데이터 처리 부록(이전 SaaS 부록)

본 데이터 처리 부록("**DPA**")은 특정 SaaS 소프트웨어 라이선스 및/또는 유지 관리 및/또는 컨설팅 서비스(본 DPA의 목적을 위해, 이하 "**서비스**") 사이의 소프트웨어 계약 및/또는 서비스 계약("**계약**")에 통합되고, 구매를 위한 공급자와 고객 간의 서면(전자 형태 포함) 계약의 일부를 구성합니다. 여기에 정의되지 않은 모든 용어는 계약에 명시된 의미를 갖습니다.

1. 정의. 문맥 또는 계약에서 정의되지 않은 용어는 아래에 할당된 의미를 갖습니다.

a) "***관리자***"는 단독으로 또는 다른 사람과 공동으로 개인 데이터 처리의 목적과 수단을 결정하는 자연인 또는 법인, 공공 기관, 기관 또는 기타 단체를 의미합니다.

b) "***데이터 보호법***"은 해당하는 경우 (i) 캘리포니아 프라이버시 권리법에 의해 개정된 캘리포니아 소비자 프라이버시법 및 그에 따라 공표된 법적 구속력이 있는 규정("**CCPA**"), (ii) 일반 데이터 보호 규정(Regulation (EU) 2016/679)("**EU GDPR**" 또는 "**GDPR**"), (iii) 스위스 연방 데이터 보호법("**FADP**"), (iv) 2018 년 유럽연합(탈퇴)법의 섹션 3 에 따라 잉글랜드 및 웨일스 법의 일부를 형성하는 EU GDPR("**영국 GDPR**"), (v) 2018 년 영국 데이터 보호법을 포함하여 계약에 따라 고객 개인 데이터 처리에 적용되는 모든 법률 및 규정을 의미합니다. 각각의 경우 수시로 업데이트, 수정 또는 교체됩니다.

c) "***데이터 주체***"는 고객 개인 데이터와 관련된 식별되었거나 식별 가능한 자연인을 의미합니다.

d) "***개인 데이터***"는 식별되었거나 식별 가능한 자연인에 대한 정보 또는 별도로 "개인 데이터", "개인 정보", "개인 식별 정보"나 데이터 보호법에 정의된 유사한 용어를 구성하는 정보를 의미합니다.

e) "***개인 데이터 위반***"은 공급자가 처리 중인 고객 개인 데이터에 대한 우발적이거나 불법적 파기, 손실, 변경, 무단 공개 또는 제 3 자의 무단 액세스를 의미하며, 각각의 경우 데이터 보호법에 따라 관리자가 권한 있는 데이터 보호 기관 또는 데이터 주체에게 통지해야 합니다.

f) "***처리***"는 수집, 기록, 구성, 구조화, 저장, 적응 또는 변경, 검색, 참조, 사용, 전송, 배포에 의한 공개 또는 다른 방식으로 제공, 정렬 또는 조합, 제한, 삭제 또는 파기와 같은 자동화된 수단에 의한 것인지 여부에 관계없이 개인 데이터에 대해 수행되는 모든 작업을 의미합니다.

g) "***처리자***"는 관리자를 대신하여 개인 데이터를 처리하는 자연인 또는 법인, 공공 기관, 기관 또는 기타 기관을 의미합니다.

h) "***표준 계약 조항***" 또는 "**EU SCC**"는 2021/914 결정에서 유럽 위원회가 승인한 표준 계약 조항을 의미합니다.

i) "***하위 처리자***"는 서비스 일부 또는 전체를 제공하기 위해 공급자(또는 공급자의 계열사)가 고용하고 본 DPA 에 따라 고객 개인 데이터를 처리하는 공급자의 계열사 및 공급자와 협력하는 제 3 자를 의미합니다.

2. 고객 개인 데이터의 처리

공급자는 관리자로서 고객을 대신하여 행동하는 처리자로서(또는 해당하는 경우 처리자로서 고객을 대신하는 하위 처리자로서) 계약에 따라 고객 개인 데이터를 처리할 수 있습니다. 공급자는 (i) 본 DPA 및 계약, (ii) 고객의 서면 지침에 따라 또는 (iii) 데이터 보호법에 따른 통지 요건을 조건으로 해당 법률에 따라 공급자의 의무를 준수하여 고객에 대한 공급자의 의무를 수행하는 목적으로만 개인 데이터 처리를 수행합니다. 처리 주제, 해당 기간, 성격 및 목적, 고객 개인 데이터의 유형 및 데이터 주체에 대한 세부 사항은 계약에 명시되어 있으며, 명시되지 않은 경우 본 DPA의 부속서 I 에 명시됩니다. 고객 및 공급자는 서비스와 관련하여 처리되는 개인 데이터에 적용되는 데이터 보호법에 따라 각자의 의무를 준수하는 데 동의합니다. 고객은 공급자에게 개인 데이터를 공개, 전송 또는 다른 방식으로 제공하기 전에 고객 개인 데이터 처리에 관한 데이터 보호법을 준수할 단독 책임이 있습니다. 공급자는 고객의 지시가 데이터 보호법을 위반한다고 생각되는 경우 즉시 고객에게 알려야 합니다.

3. 처리 보안

a) **일반 보안 정책**. 공급자는 계약에 언급되고 다음을 포함하여 https://www.oneidentity.com/legal/security.aspx (총괄하여 "***보안 사이트***")에 추가로 설명된 공급자의 보안 조치에 따라 고객 개인 데이터의 보안, 기밀성, 무결성 및 가용성을 보호하고 개인 데이터 위반으로부터 보호하도록 설계된 고객 개인 데이터의 특성에 맞도록 기술적 및 조직적 조치, 절차 및 관행을 구현하고 유지합니다.

- 정보 보안 정책
- 기술적 및 조직적 조치에 대한 서술
- 데이터 위반 대응 정책
- 개인정보 보호 정책

공급자는 제공된 전체 보호 수준을 실질적으로 낮추지 않는 한 보안 사이트를 수정할 수 있습니다.

b) **기밀 유지**. 공급자는 계약에 명시된 기밀 유지 의무에 따라 고객 개인 데이터를 보호합니다. 공급자는 고객 개인 데이터를 처리하는 직원이 서면 기밀 유지 계약을 체결했는지 확인합니다. 공급자는 해당 직원의 고용 종료 후에도 그러한 기밀 유지 의무가 유지되도록 해야 합니다. 공급자는 고객 개인 데이터에 액세스할 수 있는 개인에게 데이터 보안 및 데이터 프라이버시 요구 사항 및 원칙에 대해 정기적으로 교육합니다.

4. 데이터 주체 요청.

고객의 요청 시 공급자는 상업적으로 합리적인 조치를 통해 고객이 데이터 보호법에 따라 고객의 의무를 준수하여 데이터 보호법에 따라 본인의 권리를 행사하려는 개인의 요청에 응답하도록 지원합니다. 단, 고객이 그러한 요청을 독립적으로(서비스를 사용하는 방법 포함) 합리적인 범위에서 이행할 수 없는 경우를 조건으로 합니다. 공급자가 본 계약에 따라 처리되는 개인 데이터와 관련하여 데이터 주체 요청을 받는 경우, 공급자는 데이터 주체(데이터 주체가 고객을 식별하는 정보를 제공한 경우)에게 요청을 고객에게 리디렉션하도록 조언합니다.

5. 감사 권한.

a) **공급자의 일반적인 기록.** 공급자는 데이터 보호법에 따라 처리 기록을 보관하고 고객의 서면 요청 시 본 DPA 및 관련 데이터 보호법에 따라 공급자의 의무 준수를 입증하는 데 합리적으로 필요한 모든 기록을 고객에게 제공합니다.

b) **제3자 규정 준수 프로그램.** 공급자는 제3자 감사 및 인증 프로그램(있는 경우)을 설명하고 고객의 서면 요청 시 고객이 확인할 수 있는 감사 보고서(각각 "**감사 보고서**")의 요약 사본을 만듭니다(계약에 명시된 기밀 유지 의무를 조건으로 함). 고객은 필요에 따라 관련 정부 기관과 감사 보고서 사본을 공유할 수 있습니다.

c) **고객 감사.** 고객은 고객의 비용으로 아래 감사 요소와 일치하는 상호 합의 계획에 따라 감사("**감사**")를 수행할 수 있습니다. 고객은 (1) 공급자가 감사 보고서를 제공했지만 고객이 공급자가 본 DPA 또는 데이터 보호법을 준수한 사실을 확인하기에 충분한 정보가 제공되지 않는 경우, (2) 고객이 정부 기관 감사에 응답하는 데 필요한 경우 또는 (3) 개인 데이터 위반과 관련하여 감사 권한을 행사할 수 있습니다.

각 감사는 (1) 공급자와 기밀 유지 계약을 체결하는 독립적인 제3자가 수행하고, (2) 고객이 공급자의 본 DPA 준수 여부와 당사자들의 데이터 보호법 준수 여부를 평가하는 데 합리적으로 요구되는 사안으로 범위가 제한되며, (3) 상호 합의된 날짜와 시간에 공급자의 정규 업무 시간 중에만 일어나고, (5) 공급자가 관리하는 시설에만 적용되며, (6) 고객 개인 데이터에 대한 결과로 제한하고, (7) 모든 결과를 데이터 보호법이 허용하는 최대 범위에서 기밀 정보로 취급해야 합니다.

6. 하위 처리자 및 해외 전송.

a) **하위 처리자 사용.** 고객은 일반적으로 공급자에게 서비스 프로비저닝과 관련하여 하위 처리자를 고용할 수 있는 권한을 부여합니다. 공급자는 본 DPA의 조항 및 고객과 공급자 간의 지침에 따라 하위 처리자와 적절한 서면 계약을 체결합니다. 공급자는 공급자가 고용한 하위 처리자가 일으킨 행위의 범위까지 본 DPA 위반에 대해 책임을 집니다.

b) **하위 처리자 목록.** 공급자는 https://support.oneidentity.com/subprocessor에서의 등록을 통해 고객이 사용할 수 있는 기능 및 위치를 포함하여 소프트웨어 제품별 하위 처리자 목록을 유지합니다. 공급자는 새로운 하위 처리자에게 개인 데이터에 액세스하도록 권한을 부여하기 최소 30일 전에 하위 처리자 목록을 업데이트하고 등록 시 이메일을 통해 고객에게 알립니다.

c) **새로운 하위 처리자에 대한 이의 제기.** 고객이 새로운 하위 처리자를 승인하지 않는 경우 고객은 통지 기간이 끝나기 전에 비승인 이유에 대한 설명이 포함된 서면 종료 통지를 제공하여 해당하는 SaaS 소프트웨어에 대한 구독을 종료할 수 있습니다.

d) **해외 전송.** 유럽 및/또는 영국 개인 데이터를 개인 데이터에 대한 적절한 보호를 제공하지 않는 제3국에 있는 하위 처리자에게 전송하는 경우 공급자와 해당 하위 처리자는 유럽 및 영국 데이터 보호법에 따라 그러한 개인 데이터의 전송에 대한 적절한 안전 조치를 제공하기 위해 EU SCC를 체결했습니다.

7. 개인 데이터 위반 알림.

보안 사이트에 명시된 의무 외에도 공급자는 개인 데이터 위반을 인지한 후 즉시 고객에게 알리고 합당한 정보를 제공하여 고객이 데이터 보호법에 따라 요구되는 개인 데이터 위반을 보고해야 하는 고객의 의무를 충족할 수 있도록 지원합니다. 공급자는 이러한 정보가 입수되는 대로 단계적으로 제공할 수 있습니다. 공급자는 개인 데이터 위반의 원인을 식별하기 위해 선의의 노력을 기울이고 개인 데이터 위반의 원인을 교정하기 위해 공급자가 필요하고 합리적이라고 판단하는 조치를 취하는 데 동의합니다.

8. 고객 개인 데이터의 삭제.

고객이 서비스가 완료되기 최소 30일 전에 공급자에게 통지하지 않는 한, 계약이 종료되거나 만료된 후 공급자는 공급자의 시스템에서 모든 고객 개인 데이터를 삭제합니다. 공급자는 산업 표준 보안 삭제 관행에 따라 삭제합니다. 전술한 내용에도 불구하고 공급자는 (i) 데이터 보호법에서 요구하는 대로 또는 (ii) 표준 백업 또는 기록 유지 정책에 따라 고객 개인 데이터를 유지할 수 있습니다. 단, 두 경우 모두 공급자는 (1) 유지된 고객 개인 데이터와 관련하여 본 DPA의 해당 조항의 기밀성을 유지하고 별도로 그러한 조항을 준수하며, (2) 해당하는 그러한 데이터 보호법에 명시된 그러한 목적 및 기간을 제외하고 유지된 고객 개인 데이터를 추가로 처리하지 않습니다.

9. 데이터 보호 영향 평가.

공급자는 데이터 보호법에 따라 고객에게 고객의 의무를 이행하는 데 필요한 합리적인 협력 및 지원을 제공하여 고객의 서비스 사용과 관련된 데이터 보호 영향 평가 또는 유사한 위험 평가를 수행합니다.

DPA 부록

본 부록은 DPA 의 일부를 구성합니다.

부속서 I

A. 당사자 목록

관리자인 고객과 처리자인 공급자 간의 계약에는 다음과 같이 모든 필수 정보에 대한 설명이 포함되어 있습니다.

- 이름, 주소, 담당자 이름
- 직책 및 연락처
- 본 조항에 따라 전송된 데이터와 관련된 활동
- 서명 및 날짜

B. 처리에 대한 설명

1. 개인 데이터가 처리되는 데이터 주체의 범주

고객이 별도로 제공하지 않는 한 처리된 개인 데이터는 다음 범주의 데이터 주체와 관련됩니다.

- 고객의 직원, 계약자, 비즈니스 파트너

2. 처리되는 개인 데이터의 범주

고객은 서비스 사용에 따른 데이터 범주를 결정합니다. 처리되는 개인 데이터는 일반적으로 다음 범주의 데이터와 관련됩니다.

- 고객의 직원이나 고객에 의해 또는 고객을 대신하여 개인 정보가 제공되는 기타 제 3 자와 관련된 고용 세부 정보(회사 이름 및 주소, 직책, 직급, 인구 통계 및 위치 데이터가 포함될 수 있음)
- 고객 시스템 또는 고객이 공급자에게 제공하고 계약에 따라 구매한 서비스와 관련되고 서비스 제공에 필요한 시스템과 관련된 시스템 정보(사용자 ID 및 비밀번호, 컴퓨터 및 도메인 이름, IP 주소, GUID 번호 또는 사용 중인 컴퓨터 또는 기타 장치의 위치가 포함될 수 있음)

본 계약에 따라 처리되는 고객 개인 데이터는 과거, 현재 및 미래의 비즈니스 파트너 또는 그러한 비즈니스 파트너와 관련된 기타 개인과 관련될 수 있습니다.

3. 처리된 민감한 데이터(해당하는 경우)

특수 범주의 개인 데이터(민감한 데이터)는 사례별로 식별되지 않는 한 고객이 제공하면 안 되고, 당사자가 그러한 특수 범주의 데이터에 서비스 조항이 적용된다는 데 동의하는 범위 내에서만 제공합니다.

4. 처리 빈도(예: 데이터가 일회성으로 처리되는지 또는 지속적으로 처리되는지 여부)

서비스를 사용하는 동안 지속적으로 처리됩니다.

5. 처리 성격

a) 소프트웨어 유지 관리 계약에 따라: 소프트웨어가 사용 불가능하거나 예상대로 작동하지 않기 때문에 고객이 지원 티켓을 제출하면 공급자 또는 하위 처리자가 지원을 제공합니다. 이들은 전화를 받고 기본적인 문제 해결을 수행하며 추적 시스템에서 지원 티켓을 처리합니다.

b) 컨설팅 서비스 계약에 따라: 공급자 또는 그 하위 처리자는 서비스 주문에 따라 서비스를 제공합니다.

c) SaaS 소프트웨어 계약에 따라: 고객이 구매한 SaaS 소프트웨어 조항

6. 데이터 전송 및 추가 처리 목적

공급자가 처리하는 고객 개인 데이터에는 다음과 같은 기본 처리 활동이 적용됩니다.

a) 개인 데이터를 사용하여 공급자 서비스를 제공하고 해당하는 경우 계약에 따라 SaaS 소프트웨어에 대한 액세스 및 혜택을 제공하며 고객의 특정 요구 사항에 따라 적절하게 아래 설명된 지침을 모두 준수하여 고객의 요청 시 기술 지원을 제공
b) 개인 데이터의 저장
c) 데이터 전송을 위한 개인 데이터의 컴퓨터 처리
d) 자동화, 트랜잭션 처리 및 기계 학습을 포함하여 공급자 서비스의 일부로 제공되는 서비스 기능의 지속적인 개선
e) 계약에 따른 고객 지시의 실행

다음 추가 처리 활동은 SaaS 소프트웨어에 저장된 모든 개인 데이터에 적용됩니다.

a) 데이터 센터에 개인 데이터 저장(멀티 테넌트 아키텍처)
b) SaaS 소프트웨어에 저장된 고객 개인 데이터의 백업 및 복원
c) 개인 데이터의 컴퓨터 처리(데이터 전송, 데이터 검색, 데이터 액세스 포함)
d) 고객의 사용자에 대한 커뮤니케이션
e) SaaS 소프트웨어에 대한 수정 또는 업그레이드의 릴리스, 개발 및 업로드
f) 개인 데이터 전송을 허용하는 네트워크 액세스
g) 기본 SaaS 소프트웨어 인프라스트럭처 및 데이터베이스 모니터링, 문제 해결 및 관리
h) 보안 모니터링, 네트워크 기반 침입 탐지 지원, 침투 테스트
i) 아래에 설명된 지침에 따라 적절하게 데이터 주체의 요청과 요구에 응답하고 처리하기 위해 필요한 경우

공급자는 제품 개선을 비롯해 새로운 공급자 제품 및 서비스 개발과 관련된 목적으로 익명 데이터(고객 개인 데이터가 아니지만 고객 개인 데이터에서 파생될 수 있음)를 사용할 수 있습니다.

SaaS 소프트웨어 제품의 기능, 개인 데이터 처리 방법, 데이터 저장 위치에 대한 자세한 내용은 해당 제품 설명서 및 보안 가이드에 나와 있습니다.

7. 개인 정보가 유지되는 기간 또는 유지가 불가능한 경우 해당 기간을 정하는 기준

앞서 언급한 개인 데이터는 계약에 따라 그리고 본 DPA 의 섹션 9 를 기준으로 고객이 서비스를 사용하는 동안 처리됩니다.

8. (하위) 처리자에게 전송하는 경우 처리의 주제, 성격 및 기간도 명시

EU SCC 와 관련하여 하위 처리자로의 전송은 본 DPA 에 명시된 것과 동일한 기준에 따릅니다.

9. 지침, 고객 및 공급자 약속.

공급자가 해당 지침이 (1) 법적으로 금지되거나 해당 데이터 보호법의 위반을 초래할 가능성이 있거나 (2) 공급자의 서비스에 대한 중대한 변경이 필요하거나 (3) 본 계약의 조건 또는 본 계약에 따라 판매되는 서비스와 관련된 공급자 문서의 조건과 일치하지 않는다고 생각하지 않는 한 공급자는 고객 개인 데이터와 관련하여 고객으로부터 받은 서면 및 문서화된 지침을 따릅니다. 그러한 경우 공급자는 고객에게 해당 지침을 따를 수 없음을 즉시 알려야 합니다. 계약, 본 DPA 및 공급자의 관련 문서에 있는 모든 처리 설명은 고객의 지시로 간주됩니다.

부속서 II - 기술적 및 조직적 조치에 대한 설명

공급자는 본 계약에 따라 공급자의 고객 개인 데이터 처리에서 보안 사이트(DPA의 섹션 3(a)에 정의됨)에 명시된 적절한 기술적 및 조직적 조치를 사용합니다. 고객은 본 문서에서 동의한 전체 데이터 보호 수준을 실질적으로 감소시키지 않는 한 공급자가 고객 개인 데이터를 보호하기 위해 취하는 조치를 수정할 수 있다는 데 동의합니다.