서비스 부록으로서의 SaaS (Software as a Service)

본 SaaS(Software as a Service, 서비스형 소프트웨어) 부록(이하 "**부록**")은 귀하, 즉 고객(이하 "**고객**" 또는 "**귀하**") 및 공급자 간에 작성되며, 본 부록을 언급하는 귀하와 공급자 간 계약(이하 "**계약**")의 일부가 됩니다. 본 부록에서 사용되는 정의된 용어 중 여기에 달리 정의되지 않은 용어는 계약에 명시된 의미를 지닙니다.

1. **정의.** 문맥이나 계약에 정의되어 있지 않은 대문자로 표기된 용어는 아래에서 부여한 의미를 지닙니다.
   (a) "***적절한 보호조치***"는 아래에 정의된 표준 계약 조항과 같이 EU 위원회에서 채택한 구속력 있는 기업 규칙 또는 표준 정보보호 조항 등 GDPR 제46조에 따른 적절한 보호조치를 의미합니다.
   (b) "***컨트롤러***", "***정보 주체***", "***개인정보***", "***처리***", "***개인정보 침해***", ***"처리자"***, ***"감독 당국"***은 GDPR 제4조에 명시된 의미를 지닙니다.
   (c) "***고객 개인정보***"는 고객이 SaaS 소프트웨어를 사용하여 공급자(처리자로서의 공급자 역할)에게 제공하는 개인정보를 의미합니다.
   (d) ***"정보 보호법"***은 2016년 4월 27일 유럽의회 및 유럽이사회의 (EU) 규정 2016/679(이하 ***"GDPR"***)와 같은 유럽연합의 법률과 규정 및 경우에 따라 GDPR과 유사한 정보 보호 원칙을 시행하고 유럽위원회에서 개인정보 처리에 적용될 수 있는 적절한 수준의 보호조치를 제공하는 것으로 인정한 다른 모든 국가의 법률과 규정을 포함한 모든 법률 및 규정을 의미합니다.
   (e) ***"SaaS 환경"***은 SaaS 소프트웨어 사용과 관련하여 고객에게 액세스 권한이 제공되는 시스템을 의미합니다.
   (f) ***"표준 계약 조항"***이란 유럽 위원회에서 발행한 변경되지 않은 표준 계약 조항(https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914에서 확인 가능)으로, 후속 최종 버전의 2021/914 참조를 의미하며 이 참조는 자동으로 적용됩니다.
   (g) "***하위 처리자***"란 SaaS 소프트웨어와 관련하여 공급자 또는 공급자의 계열사가 고용한 공급자 계열사와 제3자 당사자들을 의미하며 그들은 이 부록에 따라 개인 데이터를 처리합니다.

2. **SaaS 조항.**
   (a) **데이터.** 고객은 SaaS 환경에 데이터를 저장할 수 있습니다. 고객은 SaaS 환경에 저장된 모든 고객 데이터의 수집, 입력, 검증 및 업데이트에 대해 전적인 책임이 있습니다. 고객은 고객 또는 해당 고객 계열사가 위치한 국가 내 및 국외에서 모든 고객 및/또는 제3자 데이터를 사용하고 전송하는 데 필요한 모든 권리, 승인 및 동의를 얻었음을 진술하고 보증합니다(정보처리 및 이전에 대한 적절한 공지를 제공하고 고객의 직원, 고객, 대리인, 계약자로부터 법적으로 충분한 동의 또는 승인을 얻는 것도 포함됨). 고객이 SaaS 소프트웨어로 액세스하기 위해 제3자 웹사이트 또는 기타 장소로 데이터를 전송하는 경우, 공급자가 액세스하는 것에 대해 고객이 그들로부터 동의 및/또는 허가를 받은 것으로 간주됩니다.
   (b) **행위.** 고객은 SaaS 소프트웨어를 사용할 때, (i) 관련 법률을 위반하여 SaaS 소프트웨어를 사용하는 행위(특히 고객은 불법적이거나 제3자의 지식 재산권을 침해하는 콘텐츠 또는 데이터를 전송해서는 안 됨), (ii) SaaS 소프트웨어의 작동 또는 보안을 우회하거나 위험하게 하거나 SaaS 소프트웨어, SaaS 환경 또는 공급자나 공급자의 고객 또는 공급업체의 시스템, 계정, 네트워크의 취약성을 조사, 스캔 또는 테스트하려는 시도, (iii) 원치 않는 대량 메시지 또는 상업용 메시지 전송, (iv) 웜, 트로이 목마, 바이러스, 손상된 파일 또는 이와 유사한 아이템들을 의도적으로 배포하는 행위 등을 수행해서는 안 됩니다. 고객은 SaaS 환경 중단, 보안 문제 및 본 섹션에 대한 위반이 의심되는 사항에 대한 공급자의 합당한 조사에 협조해야 하며, 고객이 본 섹션의 조항을 위반하여 해당 제3자에게 손해를 야기했다고 주장하는 제3자의 모든 청구, 소송 또는 조치(***"제3자 청구"***)로부터 공급자와 그 계열사를 자체 비용 부담으로 보호해야 합니다. 또한 고객은 제3자 청구와 관련하여 도달한 모든 판결 또는 합의 비용뿐만 아니라 제3자 청구에 대한 공급자의 대응 비용을 지불해야 합니다.
   (c) **중지.** 공급자는 SaaS 소프트웨어의 지속적인 사용이 SaaS 소프트웨어, 다른 공급자 고객 또는 제3자의 권리에 손해를 야기하게 되어 그로 인한 피해를 방지하기 위해서는 즉각적인 조치가 요구되거나, 고객이 위의 행동 섹션을 위반할 가능성이 충분히 있는 경우 피해를 방지하기 위해 SaaS 소프트웨어에 대한 고객의 액세스를 일시적으로 제한하거나 중지할 수 있습니다. 공급자는 지체 없이 제한 또는 일시 중지에 대해 고객에게 통보할 것입니다. 상황이 허락하는 경우, 고객에게 서면 또는 이메일로 사전에 통지할 것입니다. 공급자는 해당 상황에서 합리적으로 가능한 시간과 범위 내에서 일시 중지 또는 제한 사항을 한정하고, 일시 중지 또는 제한을 야기한 문제가 해결되면 즉시 액세스를 복원하고 고객에게 복원에 대해 통지할 것입니다.
   (d) **가용성.** 공급자는 예정된 유지보수, 업데이트 설치, 공급자의 합리적인 통제를 벗어난 요인, 공급자가 고객에게 전달한 최소 시스템 요구 사항을 고객이 충족하지 못하는 경우, SaaS 소프트웨어의 가용성에 영향을 미치는 고객의 계약 또는 본 부록에 대한 위반 행위를 제외하고 SaaS 소프트웨어를 하루 24시간, 주 7일 사용할 수 있도록 상업적으로 합당한 노력을 기울일 것입니다. 공급자는 예정된 유지보수에 대해 고객에게 합당한 사전 통지를 제공합니다.

3. **SaaS 보안.**
   (a) **일반 보안 정책**. 공급자는 고객 데이터(개인정보 포함)의 보안 및 기밀성을 중요하게 생각합니다. 공급자는 정보 보안 관행을 유지 및 개선하고 보안 위험에 대한 노출을 최소화하기 위해 최선을 다하고 있습니다. 그에 따른 공급자의 정보 보안 관행, 데이터 유출 대응 방침, 기술적 및 조직적 조치, 소프트웨어 개발 보안 관행에 대한 자세한 내용은 www.oneidentity.com/legal/security.aspx(이하 총칭하여 "보안 사이트")에서 확인할 수 있습니다. 고객은 공급자가 제공된 전반적인 보호 수준을 크게 낮추지 않는 한 보안 사이트를 수정할 수 있다는 데 동의합니다.

(b) **데이터 센터 보안 및 위치**. 공급자는 상용 호스팅 공급자를 사용하여 SaaS 환경을 호스팅합니다. SaaS 환경을 위한 해당 호스팅 공급자는 하위 처리자로 식별됩니다. 공급자는 업계 표준 보안 요구 사항을 충족하고 SOC(서비스 조직 제어) 감사, SSAE 18 감사 및/또는 ISO 인증과 같은 보안 절차에 대한 독립적인 평가를 받는 호스팅 공급자만을 사용합니다. 공급자는 요청 시 호스팅 공급자의 인증서 사본을 제공할 것입니다. 고객에게는 SaaS 소프트웨어의 초기 구성 시 SaaS 환경이 호스팅될 지리적 지역을 선택할 수 있는 옵션이 제공됩니다. 일단 선택되면 공급자는 고객의 사전 동의 없이 지리적 지역을 변경하지 않습니다.

(c) **데이터 기밀성.** 공급자는 특히 고객 개인정보를 포함하여 계약에 따라 "기밀"로 간주되는 데이터의 기밀성을 잘 알고 있는 직원만 그러한 데이터를 처리하도록 합니다. 공급자는 본 부록 및 계약에 따라 SaaS 소프트웨어를 지원하는 모든 공급자 직원에게 고객 개인정보를 포함한 정보 보호와 관련된 기밀 유지 계약을 체결하도록 요구합니다. 공급자는 해당 직원의 고용 종료 후에도 그러한 기밀 유지 의무가 지켜지도록 할 것입니다. 공급자는 데이터 보안, 데이터 개인정보 요구 사항 및 원칙에 따라 고객 개인정보를 비롯한 데이터에 액세스할 수 있는 개인을 정기적으로 교육합니다.

(d) **제한된 처리 및 공개.** 공급자는 고객의 개인 데이터를 포함한 데이터를 (i) 계약과 일치하는 목적을 위해 그리고 이 부록의 조건에 따라, 또는 (ii) 처리자가 따라야 하는 소환장, 사법 또는 행정 명령에 대한 응답을 포함하여 연합 또는 회원국 법률에서 요구하는 바에 따라 처리하거나 계열사 법인들에게 공개할 수 있습니다. 그러한 경우, 처리자는 해당 법률이 공익을 중요한 근거로 하여 그러한 정보를 금지하지 않는 한 처리하기 전에 해당 법적 요구 사항을 통제자에게 알려야 합니다.

4. **협조.** 법률 또는 계약에 의해 금지된 경우를 제외하고, 공급자는 고객의 요청이 있을 시 정보 주체 요청에 대해 고객에게 합당한 협조를 해야 하며 본 계약에 따라 정보가 제공된 정보 주체로부터 (a) 해당 정보 주체의 개인정보에 대한 액세스, 정정, 수정 또는 삭제 권한 요청, (b) 본 계약에 따른 개인정보 처리 반대; 및/또는 (c) GDPR에 따른 개인정보 이동권 또는 잊힐 권리에 대한 행사 희망 중 어느 하나를 요청 받는 경우 즉시 고객에게 통지합니다. 공급자는 정보 주체의 요청이 고객에게 제대로 전달되었는지 확인하기 위한 경우를 제외하고는 고객의 사전 서면 승인 없이 해당 정보 주체의 요청에 응답하지 않을 것입니다.

5. **감사 권한**. 고객의 요청과 계약의 기밀 유지 의무에 따라 공급자는 본 부록에 따른 의무 준수를 입증하는 데 합리적으로 필요한 정보를 고객에게 제공하고 공급자의 개인정보 처리와 관련하여 고객의 비용으로 고객(또는 제3자 감사인)이 수행한 검사를 포함한 감사를 허용하고 이에 협조합니다.

6. **국제 데이터 전송.** SaaS 소프트웨어 및 관련 서비스의 제공이 GDPR 또는 해당 데이터 보호법의 적용을 받는 개인 데이터를 GDPR 제 45조에 따라 유럽 위원회에서 충분한 데이터 보호를 제공하는 국가 또는 국가들("***제3국***")로 전송하는 것이 포함된 경우, 그리고 GDPR 또는 해당 데이터 보호법에 따라 필요한 적절성 수단이 표준 계약 조항을 체결하여 충족될 수 있는 경우에, 공급자(또는 공급자를 대신하는 공급자 계열사)는 데이터 수령자인 각 하위 처리자와 표준 계약 조항을 체결합니다. 표준 계약 조항의 모듈 3(처리자에서 처리자로)은 이러한 전송에 적용됩니다. 이러한 이전과 관련된 모든 목적을 위해 이 부록의 첨부는 표준 계약 조항의 첨부를 구성합니다.

7. **하위 처리자.**

(a) 고객은 공급자가 SaaS 소프트웨어의 제공과 관련하여 공급자의 계열사 및 제3자 공급자를 하위 처리자로 고용할 수 있음을 인정하고 이에 동의합니다.

(b) 공급자는 고객과 공급자 간의 본 부록의 조항 및 본 문서의 지침에 따라 하위 처리자와 적절한 서면 계약을 체결합니다. 이 부록에 명시된 것과 동일한 데이터 보호 의무가 모든 하위 처리자에게 부과됩니다.

(c) 공급자는 공급자가 고용한 하위 처리자가 본 부록을 위반시 하위 처리자로 인해 발생한 범위까지만 책임을 집니다.

(d) 공급자는 고객이 이용할 수 있는 제품별 하위 처리자의 목록을 웹페이지(https://support.oneidentity.com/subprocessor)에서 관리하고 있습니다. 신규 하위 처리자에게 개인정보에 대한 액세스 권한을 부여하기 최소 십(10) 영업일 전에 공급자는 하위 처리자 목록을 업데이트하고 고객에게 해당 업데이트에 대한 통지를 받을 수 있는 방법을 제공합니다. 공급자가 처리자인 경우 다음 조건이 적용됩니다.

i) 고객이 신규 하위 처리자를 승인하지 않는 경우, 고객은 통지 기간이 끝나기 전에 비승인 사유에 대한 설명이 포함된 서면 해지 통지서를 제공하여 위약금 없이 해당 SaaS 소프트웨어의 구독을 해지할 수 있습니다.

ii) 바로 위에 설명된 해지 후에도 고객은 주문 또는 기타 계약 의무에 따라 요구되는 모든 지불을 이행할 의무가 있으며 파트너 및/또는 공급자로부터 어떠한 결제 대금도 환불 받거나 반환받을 수 없습니다.

8. **개인정보 침해 통지.** 보안 사이트에 명시된 의무 외에도 공급자는 개인정보 침해를 인지한 후 지체 없이 고객에게 통지하고 정보 보호법에 따라 요구되는 대로 고객이 개인정보 침해를 보고해야 하는 의무를 이행할 수 있도록 보유하고 있는 합당한 정보를 제공합니다. 공급자는 그러한 정보를 이용할 수 있게 되는 대로 단계적으로 제공할 수 있습니다. 공급자는 그러한 개인정보 침해의 원인을 파악하기 위해 선의의 노력을 기울이고, 공급자의 합리적인 통제 범위 내에서 개인정보 침해의 원인을 해결하기 위해 필요하고 합리적이라고 판단하는 조치를 취하는 데 동의합니다.

9. **고객 개인정보의 반환 및 삭제.**

(a) 고객은 어떠한 의도의 이유에서든 고객 개인정보를 고객에게 반환하거나 삭제하고자 한다면 SaaS 기간이 만료되거나 조기 종료되기 최소 삼십(30) 일 전에 공급자에게 통지해야 합니다. 고객 개인정보를 반환하도록

요청 받는 경우 공급자는 일반적으로 사용되는 형식으로 관련 법률에서 허용하는 범위까지 고객 개인정보를 반환해야 합니다.

(b) 고객이 SaaS 기간 종료 후에 고객의 개인 데이터 반환을 요청하지 않는 한, 공급자는 공급자가 법적 또는 규제 당국의 명령이나 요구 사항을 준수하기 위해 허용되는 필요한 한도를 제외하고 공급자가 보유한 고객 개인 데이터를 삭제해야 합니다.

10. **정보 보호 영향 평가.** 공급자는 GDPR에 따라 고객의 SaaS 소프트웨어 사용과 관련된 정보 보호 영향 평가를 수행해야 하는 고객의 의무를 이행하는 데 필요한 합당한 협조와 지원을 고객에게 제공합니다.

부록의
첨부

이 첨부는 부록의 일부를 구성합니다.

보충서 I

A. 당사자 목록

통제자인 고객과 처리자인 공급자 간의 계약에는 다음과 같은 모든 필수 정보 내역이 포함되어 있습니다.

- 이름, 주소, 담당자 이름,
- 직위와 연락처,
- 이 조항에 따라 전송된 데이터와 관련된 활동, 그리고
- 서명 및 날짜.

B. 처리에 대한 설명

1. 개인 데이터가 처리 대상이 되는 데이터 주체의 범주

달리 고객이 제공하지 않는 한, 처리된 개인 데이터는 SaaS 소프트웨어에 저장된 개인 데이터를 가지고 있는 직원, 하청업체, 비즈니스 파트너 또는 기타 개인 등과 같은 범주의 데이터 주체들과 관련이 있습니다.

2. 처리되는 개인 데이터의 범주

고객은 SaaS 소프트웨어 사용 때마다 데이터 범주를 결정합니다. 처리되는 개인 데이터는 다음의 데이터 범주와 관련이 있습니다.

- 고객에 의해 또는 고객을 대신하여 개인 정보가 제공되는 고객 또는 기타 제3자의 직원과 관련된 고용 세부 정보(회사 이름 및 주소, 직위, 등급, 인구 통계 및 위치 데이터 포함 가능),
- 고객 시스템 또는 고객이 공급자에게 제공하고 본 계약에 따라 구매한 서비스와 연관된 시스템으로 SaaS 소프트웨어 제공에 필요한 시스템 정보(사용자 ID 및 암호, 컴퓨터 및 도메인 이름, IP 주소, 사용 중인 GUID 번호 또는 컴퓨터나 기타 사용 장치의 위치 포함 가능).

본 계약에 의거하여 처리되는 고객 개인 데이터는 과거, 현재 및 가망 비즈니스 파트너 또는 그러한 비지니스 파트너와 관련된 개인과 연관될 수 있습니다.

3. 처리되는 민감한 데이터(해당되는 경우)

특별 범주의 개인 데이터(GDPR 9조에 정의됨)는 사례별로 식별되지 않는 한 고객이 제공해서는 안 되며 당사자들이 그러한 특수 범주의 데이터가 SaaS에 의해 보호된다고 동의하는 경우에만 제공됩니다.

4. 처리의 빈도(예: 데이터가 일회성으로 아니면 연속적으로 처리되는지 여부).

SaaS 소프트웨어 사용 기간 동안 지속적으로 처리함.

5. 처리의 속성

고객이 구매한 형태의 서비스 제공.

6. 데이터 전송 및 추가 처리의 목적

공급자가 처리하는 고객 개인정보에는 다음과 같은 기본 처리 활동이 적용됩니다.

- 계약에 따라 SaaS 소프트웨어에 대한 액세스 및 SaaS 소프트웨어 혜택을 제공하고 고객의 요청에 따라, 그리고 고객의 특정한 요구 상항에 따라, 적절한 경우, 아래에 설명된 지시에 따라 고객의 개인 데이터 사용,
- 데이터 센터(멀티 테넌트 구조 – 복수 사용자 구조)에 고객의 개인 데이터를 저장,
- SaaS 소프트웨어에 저장된 고객 개인 데이터의 백업 및 복구,
- 데이터 전송, 데이터 검색, 데이터 액세스를 포함한 고객 개인정보의 컴퓨터 처리.
- 고객의 사용자에 대한 커뮤니케이션,
- SaaS 소프트웨어에 대한 수정 또는 업그레이드의 릴리스, 개발 및 업로드,
- 개인 데이터 전송을 허용하는 네트워크 액세스,
- 기본 SaaS 소프트웨어 인프라 및 데이터베이스를 모니터링 하고, 문제를 해결하고 및 관리,
- 보안 모니터링, 네트워크 기반 침입 탐지 지원, 침입 테스트,
- 계약 및 이 부록에 따라 고객의 지시 이행, 그리고
- 데이터 주체의 요청 및 요구에 적절하게 응답하고 바로 아래에 설명된 지침에 따라 처리하는 데 필요한 만큼.

공급자는 제품 개선 및 신규 공급자 제품과 서비스의 개발과 관련된 목적으로 익명화된 데이터(고객 개인정보가 아니지만 고객 개인정보에서 파생될 수 있음)를 사용할 수 있습니다.

제품의 용도, 개인 데이터를 처리하는 방법 및 데이터 저장 위치에 대한 자세한 내용은 해당 제품 문서 및 보안 가이드에 나와 있습니다.

7. 개인 데이터가 보존되는 기간 또는 이것이 불가능한 경우 해당 기간을 결정하는 데 사용되는 기준

앞서 언급한 개인 데이터는 계약에 따라, 그리고 본 부록의 섹션 9에 의거하여 고객이 SaaS 소프트웨어를 사용하는 동안 처리됩니다.

8. **(하위) 처리자로 전송하는 경우 처리의 주제 사안, 속성 및 기간을 명시하십시오.**
표준 계약 조항과 관련하여 하위 처리자로의 이전은 이 부록에 명시된 것과 동일한 기준에 따릅니다.

9. **지침, 고객 및 공급자의 약속.**
계약, 본 부록, 공급자의 관련 SaaS 소프트웨어 문서의 정보 처리에 대한 설명은 고객 및 공급자의 지침으로 간주되어야 합니다. 공급자는 고객 개인정보와 관련하여 고객으로부터 받은 서면 및 문서화된 지침을 따릅니다. 단, 공급자의 관점에서 그러한 지침이 (1) 법적으로 금지되거나 적용 가능한 정보 보호법을 위반하게 될 가능성이 높거나, (2) 공급자의 SaaS 소프트웨어에 대한 중대한 변경이 요구되거나, (3) 본 문서에 따라 판매되는 SaaS 소프트웨어와 관련된 계약 또는 공급자의 문서 조항과 모순되는 경우는 제외됩니다. 이러한 경우 공급자는 해당 지침을 따를 수 없음을 고객에게 즉시 통지해야 합니다.

보충서 II – 기술적 및 조직적 수단에 대한 설명

공급자는 본 계약에 따른 고객의 개인 데이터 처리에 있어 보안 사이트(부록의 섹션 3(a)에 정의됨)에 명시된 적절한 기술적 및 조직적 수단을 사용합니다. 고객은 공급자가 본 문서에서 합의된 전반적인 정보 보호 수준을 실질적으로 경감시키지 않는 한 고객 개인정보를 보호하기 위해 취한 조치를 수정할 수 있다는 데 동의합니다.