PTC 사이버 보안 및 데이터 프라이버시 부록(DPA).

본 DPA는 고객과 PTC(본 계약에서 정의함) 간의 계약의 일부를 구성한다. 고객은 자신의 명의로, 그리고 관련 법률이 요구하는 경우에는 계열사를 대리하여 계열사의 명의로 본 DPA를 체결한다. 달리 명시되지 않은 한, 본 DPA에 한하여 "고객"이라는 용어에는 고객과 그 계열사가 포함된다. 본 DPA에 정의되지 않은 모든 대문자 용어는 본 계약에서 정한 의미를 갖는다.

1. 목적 및 적용 범위

당사자들은 본 DPA가 PTC가 고객을 대신하여 수행하는 개인 정보를 포함한 모든 고객 데이터 처리에 적용된다는 점과 본 계약 조건을 보충한다는 점에 동의한다. 계약 조건과 본 DPA가 충돌하는 경우, DPA의 조건이 우선한다.

2. 해석

2.1. **계약**이란 PTC Cloud/SaaS 서비스 약관, PTC 고객 계약(라이선스 계약), 글로벌 서비스 계약 등을 포함해, PTC가 고객에게 서비스를 제공하는 조건을 정한 PTC와 고객 간의 모든 계약을 의미한다.

2.2. **관련 법률**이란 GDPR, 영국 GDPR, CCPA, LGDP, 그리고 개인 정보의 처리 및/또는 개인 정보 보호 또는 개인 정보 처리에 대한 개인의 권리 보호와 관련된 기타 모든 법률 또는 규정을 의미한다.

2.3. **CCPA**란 캘리포니아 소비자 개인정보보호법(2020년 캘리포니아 개인정보보호 권리법)[Ca. Civ. Code 1798.100, et seq.]에 의해 개정됨)과 캘리포니아 법무장관이 제공하는 관련 규정 또는 지침을 의미한다.

2.4. **개인정보처리자**란 개인 정보의 처리의 목적과 수단을 정하는 주체를 의미한다.

2.5. **고객 데이터**는 고객 계정 데이터 및 고객 사용 데이터를 제외하고 비 PTC 애플리케이션을 제외한 서비스 또는 고객을 대신하여 PTC에서 처리하는 서비스에 고객이 제출하는 전자 데이터 및 정보를 의미한다.

2.6. **고객 계정 데이터**란 PTC가 고객이 자신의 계정과 연결한 고객 계정 및 청구 정보(청구 주소 포함)에 액세스하도록 승인한 개인의 이름 또는 연락처 정보(예: 이메일 주소, 전화번호, 직책)를 포함하여 PTC와 고객의 관계와 관련된 개인 데이터를 의미한다. 고객 계정 데이터에는 PTC가 고객과의 관계를 관리하거나, 신원을 확인하기 위해 또는 관련 법률 및 규정이 요구하는 바에 따라 수집해야 하는 모든 데이터도 포함된다.

2.7. **고객 사용 데이터**란 고객 및 그 사용자가 이용하는 서비스 유형과 관련된 사용자 활동, 사용자의 컴퓨터 구성, 이들의 본 서비스 이용과 관련된 성능 지표, 통신의 출처 및 대상 식별에 사용되는 데이터, 활동 로그, 서비스 이행을 최적화/유지관리하고 시스템 악용을 조사/방지하기 위해 사용하는 데이터 등을 포함해, 본 서비스 제공과 관련하여 회사가 수집하고 처리하는 서비스 사용 데이터를 의미한다.

2.8. **데이터 침해**란 고객 데이터의 불법적인 파괴, 멸실, 변경, 무단 공개 또는 무단 액세스를 야기하는 고객 데이터의 보안, 기밀성, 가용성 또는 무결성의 손상을 초래하는 사건을 의미한다.

2.9. **GDPR**은 유럽 의회의 일반 데이터 보호 규정(EU) 2016/679와 동 규정을 국가별로 구현한 것을 의미한다.

2.10. **개인**은 식별되었거나 식별 가능한 자연인을 의미한다. 식별 가능한 자연인이란 특히 해당 자연인과 관련된 식별자 또는 기타 정보를 참조하여 직접적 또는 간접적으로 식별할 수 있는 사람을 의미한다.

2.11. **LGPD**란 2018년 8월 14일 자 법률 제13.709호, 브라질 일반 개인 데이터 보호법(2019년 7월 8일 법률 제13.853호에 의해 개정됨)을 의미한다.

2.12. **개인 정보**란 직접적 또는 간접적으로 특정 개인과 관련 또는 연결되어 있거나, 합리적으로 판단할 때 특정 개인과 관련 또는 연결할 수 있는 정보로서, 고객 데이터 내의 모든 정보를 의미한다.

2.13. **처리**란 자동 수단 이용 여부와 관계없이 액세스, 수집, 기록, 조직화, 구조화, 저장, 각색 또는 변경, 검색, 참고, 사용, 전송/배포/기타 방식에 의한 공개, 정렬 또는 조합, 제한, 삭제, 파기 등 고객 데이터에 대해 행해지는 작업 또는 일련의 작업을 의미한다.

2.14. **서비스**는 본 계약에서 정의된 모든 서비스를 의미한다.

2.15. **표준 계약 조항**이란 유럽 의회 및 이사회 규정(EU) 2016/679에 따라 개인 데이터를 제3국으로 이전하는 데 적용되는 표준 계약 조항에 관한 2021년 6월 4일 자 시행 결정 2021/914, 그리고 스위스의 개인 데이터 이전에 적용되는 승인된 관련 개정 사항을 의미한다.

2.16. **영국 부록**이란 영국 정보 커미셔너가 공포하고 2022년 3월 21일부터 시행되는 EU 집행 위원회 표준 계약 조항에 대한 국제 데이터 이전 부록의 버전 B1.0을 의미한다.

2.17. **영국 GDPR**이란 2018년 영국 유럽 연합법(철회) 제3조에 의해 영국법에 통합된 GDPR을 의미한다.

본 DPA는 관련 법률이 규정하는 권리/의무에 반하는 방식 또는 개인의 기본적 권리나 자유를 침해하는 방식으로 해석할 수 없다.

3. 목적 제한

PTC는 서비스 제공에 필요한 대로, 그리고 계약과 본 DPA에 명시된 대로만 고객 데이터를 처리한다. PTC는 (i) 고객 데이터를 판매하거나, (ii) 본 DPA에 명시된 서비스 제공 이외의 상업적 목적으로 고객 데이터를 보관, 사용, 공개하거나, (iii) 본 계약을 벗어나 고객 데이터를 보관, 사용, 공개하지 않는다. PTC는 고객 데이터에 대해 유치권, 부담 또는 기타 권리를 보유하거나 주장하지 않고, 그리고 제3자가 이를 주장하도록 허락하지 않는다.

4. 처리 기간

PTC의 고객 데이터 처리는 본 계약(본 DPA 포함) 기간에만 행해진다.

5. 처리의 보안

5.1 PTC는 고객 데이터의 보안을 보장하고 데이터 침해로부터 고객 데이터를 보호하기 위해, 부속문서 II에 명시된 기술적/조직적 조치를 구현하였으며, 계약 기간 동안 이를 유지한다. 적절한 수준의 보안을 평가할 때 최신 기술, 구현 비용, 처리의 성질, 범위, 맥락, 목적 및 관련 위험을 고려하였다.

5.2 PTC는 서비스 제공을 위해 반드시 필요한 경우에 한하여 고객 데이터에 대한 액세스 권한을 그 직원 및 하위 개인정보처리 수탁자에게만 부여한다. PTC는 고객 데이터를 처리할 권한이 있는 사람이 기밀 유지 의무를 약속했는지 또는 법령상 적절한 기밀 유지를 부담하는지 확인해야 한다.

PTC는 관련 사이버 보안 및 데이터 프라이버시 수단 내에서 고객 데이터에 액세스할 수 있는 직원을 정기적으로 교육한다.

5.3 PTC는 모든 고객 데이터를 엄격하게 기밀로 취급해야 하며, 고객 데이터를 처리하는 모든 직원, 대리인 및/또는 승인된 하위 개인정보처리 수탁자에게 고객 데이터의 기밀성을 알려야 한다. 단, 이는 당사자 간의 기존 계약상의 조치에 영향을 미치지 않는다.

6. 감사

6.1 PTC는 사이버 보안 및 개인정보보호를 위한 기술적/조직적 조치의 충분성을 확인하기 위해 독립적인 제3자 감사인 및/또는 내부 감사인의 감사를 정기적으로 받는다. 요청하는 경우, PTC는 i) 감사 보고서 요약본을 고객에게 제공하고, ii) PTC가 본 DPA 및 관련 법률 준수를 확인하는 데 필요한 정보 보안 및 감사 질문에 대한 응답을 포함하여 고객 데이터 처리와 관련해 고객의 모든 합리적인 정보 요청에 대해 서면으로 응답한다. 단, 고객은 1년에 최대 한 번만 이 권리를 행사할 수 있다. 문서에 명시된 바에 따라 PTC가 ISO 27001 인증 및 특정 서비스에 대한 SSAE 18 SOC(Service Organization Control) 2 보고서를 획득한 경우, PTC는 계약 기간 동안 이러한 인증 또는 표준, 또는 그에 상응하는 적절하고 유사한 후속 인증이나 표준을 유지하기로 동의한다.

6.2 관련 법률이 요구하는 경우, 그리고 고객이 합리적으로 판단할 때 위의 제6.1항에 따른 고객의 권리 행사를 통해 본 DPA 및 관련 법률의 준수가 입증되지 않은 경우에 한하여, 고객과 권한을 부여받은 담당자는 본 계약 기간 중에 PTC가 본 DPA 조건을 준수하는지 확인하기 위한 감사(검사 포함)를 수행할 수 있다. 이러한 감사(또는 검사)는 합당한 통지를 한 후에 PTC의 정규 업무 시간 중에 해야 한다. PTC와 고객은 감사 범위(감사 시간 및 기간 포함) 및 고객이 책임져야 하는 상환 비율에 합의해야 한다. 모든 상환 비율은 합리적이어야 하며, PTC 또는 그 대리인이 지출한 리소스를 고려해야 한다.

6.3 본 제6조는 본 DPA 및 관련 법률의 준수를 입증하는 과정에서 공개/제공되는 모든 정보의 기밀성을 보호하기 위해 고객 및 해당 독립 조사관이 NDA를 체결할 것을 전제로 한다.

7. 데이터 침해 알림

7.1 PTC는 데이터 침해로 여겨질 수 있는 사고를 감지하고 즉각적으로 대응할 수 있도록 설계된 통제 수단 및 정책을 구현했다. PTC는 데이터 침해가 실제로 발생했는지 확인하기 위해, 그리고 데이터 침해의 근본 원인을 식별하고 발생할 수 있는 부작용을 완화하며 재발을 방지하기 위해 고안된 합리적인 조치를 취하기 위해, 해당 사고를 조사할 에스컬레이션 경로를 즉시 정한다. 데이터 침해가 발생한 경우 처리의 성질과 가용 정보를 고려하여, PTC는 고객이 관련 법률상의 의무를 이행할 수 있도록 협력하고 지원해야 한다.

7.2 데이터 침해가 발생한 경우, PTC는 부당한 지체 없이 어떤 경우에도 PTC가 데이터 침해를 인지한 후 72시간 이내에 이러한 사실을 고객에게 통지해야 한다. 가능한 경우, 그러한 통지에는 최소한 다음 사항이 포함되어야 한다.

(a) "발생한 사건": 데이터 침해의 성질, 처음 파악된 날짜와 시간, 아는 범위 내에서 발생할 수 있는 결과에 대한 설명

(b) "관련된 정보": 영향을 받는 고객 데이터의 성질(가능한 경우), 관련 개인 및 데이터 기록의 범주 및 대략적인 수(알고 있는 경우)

(c) "PTC가 취하고 있는 조치": 가능성 있는 역효과를 완화하는 것을 포함해 데이터 침해를

해결하기 위해 취하거나 제안된 조치

(d) "고객이 할 수 있는 조치": 데이터 침해의 영향을 완화하기 위해 PTC가 고객에게 권장하는 조치

(e) "추가 정보": 데이터 침해에 관한 추가 정보를 얻을 수 있는 연락 담당자의 세부 정보

7.3 이 모든 정보를 동시에 제공할 수 없는 경우, 추가 정보를 이용할 수 있게 될 때 과도한 지체 없이 추가 정보를 제공해야 한다.

7.4 관련 법률이 요구하는 경우를 제외하고, PTC는 먼저 고객과 협의하고 고객의 서면 동의를 얻지 않은 상태에서(이러한 동의는 합리적인 이유 없이 거절할 수 없음) 데이터 침해와 관련된 고객의 이름이나 신원을 법집행 기관, 포렌식 조사관, 보험회사 또는 법률 고문 이외의 개인이나 제3자에게 알릴 수 없다. 데이터 침해가 PTC의 다른 고객에게 영향을 미치는 경우, 고객의 신원이 공개되지 않는 범위 내에서 일반적으로 공개 발표할 수 있다.

8. 개인 정보의 처리

8.1 당사자들은 개인 정보 처리 그 자체가 본 서비스의 내용이 아니라는 점에 명시적으로 동의한다. 그러나 당사자들은 일정한 범위 내에서 PTC가 개인 정보를 받을 수 있다는 사실을 완전히 배제할 수 없음을 인정한다. 따라서 본 DPA의 조건은 그러한 개인 정보의 공개로 인해 PTC가 고객을 대신하여 행하는 개인 정보의 처리에 적용된다. 개인 정보와 관련하여 고객은 i) 처리의 법적 근거를 확인하고, ii) 해당 개인에게 해당하는 모든 개인정보보호 고지를 제공하며, iii) 관련 법률이 요구하는 경우 동의를 받아야 할 책임이 있다. 고객은 건강 데이터, 정부 ID, 신용 카드 또는 지불 카드 정보, 관련 법률이 정한 특별 범주의 데이터와 같은 민감한 정보가 개인 정보에 포함되지 않도록 합당한 조치를 취해야 한다. 특히 개인 정보의 범주와 고객을 대신하여 개인 정보를 처리하는 목적 등의 처리 작업의 세부 사항은 부속문서 I에 명시되어 있다.

8.2 PTC는 고객의 문서화된 지침에 따라서만 개인 정보를 처리한다. 본 계약(본 DPA 포함)은 최초로 문서화된 지침이 된다. PTC는 관련 법률이 요구하고, 기술적으로 타당하며, 서비스 이행의 변경이 필요하지 않은 한 고객의 다른 지침을 따르기 위해 합당한 노력을 기울인다. 앞에서 언급한 예외가 적용되거나, 달리 PTC가 지침을 준수할 수 없거나 해당 지침이 관련법을 위반한다고 판단하는 경우, PTC는 즉시 고객에게 이를 통지한다(이메일 허용).

8.3 PTC는 관련 법률이 요구하는 경우 개인 정보를 처리할 수도 있다. 그러한 경우 법률이 중요한 공익상의 이유로 통지를 금지하는 경우를 제외하고, PTC는 개인 정보 처리에 앞서 그러한 법적 요구를 고객에게 통지해야 한다.

8.4 개인 정보의 정확성, 품질, 적법성과 고객이 개인 정보를 획득한 방법은 고객의 단독 책임이다. 따라서 관련 법률을 준수하면서 개인 정보를 수집하고 PTC로 전송하는 것, 특히 처리의 법적 근거를 확보하고 해당 개인에게 개인 정보의 수집/처리에 관해 적절히 알리는 것은 고객의 책임이다.

9. 하위 개인정보처리 수탁자의 활용

9.1 PTC는 서비스 이행을 위해 반드시 필요한 경우, 개인 정보 처리를 위한 하위 개인정보처리 수탁자의 고용에 대해 고객의 일반적인 승인을 받는다. 고객은 https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions에 명시된 그러한 하위 개인정보처리 수탁자 목록을 승인한다. PTC는 하위

개인정보처리 수탁자를 추가 또는 교체하여 해당 목록을 변경하고자 하는 경우, 늦어도 30일 전까지 그러한 사실을 고객에게 서면으로 알려 하위 개인정보처리 수탁자 고용에 앞서 고객이 그러한 변경에 반대할 수 있도록 충분한 시간을 제공해야 한다. PTC는 고객이 반대할 권리를 행사할 수 있도록 필요한 정보를 고객에게 제공해야 한다.

9.2 PTC가 하위 개인정보처리 수탁자를 고용하는 경우, 고용은 본 DPA상의 PTC의 의무와 동일한 처리 의무 및 사이버 보안 의무를 실질적으로 하위 개인정보처리 수탁자에게 부과하는 계약을 통해 이루어져야 한다.

9.3 PTC는 본 DPA에 따른 하위 개인정보처리 수탁자의 의무 이행과 관련하여 고객에게 전적으로 책임진다.

10. 개인 정보의 해외 이전

10.1 PTC는 글로벌 기업이기 때문에 고객 또는 개인이 있는 국가의 외부에서 개인 정보를 처리해야 할 수도 있다. PTC는 개인 정보를 이전할 때 언제나 관련 법률을 준수해야 하며, 적절한 보호 조치를 유지하고 개인의 권리가 행사될 수 있게 보장하며 효과적인 법적 구제 수단을 제공해야 한다.

10.2 **EEA 및 스위스의 개인 정보**: 당사자들은 고객이 개인 정보를 직접 또는 제3자를 거쳐 EEA 또는 스위스에서 PTC로 전송하는 범위 내에서, 유럽 집행위원회(또는 스위스에서 이전하는 경우 해당 관할 당국)가 개인 데이터를 충분한 수준으로 보호하는 것으로 인정하지 않은, EEA 또는 스위스 이외의 국가나 수령인에게 이전되는 개인 정보에 표준 계약 조항이 적용된다는 점에 동의한다. EU 표준 계약 조항이 적용되는 개인 정보를 EEA에서 이전하는 경우, 부속문서 III에 따라 EU 표준 계약 조항이 체결된 것으로(그리고 본 참조에 의해 본 DPA에 통합된 것으로) 간주한다.

10.3 PTC의 구속력 있는 기업 규칙 (개인정보처리 수탁자 정책)이 적용되는 경우, 구속력 있는 기업 규칙(개인정보처리 수탁자 정책)의 모든 조항은 참조를 통해 본 DPA에 통합되며, 본 DPA에 기업 규칙 전부가 명시된 것처럼 구속력을 가지며 고객이 집행할 수 있다. 본 DPA와 구속력 있는 기업 규칙(개인정보처리 수탁자 정책) 간에 충돌이나 불일치가 발생하는 경우, 구속력 있는 기업 규칙 (개인정보처리 수탁자의 정책)이 우선한다.

우선 순위. 고객과 PTC 간에 둘 이상의 이전 메커니즘이 적용되는 경우, 개인 정보 이전에는 (i) 구속력 있는 기업 규칙(개인정보처리 수탁자의 정책), 그리고 (ii) 표준 계약 조항의 순서로 하나의 이전 메커니즘이 적용된다.

10.4**영국 부록** 당사자들은 고객이 개인 정보를 직접 또는 제3자를 거쳐 영국에서 PTC로 전송하는 범위 내에서, 관할 영국 규제 당국 또는 영국 정부 기관이 개인 데이터를 충분한 수준으로 보호하는 것으로 인정하지 않은, 영국 이외의 국가나 수령인에게 이전되는 개인 정보에 영국 부록이 적용되며 부속문서 III에 따라 시작되고(이 언급에 의해 본 DPA에 통합됨) 완료된 것으로 간주된다는 점에 동의한다.

10.5**기타 해외 이전:** PTC가 EEA 이외의 국가, 스위스 또는 영국에 사업장이 있는 고객을 대신하여 개인 정보를 처리하는 경우, PTC는 관련 법률에 따라 개인 정보를 이전해야 한다. 여기에는 관련 법률에 따라 구속력 있는 기업 규칙을 갖춘 수령인, 또는 관련 데이터 보호 당국이 채택하거나 승인한 표준 계약 조항을 체결한 수령인에게 개인 정보를 이전하는 것이 포함된다.

11. 데이터 프라이버시 의무와 관련한 고객 지원

11.1 PTC는 개인으로부터 관련 법률에 따라 자신의 권리를 행사하겠다는 요청을 받은 경우, 이를 고객에게 즉시 알려야 한다. 고객이 승인하지 않는 한, PTC는 요청 자체에 응답하지 않아야 한다.

11.2 PTC는 처리의 성질과 보유하고 있는 가용 정보를 고려하여 a) 고객이 개인의 권리 행사 요청에 응답할 의무를 이행하고, b) 고객이 관련 법률에 따라 다음 의무를 준수하도록 도와야 한다.

(a) 개인 정보 처리에 관한 위험 평가 및/또는 예상 처리 작업이 개인 정보의 보호에 미치는 영향의 평가('데이터 보호 영향 평가')를 수행할 의무
(b) 데이터 보호 영향 평가를 수행한 결과, 고객이 위험 완화 조치를 하지 않으면 그러한 처리가 높은 위험을 초래할 수 있다고 나타난 경우, 개인 정보 처리에 앞서 관할 감독 당국과 협의할 의무
(c) PTC가 처리 중인 개인 정보가 정확하지 않거나 오래된 것이라는 사실을 알게 된 경우, 지체 없이 고객에게 이를 통지하여 정확하고 최신 상태의 개인 정보를 유지할 의무
(d) 고객이 개인 정보 처리의 보안과 관련된 의무를 준수하는 것을 지원할 의무

12. 개인정보처리자로서의 PTC:

고객은 고객 계정 데이터 및 고객 사용 데이터와 관련하여 PTC가 고객과의 공동 개인정보처리자가 아니라 독립적인 개인정보처리자임을 인정하고 이에 동의한다. PTC는 (i) 고객과의 관계를 관리하고, (ii) 회계 및 규정 준수, 그리고 고객과의 관계 관리 등을 목적으로 당사의 핵심 비즈니스 활동을 수행하고, (iii) 사기, 보안 사고, 기타 서비스 오용을 모니터링, 조사, 예방, 탐지하고, 고객 및 고객 데이터의 피해를 방지하며, (iv) 신원을 확인하고, (v) 개인 정보의 처리 및 보존과 관련하여 PTC에 적용되는 법적/규제적 의무를 준수하기 위해, 그리고 (vi) 기타 관련 법률과 본 DPA 및 본 계약에 따라 달리 허용되는 경우, 개인정보처리자의 자격으로 고객 계정 데이터 및 고객 사용 데이터를 처리한다. 또한 PTC는 관련 법률이 허용하는 범위 내에서 문제 해결, 새로운 제품/기능의 개발 및 알림 등 서비스의 제공, 최적화, 개선, 유지관리를 위해 개인정보처리자의 자격으로 고객 사용 데이터를 처리할 수 있다. 개인정보처리자인 PTC는 다음의 PTC의 개인 정보 보호 정책에 따라 개인 정보를 처리한다: https://www.ptc.com/en/documents/policies/privacy.

13. CCPA 조항

고객과 PTC 간에 CCPA를 적용할 때, 고객은 "사업체"이고 PTC는 "서비스 제공자"이며 비즈니스 목적으로 개인 정보를 수령한다. PTC는 개인 정보를 "제3자"에게 "판매" 또는 "공유"하지 않으며, 본 계약에 따라 또는 본 계약에 명시되거나 CCPA에서 허용하는 방식으로 고객에게 서비스를 제공하기 위한 구체적 목적에 필요한 경우를 제외하고 개인 정보를 보존, 사용 또는 공개하지 않는다. 이러한 목적상, "사업체", "서비스 제공자", "제3자", "판매" 및 "공유"는 CCPA의 섹션 1798.140에서 정의한 의미를 갖는다. PTC는 본 제13조의 제한 사항을 이해하고 준수할 것을 보증한다.

본 DPA 미준수 및 해지

본 DPA에 따른 각 당사자 및 그 계열사의 책임에는 본 계약에 명시된 책임 배제/제한이 적용된다. 본 DPA에 따라 PTC 또는 그 계열사를 대상으로 하는 모든 클레임은 계약 당사자인 고객 법인만 제기해야 한다. 어떤 경우에도 본 DPA 또는 당사자는 개인 또는 관할 감독 당국의 권리를 제약 또는 제한할 수 없다.

14. 고객 데이터 검색 및 삭제

본 계약이 해지되거나 만료되는 경우, 고객은 본 계약에 명시된 바에 따라 고객 데이터를 내보낼 수 있으며, 고객 데이터를 내보낼 수 없는 경우 PTC는 고객 데이터를 고객에게 반환해야 한다. PTC는 관련 법률에서 고객 데이터의 지속적인 보관을 요구하지 않는 한, 본 계약 조건에 따라 계약 종료 후 약 30일 이내에 모든 고객 데이터를 삭제해야 한다. 고객 데이터가 삭제되거나 반환될 때까지 PTC는 본 DPA를 계속 준수해야 한다.

15. 기타 조항

15.1 당사자들은 본 서비스와 관련하여 당사자들이 지금까지 체결한 기존 DPA가 있는 경우 본 DPA가 이를 대체한다는 점에 동의한다.

15.2 관련 법률에서 달리 요구하지 않는 한, 본 DPA는 본 계약의 준거법 및 관할 조항에 따라 적용하고 해석한다.

15.3 본 DPA와 표준 계약 조항은 본 DPA의 제15조에 따라 PTC가 고객 데이터를 삭제하는 동시에 자동으로 종료된다.

(이하 여백)

부속문서 I

개인 정보가 처리되는 정보 주체의 범주

고객은 본 서비스에 개인 정보를 제출할 수 있으며, 단독 재량으로 그 범위를 결정하고 관리한다. 여기에는 다음 범주의 개인에 관한 개인 정보가 포함될 수 있지만 이에 국한하지 않는다.

- (자연인인) 고객의 직원, 대리인, 고문, 프리랜서
- 고객의 고객, 잠재 고객, 비즈니스 파트너, 벤더의 직원 또는 연락 담당자
- 고객이 본 서비스를 사용할 수 있도록 승인한 고객의 사용자

처리되는 개인 정보의 범주

고객은 본 서비스에 개인 정보를 제출할 수 있으며, 단독 재량으로 그 범위를 결정하고 관리한다. 여기에는 다음 범주의 개인 정보가 포함될 수 있지만 이에 국한하지 않는다.

- 성명
- 직책
- 직위
- 고용주
- 연락처 정보(회사, 이메일, 전화번호, 실제 사업체 주소)
- ID 데이터
- .

처리되는 민감한 데이터(해당하는 경우), 그리고 데이터의 성질 및 관련 위험을 완전히 고려하여 적용하는 제한 또는 보호 조치(예: 엄격한 목적 제한, 액세스 제한(특수 교육을 이수한 직원에게만 액세스 권한 허용 포함), 데이터 액세스 기록 작성, 제3자 이전 제한 또는 추가 보안 조치).

- 없음

처리의 성질

- 본 서비스 제공에 필요할 수 있는 수집, 기록, 조직화, 구조화, 저장, 각색 또는 변경, 검색, 참고, 전송이나 배포 또는 기타 방식에 의한 공개, 제한, 삭제, 파기

고객을 대신하여 개인 정보를 처리하는 목적

- 본 서비스 제공(본 계약에서 구체적으로 정의함)

처리 기간

- PTC 가 본 계약에 따라 본 서비스를 제공하는 기간 및 그 연장/갱신 기간.

부속문서 II

고객 데이터의 보안을 보장하기 위한 기술적/조직적 조치 등을 포함한 기술적/조직적 조치

"네트워크"란 LAN(Local Area Network), WAN(Wide Area Network)을 사용하여 함께 연결된 데이터를 공유할 수 있도록 서로 연결된 컴퓨터, 서버, 메인프레임, 네트워크 기기, 주변기기 또는 기타 기기의 집합을 의미한다.

"보안 컨트롤"이란 정보 기술 시스템 및 관련된 물리적 장소에 대한 보안 위험을 해결하거나 관련 정책을 구현하기 위한 방법으로, 본 계약 조건에 따라 NIST 800-53을 시행하는 데 필요한 특수한 하드웨어, 소프트웨어, 관리 메커니즘을 의미한다. 보안 컨트롤에는 특정 그룹, 개인 또는 기술과 관련된 보안 정책 요소의 구현에 사용되는 기술, 방법론, 구현 절차 및 기타 세부 요소 또는 기타 프로세스를 명시한다.

"보안 정책"이란 보안과 관련하여 회사 정보의 보호와 관련 법률 및 규정 준수 요구하는 지침을 의미한다.

"보안 절차"란 NIST 800-53 및/또는 ISO27001 인증을 획득하고 이러한 인증을 준수할 수 있도록 하기 위해 취해지는 단계별 조치를 의미한다.

"시스템"이란 컴퓨터 소프트웨어, 펌웨어, 컴퓨터 하드웨어(일반 또는 특수 목적용), 통신 기능(모든 음성, 데이터, 비디오 네트워크 포함) 및/또는 이와 유사한 자동화, 컴퓨터 기능 및/또는 소프트웨어 관련 항목을 의미한다.

본 계약 및 DPA 조건에 따른 보안 의무를 준수하기 위해 PTC는 항상 (i) ISO27001 인증과 같은 업계 최고 표준을 따르는 보안 프로세스를 마련하거나 미국 국립표준기술연구소(NIST) 800-53 보안 요구사항에 따른 "보통" 영향에 해당하는 컨트롤을 시행하고, (ii) 본 DPA에 명시된 보안 요구사항, 의무, 사양 및 이벤트 보고 절차를 갖추어야 한다.

1. 보안 프로그램 및 거버넌스

PTC는 다음 사항을 포함하는 보안 프로그램을 항상 유지한다.

(a) 아래 요구사항을 관리하는 CISO 또는 보안 담당자
(b) 보안 정책, 보안 절차 및 보안 컨트롤
(c) 보안 사고 관리 프로그램
(d) 이 업무를 지원하는 모든 직원을 위한 보안 인식 및 교육 프로그램
(e) 보안 변경 프로세스가 진행되는 동안 PTC 보안 환경의 안정성과 신뢰성을 강화하기 위한 보안 변경 관리 프로그램
(f) 정기적인 테스트를 포함하는 비즈니스 연속성 및 재해 복구 계획
(g) 위험 처리의 식별, 평가, 대응, 구현을 위한 보안 위험 평가 프로세스
(h) 제공자가 이 업무의 일환으로 소프트웨어를 개발하고 제공하는 경우, 제공자는 OWASP OPEN SAMM과 같은 산업 표준에 따른 안전한 소프트웨어 개발 수명 주기를 유지한다
(i) 제공자가 이 업무의 일환으로 클라우드 서비스(IaaS, PaaS, SaaS)를 제공하는 경우, 제공자는 CSA CCM,

SOC2 표준에 따라 관행을 유지한다

2. 설계 및 테스트를 통한 보안

PTC는 다음을 유지한다.

(a) 효과적인 NIST 800-53 보안 컨트롤의 조정/구현을 합리적으로 보장하는 보안 아키텍처
(b) 데이터 보호에 필요한 효과적인 방화벽 및 침입 탐지 기술 시스템
(c) 데이터 분리를 위한 적절한 네트워크 보안 설계 요소
(d) 전송 및 저장 시 정보를 암호화하는 절차
(e) PTC의 보안 시스템 및 프로세스를 정기적으로 테스트하는 절차
(f) 웹사이트 애플리케이션이 해당 시스템을 통해 수집, 처리, 전송하는 고객 데이터를 보호할 수 있도록 설계해 주는 데이터베이스 및 애플리케이션 계층 설계 프로세스

3. 모니터링 및 패치 관리

PTC는 다음 사항을 마련하였으며, 계약 기간 동안 이를 유지한다.

(a) 보안 패치를 최신 상태로 유지하는 메커니즘
(b) 고객 데이터에 대한 실제 공격이나 침입, 또는 그러한 시도를 탐지하는 모니터링 시스템 및 절차
(c) 보안 경보의 모니터링, 분석, 대응 절차
(d) 최신 상용 바이러스 백신 및 맬웨어 방지 소프트웨어 사용 및 정기적 업데이트
(e) 설치된 소프트웨어의 무결성을 정기적으로 확인하는 절차

4. 승인된 PTC 사용자에 대한 원격 액세스 제어

PTC는 다음을 시행한다.

(a) "알아야 할 사항" 정책에 따른 사용자 인증 및 권한 부여를 위한 적절한 메커니즘
(b) PTC와 하위 개인정보처리 수탁자(해당하는 경우)와 같이 승인된 원격 사용자에게 엄격한 액세스 제한을 적용하기 위한 보안 컨트롤
(c) 승인된 사용자 계정 및 인증 관리를 위한 적시의 정확한 관리
(d) 모든 비밀번호를 암호화하고 해시하는 메커니즘
(e) 비활성 계정/해지된/이전된 승인된 사용자의 액세스 권한을 즉시 취소하는 절차
(f) 업무 분담을 유지하는 절차
(g) 컴퓨터 액세스 권한이 있는 각 승인된 사용자에게 고유한 ID를 할당하는 절차
(h) PTC가 제공한 비밀번호 및 보안 매개변수 기본값을 변경하고 적절하게 관리하는 절차
(i) 고객 작업 명세서와 관련된 시스템에 대한 다단계 인증(MFA)의 합리적인 적용

5. 시설 출입 통제

PTC는 다음 사항을 마련하였으며, 계약 기간 동안 이를 시행한다.

(a) 모든 정보 자산 및 정보 기술이 적절한 데이터 센터에 저장되고 보호되도록 보장하는 해당 자산 및 기술에 대한 물리적 보호 메커니즘
(b) 시스템에 대한 물리적 접근을 제한하는 적절한 시설 출입 통제 유지
(c) "알아야 할 사항" 정책을 기준으로 시설 출입을 모니터링하고 제한하는 절차
(d) 화재 및 수해에 의한 손상이나 기술적 장애 등 잠재적인 환경 위험으로 인해 고객 데이터 및 고객이

의존하는 시스템이 파괴, 멸실, 손상되지 않도록 보호하는 조치

(e) 고객의 모든 민감한 정보를 물리적으로 보호하고 더 이상 필요하지 않을 때는 해당 정보를 적절하게 파기하는 보안 컨트롤

[PTC의 사이버 보안 및 프라이버시 프로그램에 대한 자세한 내용은 PTC의 Trust Center(https://www.ptc.com/en/about/trust-center)를 참조한다. 여기에서는 PTC의 ISO27001 및 SOC2 Type II 보고서 사본을 얻을 수 있다.]

부속문서 III

표준 계약 조항

다음의 표준 계약 조항 모듈은 PTC Inc.(데이터 수입자)와 고객(고객이 계열사 또는 이전과 관련된 다른 개인정보처리자를 대신하여 개인정보처리자 역할을 하는 경우 포함)(데이터 수출자) 사이에 적용되며, 본 문서를 통해 체결되고 참조를 통해 본 계약에 통합된다.

모듈 1 – 개인정보처리자와 개인정보처리자 간의 이전(고객이 개인정보처리자이고 PTC 가 본 DPA 에 따라 독립적인 개인정보처리자의 자격으로 개인 정보를 처리하는 경우)
모듈 2 – 개인정보처리자와 개인정보처리 수탁자 간의 이전(개인정보처리 수탁자인 PTC 에 개인 정보를 이전하는 경우)
모듈 3 - 개인정보처리 수탁자와 개인정보처리 수탁자 간의 이전(고객이 개인정보처리 수탁자이고 PTC 가 하위 개인정보처리 수탁자인 경우)

표준 계약 조항과 관련하여 다음을 적용한다.

- 제 9 조 – 하위 개인정보처리 수탁자의 활용.
    - 모듈 2 및 모듈 3
        - 옵션 2, 일반 서면 승인
        - 데이터 수입자는 하위 PTC 수탁자를 추가 또는 교체하여 해당 목록을 변경하고자 하는 경우, 늦어도 30 일 전까지 그러한 사실을 데이터 수출자에게 서면으로 구체적으로 알려 하위 PTC 수탁자 고용에 앞서 데이터 수출자가 그러한 변경에 반대할 수 있도록 충분한 시간을 제공해야 한다.
- 제 17 조 – 준거법
    - 모듈 1, 2 및 3
        - 옵션 1
        - 이러한 조항에는 EU 회원국 중 한 국가의 법률이 적용된다. 단, 해당 법률이 제 3 수익자의 권리를 허용해야 한다. 당사자들은 그 법률이 아일랜드공화국 법률이라는 점에 동의한다
- 제 18 조 - 법정지 선택 및 관할권
    - 모듈 1, 2 및 3
    - (b) 당사자들은 그 법원이 아일랜드공화국 법원이라는 점에 동의한다.

표준 계약 조항의 부속문서 I
A. 당사자 목록

- 1 – 데이터 수출자는 유럽 연합, 영국, 스위스에 소재하는 개인정보처리자를 대신하여 자신의 명의로 행위하는 고객이다.
- 2 – 데이터 수입자는 PTC Inc.(주소: 121 Seaport Boulevard, Boston, MA 02021)이다. 그리고 본 계약 내의 고객 및 PTC 각각의 연락처 정보가 적용된다.

B. 이전에 관한 설명

개인 데이터가 이전되는 데이터 주체의 범주

- 모듈 1 – 개인정보처리자와 개인정보처리자 간의 이전
  - 고객이 PTC 제품을 사용하거나 PTC 서비스에 액세스할 수 있도록 승인한 개인은 고객의 직원, 컨설턴트, 하도급업체, 공급업체, 비즈니스 파트너 및 고객임.
- 모듈 2 – 개인정보처리자와 개인정보처리 수탁자 간의 이전
  - 고객의 직원, 컨설턴트, 하도급업체, 공급업체, 비즈니스 파트너 및 고객. 고객이 본 서비스에 개인 데이터를 업로드할 수 있는 기타 개인
- 모듈 3 – 개인정보처리 수탁자와 개인정보처리 수탁자 간의 이전
  - 고객의 직원, 컨설턴트, 하도급업체, 공급업체, 비즈니스 파트너 및 고객. 고객이 본 서비스에 개인 데이터를 업로드할 수 있는 기타 개인

개인 데이터가 이전되는 데이터 주체의 범주:

이전되는 개인 데이터는 다음 데이터 카테고리에 해당할 수 있다.

- 모듈 1:
  성명, 회사, 사용자 이름, 사용자 ID, 조직, 비즈니스 연락처 정보, PTC 제품 및 서비스와의 상호 작용 정보(예: 로그 파일 및 사고 보고서) IP 주소, 쿠키 데이터, 장치 식별자 및 이와 유사한 장치 관련 정보
- 모듈 2 및 모듈 3: 성명, 회사, 조직, 비즈니스 연락처 정보, PTC 제품 및 서비스와의 상호 작용 정보(예: 로그 파일 및 사고 보고서), PTC 서비스에 업로드되는 개인 데이터 민감한 데이터는 이전되지 않는다

이전 빈도(예: 데이터가 한 번만 이전되는지 아니면 계속 이전되는지 등).

계속

처리의 성질

데이터 수입자는 본 서비스(본 계약에서 더 구체적으로 설명함) 제공에 필요한 경우에 본 계약(DPA 포함) 조건에서 승인한 바에 따라 개인 데이터를 처리해야 하며, 그러한 처리에는 다음 사항이 포함된다.

데이터 수입자가 본 서비스를 제공하는 데 필요할 수 있는 수집, 기록, 조직화, 구조화, 저장, 각색 또는 변경, 검색, 참고, 전송이나 배포 또는 기타 방식에 의한 공개, 제한, 삭제, 파기.

개인 데이터 보관 기간, 또는 이것이 불가능한 경우에는 해당 기간을 결정하는 기준:

개인 데이터는 본 계약 조건에 따라 서비스 종료 시 본 서비스에서 삭제된다.

(하위) PTC 수탁자에 이전하는 경우, 처리 주제, 성질, 기간도 명시한다.

참조: https://www.ptc.com/en/documents/legal-agreements/data-processing-terms-and-conditions

C. 관할 감독 당국

- 제 13 조에 따라 관할 감독 당국을 명시한다.
    - 관할 감독 기관은 아일랜드공화국의 데이터 보호 위원회이다.

표준 계약 조항의 부속문서 II - 기술적/조직적 조치.

본 DPA 의 부속문서 II 가 적용된다

영국 – 부록

(a) 영국 부록의 표 1 에서, 당사자들의 세부 정보 및 주요 연락처 정보는 본 부속문서 III 의 단락 A 에 있다.

(b) 영국 부록의 표 2 에서, 본 영국 부록이 추가되는 승인된 EU SCC 의 버전, 모듈 및 선택된 조항에 관한 정보는 본 부속문서 III 의 단락 B 에 있다.

(c) 영국 부록의 표 3 에서:

1. 당사자 목록은 본 부속문서 III 의 단락 A 에 있다.
2. 이전에 대한 설명은 부속문서 III 의 단락 B(처리의 성질)에 명시되어 있다.
3. 부속문서 II(기술적/조직적 보안 조치)는 영국 부록 부속문서 II 로 적용된다.
4. 하위 개인정보처리 수탁자의 목록은 https://www.ptc.com/-/media/Files/PDFs/legal-agreements/fy18/PTC-Inc-List-of-Sub-processors.pdf 에 있다.

(d) 영국 부록의 표 4 에서, 수입자와 수출자는 모두 영국 부록의 조건에 따라 영국 부록을 해지할 수 있다.

2.5 충돌. 표준 계약 조항 또는 영국 부록과 본 DPA 또는 계약의 다른 조건 사이에 충돌이나 불일치가 존재하는 경우, 본 계약, 표준 계약 조항 또는 영국 부록(해당하는 경우)이 우선한다.