영 정보. 개인 식별자, 음성, 동영상 및 데이터 기록, 사용자 ID 및 비밀번호 세부 정보, 컴퓨터 이름, 이메일 주소, 도메인 이름, 사용자 이름, 비밀번호, IP 주소, 권한 데이터(직무 역할별), 통신 서비스를 위한 계정 및 위임 정보, 개인 사서함 및 디렉토리, 채팅 커뮤니케이션 데이터, 소프트웨어 및 하드웨어 인벤토리, 소프트웨어 및 인터넷 사용 패턴 관련 추적 정보(예: 쿠키), 운영 및/또는 교육 목적으로 기록된 정보를 포함할 수 있습니다.

C. 데이터 주체의 이메일 내용 및 트래픽/전송 데이터, 온라인 대화 및 음성 통신(예: 블로그, 채팅, 웹캠, 네트워킹 세션), 지원 서비스(부수적 액세스는 이메일 전송, 라우팅 및 전달과 관련한 데이터와 이메일 통신 내용의 액세스를 포함할 수 있음).

D. 고객이 고객의 처리자인 공급업체에 제출한 기타 개인 데이터.

3. 처리의 성격.

A. IT 지원. 처리자는 주로 사용자에게 할당될 수 있는 IT 시스템의 IP 주소, MAC 주소 또는 기타 기술 ID를 처리합니다. 이는 필요한 경우에 오류 로그를 분석할 때 일반적으로 발생합니다.

B. 지원 서비스. 처리자의 직원은 고객 기술 지원 서비스를 제공할 때 통제권자의 내부 정책에 따라 개인 데이터와 접촉할 수 있습니다. 이는 원격 지원을 제공하거나 하드웨어 수리를 위해 고객의 영역에 들어갈 때 발생할 수 있습니다. 이러한 경우 해당 개인이 화면에서 문서, 이름표 또는 콘텐츠를 우연히 확인할 수 있습니다. 고객이 Webex와 같은 원격 지원 화면 공유 방식에서 연결이 설정되기 전에 관련 프로그램/소프트웨어를 종료하지 않은 경우 동일한 문제가 발생할 수 있습니다.

C. 추적 덤프 파일. 특정 공급업체 오퍼링 및 특정 지원 상황에서는 추적 덤프 파일을 분석하여 문제를 평가할 수 있습니다. 추적 덤프에는 오류와 관련된 읽기/쓰기 또는 전송 작업이 포함되어 있습니다. 콘텐츠는 일반적으로 OS 오류 형식으로 작성되며 파일 형식에 구애받지 않습니다. 파일 및 잠재적 콘텐츠의 재구성은 분석 작업에 포함되지 않습니다. 분석 중에 개인 정보를 읽을 수 있을 가능성은 매우 낮습니다.

D. 데이터 스토리지 디바이스. 하드웨어 스토리지 디바이스(예: HDD, SSD 등)의 반품 또는 리퍼비시에서는 모든 데이터가 자동화된 프로세스에서 삭제되거나 파괴됩니다.

E. Dell Cloud 및 aaS 구독. 개인 데이터는 Dell Cloud 및 aaS 구독의 제공을 위해 관련성 있는 방식으로 그리고 선택된 서비스 수준 및 지원 옵션을 준수하면서 처리해야 합니다. 본 계약과 해당 구독 설명서 및 작업 기술서는 세부 사항 및 가능한 추가 서비스에 적용됩니다.

4. 통제권자를 대신하여 개인 데이터가 처리되는 목적. 개인 데이터는 보증 및 지원 관련 서비스 및/또는 배포 서비스의 제공을 위해 관련성 있는 방식으로 그리고 선택된 서비스 수준 및 지원 옵션을 준수하면서 처리해야 합니다. 계약과 해당 서비스 설명서 및 작업 기술서가 적용됩니다.

5. 처리 기간. 처리 기간은 본 계약에 따릅니다.

6. 하위 프로세서. 처리자는 관련 국외 전송에 대한 표준 계약 조항/모델 조항/전송 계약의 체결을 포함하는 Dell Technologies 데이터 처리 명세서의 요구 사항에 따라 하위 처리자를 고용할 수 있습니다. 공급업체의 하위 처리자에 관한 자세한 내용은 www.dell.com/subprocessors에서 확인할 수 있습니다.

부록 II: 기술적 및 조직적 보안 조치

1. 일반 사항. 본 부록은 공급업체 계열사가 처리하고 전송하는 개인 데이터의 보호를 위한 공급업체의 기업 통제 조치에 적용됩니다. 공급업체 직원은 공급업체의 정보 보안 프로그램을 사용하여 본인의 책임을 확인할 수 있습니다. 고객은 공급업체와 별도로 합의된 작업 기술서에 명시된 대체 보호 조치를 마련할 수 있습니다.

2. 보안 관행. 공급업체는 공급업체의 기업 환경을 보호하고 (a) 정보 보안, (b) 시스템 및 자산 관리, (c) 개발, 그리고 (d) 거버넌스를 해결하기 위해 고안된 회사 정보 보안 관행 및 기준을 구현했습니다. 이러한 관행과 기준은 공급업체 CIO의 승인을 거치며 매년 공식적으로 검토됩니다.

3. 조직적 보안. 조직의 모든 개인은 이러한 관행 및 기준을 준수할 책임이 있습니다. 회사에서 이러한 관행 및 기준을 준수하도록 촉진하기 위해 정보 보안 기능은 다음을 제공합니다.

A. 전략, 정책/기준 및 규정 준수, 인식 및 교육, 위험 평가 및 관리, 계약 보안 요구 사항 관리, 애플리케이션 및 인프라 컨설팅, 보증 검사, 고객의 보안 방향 추진

B. 환경 전반에 걸쳐 보안 관리 채택을 지원하기 위한 보안 솔루션의 보안 검사, 설계 및 구현

C. 구현된 보안 솔루션, 환경 및 자산의 보안 운영, 인시던트 대응 관리

D. 보안 운영, 법률, 데이터 보호 및 수사 인적 자원(eDiscovery 및 eForensics 포함)을 통한 포렌식 수사

4. 자산 분류 및 관리. 공급업체는 물리적 및 논리적 자산 흐름을 추적하고 관리합니다. 공급업체가 추적할 수 있는 자산에는 다음이 포함됩니다.

A. 정보 자산(예: 식별된 데이터베이스, 재해 복구 계획, 비즈니스 연속성 계획, 데이터 분류 및 보관된 정보)

B. 소프트웨어 자산(예: 식별된 애플리케이션 및 시스템 소프트웨어)

C. 물리적 자산(예: 식별된 서버, 데스크탑/노트북, 백업/보관 테이프, 프린터 및 통신 장비)

D. 자산은 대외비 요구 사항을 결정하기 위한 비즈니스의 중요성에 따라 분류됩니다. 개인 데이터 처리를 위한 산업 지침은 기술적, 조직적, 물리적 보호를 위한 프레임워크를 제공합니다. 여기에는 액세스 관리, 암호화, 로깅 및 모니터링, 데이터 파기와 같은 통제 조치가 포함될 수 있습니다.

5. 개인 보안. 채용 과정의 일환으로 직원은 지역 법률에 따라 해당 심사 과정을 진행합니다. 공급업체의 연례 규정 준수 교육에 따라 직원은 온라인 과정을 완료하고 정보 보안 및 데이터 프라이버시를 포괄하는 평가를 통과해야 합니다. 또한 보안 인식 프로그램에서는 특정 직무 관련 자료를 제공할 수 있습니다.

6. 물리적/환경적 보안. 공급업체는 물리적 보안 프로그램에서 위험 완화와 관련된 다양한 기술적/조직적 접근 방식을 사용합니다. 보안 팀은 각 현장과 긴밀하게 협력하여 적절한 조치가 취해지고 있는지 확인하고 물리적 인프라, 비즈니스 및 알려진 위협에 대한 변경 사항을 계속 모니터링합니다. 또한 업계의 다른 업체에서 사용되는 모범 사례 조치를 모니터링하고 공급업체의 고유한 비즈니스 관행과 기대치를 모두 충족하는 방법을 신중하게 선택합니다. 공급업체는 아키텍처, 운영, 시스템을 비롯한 관리 요소를 고려하여 보안 방식을 조율합니다.

7. 커뮤니케이션 및 운영 관리. 공급업체의 IT 조직은 중앙 집중식 변경 관리 프로그램을 통해 회사 인프라, 시스템 및 애플리케이션에 대한 변경 사항을 관리하며, 여기에는 해당되는 경우 테스트, 비즈니스 영향 분석, 관리 승인이 포함될 수 있습니다. 인시던트 분석, 제약, 대응, 문제 해결, 보고, 정상 운영 복구를 비롯하여 보안 및 데이터 보호 인시던트에 대한 인시던트 대응 절차가 존재합니다. 악의적인 자산 이용과 악성 소프트웨어를 방지하기 위해 위험에 따라 추가적인 통제 조치를 구현할 수 있습니다. 이러한 통제 조치는 정보 보안 관행 및 기준, 제한적인 액세스, 지정된 개발 및 테스트 환경, 서버, 데스크톱 및 노트북의 바이러스 탐지, 바이러스 이메일 첨부 파일 검사, 시스템 규정 준수 검사, 침입 방지 모니터링 및 대응, 주요 이벤트에 대한 로깅 및 알림, 데이터 유형별 정보 처리 절차, 전자상거래 애플리케이션 및 네트워크 보안, 시스템 및 애플리케이션 취약성 검사를 포함하되 이에 국한되지 않습니다.

8. 액세스 제어. 적절한 승인 확인 절차에 따라 회사 시스템 액세스가 제한됩니다. 고의 여부를 불문하고 오용 위험을 줄이기 위해 업무와 최소한의 특권 분리에 기반하여 액세스 권한이 제공됩니다. 원격 액세스와 무선 컴퓨팅 기능은 제한되며 사용자 보호와 시스템 보안을 모두 적용해야 합니다. 인시던트 대응 및 포렌식 수사를 지원하기 위해 예외 기준에 따라 주요 장치와 시스템의 특정 이벤트 로그를 중앙에서 수집하여 보고합니다.

9. 시스템 개발 및 유지 보수. 공개된 제3자 취약성을 공급업체의 환경에 적용 가능한지 검토합니다. 공급업체의 비즈니스와 고객에 대한 위험도에 따라 문제 해결 시간이 미리 결정됩니다. 또한 위험도에 따라 신규 및 주요 애플리케이션과 인프라에 대해 취약성 검사 및 평가를 실시합니다. 운영 환경으로 전환하기 전에 개발 환경에서 코드 검토와 스캐너를 사용하여 위험도에 따른 코딩 취약성을 사전 예방적으로 감지합니다. 이 과정에서 취약성과 규정 준수를 사전 예정적으로 파악할 수 있습니다.

10. 규정 준수. 정보 보안, 법무, 개인 정보 보호 및 규정 준수 부서는 공급업체에 적용되는 지역 법률 및 규정을 파악하기 위해 노력합니다. 이러한 요구 사항에는 지적 재산, 소프트웨어 라이선스, 직원 및 고객의 개인 정보 보호, 데이터 보호, 데이터 처리 절차, 해외 데이터 전송, 재무 및 운영 절차, 기술 관련 규제 수출 통제, 포렌식 요구 사항 등이 포함됩니다. 정보 보안 프로그램, 개인 정보 보호 집행 위원회, 내외부 감사/평가, 내외부 법률 위원회 협의, 내부 통제 평가, 내부 침투 테스트 및 취약성 평가, 계약 관리, 보안 인식, 보안 컨설팅, 정책 예외 검토, 위험 관리와 같은 메커니즘을 결합하여 이러한 요구 사항의 규정 준수를 추진합니다.

부록 III – 데이터 전송 조건

1. 일반 사항. 공급업체 오퍼링의 제공이 유럽 경제 지역("EEA"), 영국 또는 스위스에서 EEA, 영국 또는 스위스 이외의 국가로 개인 데이터의 전송을 수반하는 경우(개인 정보 보호법에 따른 적정성 결정 대상이 아닐 것), 공급업체는여기에 명시된 해당 EC SCC의 적용을 받는다는 데 동의합니다. 영국의 경우, EC SCC와 함께 영국 국외 데이터 전송 부록이 영국 개인 데이터의 전송에 적용됩니다.

1.1 모듈 I 통제권자에서 통제권자로의 전송에 관한 EC SCC. 공급업체가 통제권자로서 개인 데이터를 처리하는 경우 공급업체와 고객은 통제권자 간 전송(모듈 I)과 관련된 범위에서 EC SCC를 준수합니다.

1.2 모듈 II 통제권자에서 처리자로의 전송에 관한 EC SCC. 공급업체가 고객을 대신하여 처리자로서 개인 데이터를 처리하는 경우 공급업체는 통제권자와 처리자 간 전송(모듈 II)과 관련된 범위에서 EC SCC를 준수합니다. 공급업체와 고객은 개인 데이터를 처리하기 위한 하위 처리자의 고용과 관련하여 제II절, 모듈 II, 제9조제(a)항(하위 처리자의 사용)의 옵션 2(일반 서면 승인)가 적용되고, 해당 기간이 30일이라는 데 동의합니다.

1.3 모듈 III 처리자에서 처리자로의 전송에 관한 EC SCC. 공급업체가 고객을 대신하여 하위 처리자로서 개인 데이터를 처리하는 경우 공급업체와 고객은 처리자 간 전송(모듈 III)과 관련된 범위에서 EC SCC를 준수합니다. 공급업체와 고객은 개인 데이터를 처리하기 위한 하위 처리자의 고용과 관련하여 제II절, 모듈 III, 제9조제(a)항(하위 처리자의 사용)의 옵션 2(일반 서면 승인)가 적용되고, 해당 기간이 30일이라는 데 동의합니다.

2. 준거법 및 관할권. SCC의 제IV절 제17조와 제18조에 따라, 옵션 1과 옵션 (b)가 각각 적용되며, EU 회원국은 아일랜드로 합니다.

3. EC SCC 부속서 I.

3.1. 당사자들 목록. EC SCC 부속서 I(A)에 따라 (a) 고객이 통제권자 또는 처리자인 경우 데이터 수출자는 고객이고 데이터 수입자는 공급업체가 됩니다.

3.2 전송에 대한 설명. EC SCC 부속서 I(B)에 따라, 다음에서 정하는 바를 따릅니다.

A. 데이터 주체, 처리할 개인 데이터의 범주: 본 명세서의 부록 I을 참조합니다.

B. 전송의 성격 및 목적: 본 계약에 명시된 의무를 이행하고 본 명세서의 부록 I에 자세히 설명된 처리 활동을 완료합니다.

C. 전송 빈도: 데이터 수입자는 본 계약에 따른 의무를 이행하기 위해 본 명세서의 조건에 따라 개인 데이터를 보존 및 전송합니다.

D. 보존 기간: 공급업체 오퍼링의 완료(해당하는 경우) 또는 본 계약 해지 및 고객의 서면 요청이 있는 때까지 개인 데이터를 보존해야 합니다. 단, 데이터 보호 요구 사항에서 해당 개인 데이터를 장기간 보존하도록 규정하는 경우는 예외로 합니다. 이 경우 고객은 해당 데이터 보호 요구 사항에서 규정한 기간 동안만 해당 개인 데이터를 보존해야 합니다.

3.3. 관할 감독 기관. EC SCC 부속서 I(C)에 따라, 관할 감독 기관은 아일랜드의 데이터 보호 위원회로 합니다.

3.4 기술적 및 조직적 조치: EC SCC 부속서 I(D)에 따라 데이터 수입자는 최소한 본 명세서의 부록 II에 명시된 수준의 보안 표준을 구현하고 유지해야 합니다. 하위 처리자가 취해야 하는 기술적 및 조직적 조치는 최소한 본 명세서의 부록 II에 기술된 보호 수준으로 수행되어야 합니다.

3.5 하위 처리자: EC SCC 부속서 III(E)에 따라 Dell Technologies 하위 처리자에 대한 자세한 정보는 www.dell.com/subprocessors에서 확인할 수 있습니다.