정보 처리 계약

본 정보 처리 계약(이하 "계약")은 Siemens Industry Software로도 알려진 Siemens Product Lifecycle Management Software Inc.(이하 "SISW")와 본 계약 조건에 수락의 의사표시를 한 고객(이하 "고객") 간에 체결한다. SISW는 본 계약에 따른 모든 권리를 추구하고 의무를 이행하는 데 있어서 계열사를 활용할 수 있는 권한을 보유한다. 따라서, 여기에 사용된 "SISW"라는 용어는 Siemens Product Lifecycle Management Software Inc.의 최종 모회사가 직, 간접적으로 소유하거나 통제하고 있으며, Siemens Product Lifecycle Management Software Inc.로부터 SISW 클라우드 서비스(이하 "클라우드 서비스")를 배포할 수 있는 권한을 부여받은 계열사를 의미할 수 있다.

고객은 정보 유형의 결정 및 처리에 의해 영향을 받는 개인들에 대하여 단독으로 책임을 지며, 클라우드 서비스를 수단으로 하는 그러한 처리의 합법성을 보장하여야 한다. 고객은 또한 클라우드 서비스가 제공하는 기능을 사용한 개인 정보의 정정, 삭제 또는 차단에 대한 책임을 져야 한다. 고객은 클라우드 서비스가 제공하는 기능을 사용하여 개인 정보를 포함한 자신의 정보를 내보내기 및 삭제할 수 있다. 본 정보 처리 계약이 종료된 후 30일 이내에 고객은 SISW에 서면 요청을 보내서 고객이 고객 정보를 다운로드 할 수 있도록 해달라고 요청할 수 있다. 이러한 요청에 대한 응답으로 SISW가 정한 임의의 기간이 만료된 후, 고객의 잔존 정보는 삭제 대상이 되며 더 이상 고객이 사용할 수 없다. SISW와 고객은 클라우드 서비스의 범위 내에서, 고객이 클라우드 서비스가 제공하는 기능을 사용함으로써만 지시를 발행할 수 있는 권한을 행사할 수 있다는 데 동의한다. 고객 정보에 관한 추가 지시는 해당 지시를 수행하기 위해 고객이 지불해야 하는 추가 비용에 대한 합의를 포함하여 SISW과 고객 사이의 별도 서면 계약이 필요하다. 고객은 클라우드 서비스에 보호되는 건강정보(PHI)를 업로드하거나 저장하지 않을 것을 서약한다. 단, 고객과 SISW가 클라우드 서비스에 PHI의 저장을 명시적으로 허용하는 별도의 서면 계약을 체결하는 경우는 예외로 한다.

클라우드 서비스를 제공함에 있어서 생산 시스템과 관련하여, SISW는 본 정보 처리 계약의 첨부 A의 부록 2에 규정된 기술적, 체계적 조치에 따라야 한다. 클라우드 서비스와 관련된 비생산 시스템은 첨부 A의 부록 2에 규정된 조치를 준수할 수도 있고, 그렇지 않을 수도 있다. 또한 SISW는 생산 시스템에 적용할 기술적, 체계적 조치를 수시로 변경할 수 있다. 단, 그러한 변경이 해당 조치에 의해 제공되는 보호의 수준에 심각하게 부정적인 영향을 주지 않는 경우에 한한다. SISW는 직원이 승인없이 개인 정보를 수집, 처리 혹은 사용하는 것을 제한하고, 정보의 개인 정보 보호 요구 사항을 준수하도록 구체적으로 지시된 직원만을 고용하여 고객의 개인 정보를 처리도록 한다.

SISW는 클라우드 서비스의 수행에 있어서 하청업체를 고용할 권한이 있다. 고객의 개인 정보에 대한 하청업체의 액세스가 배제될 수 없는 경우에 한하여, SISW는 요청에 따라 고객에게 이러한 하청업체의 목록과 그 각각의 위치를 제공하며, 새로운 하청업체에게 고객의 개인 정보에 대한 액세스를 부여하기 전에 해당 목록을 업데이트 한다. 고객이 합리적으로 새로운 하청업체에 대해 이의가 있는 경우, 고객은 그러한 이의에 대하여 SISW에게 통보하고, SISW가 새로운 하청업체의 개입을 계속 주장할 경우, 정당한 이유로 본 정보 처리 계약을 해지할 권한을 가진다. 이러한 하청업체의 도입이 개인 정보의 국경 간 이동을 포함할 경우, SISW는 그러한 하청업체가 개인 정보에 대한 정보 보호의 적절한 수준을 유지하도록 노력한다.

SISW는 정기적으로 해당 기술적, 체계적 조치에 대한 준수 여부를 검증하고, 고객의 합리적인 요청이 있는 경우 고객에게 기술적, 체계적 조치가 준수되고 있음을 확인하여 준다. 고객이 SISW에서 발급한 확인이 잘못되었다고 생각하는 합리적인 이유가 있을 경우, 고객은 합리적인 사전 통지에 따라 SISW와 감사 일정을 잡고 기술적, 체계적 조치에 대한 준수를 확인할 권리를 가진다. 이러한 감사는 고객의 비용으로 수행되어야 한다.

SISW와 고객은 유럽 연합(EU) 국가들에서 EU가 개인 정보 보호 수준이 적절하지 않은 것으로 간주하는 EU 외부 국가들로 고객의 개인 정보를 전송할 경우, 동 전송이 EU의 표준 계약 조항에 따라 수행될 것에 동의하며, 해당 본문은 첨부 A에 명시되어 있으며 완전하게 본 계약에 통합된다. 본 정보 처리 계약과 표준 계약 조항의 조건이 상충하는 경우, 표준 계약 조항의 규정이 우선한다. 표준 계약 조항에는 정보 송신자(첨부 A에 정의됨)가 설립된 EU 회원국의 법률이 적용된다.

첨부 A

EU 표준 계약 조항

적절한 수준의 정보 보호를 보장하지 않는 제3국에 있는 처리업체로 개인정보를 전송하는 것에 관한 95/46/EC 지침의 제26조(2)항의 목적에 있어서,

고객 및/또는 유럽 연합(EU)에 소재한 고객의 제휴사

(이하, **"정보 송신자"**)

및

Siemens Industry Software로도 알려진 Siemens Product Lifecycle Management Software Inc.의 최종 모회사가 직, 간접적으로 소유하거나 통제하고 있으며 Siemens Product Lifecycle Management Software Inc.에 의하여 그를 대신하여 정보를 처리할 권한을 부여받은 계열사를 포함한 Siemens Product Lifecycle Management Software Inc.

(이하, **"정보 수신자"**)

각각 "당사자", 통칭하여 "양당사자"는

부록 1에 명시된 개인 정보를 정보 송신자가 정보 수신자에게 전송함에 있어서, 개인 정보 보호 및 개인의 기본 권리 및 자유와 관련하여 적절한 보호조치를 제시할 수 있도록 다음 계약 조항(이하 "본 조항")에 합의하였다.

제1절. 정의

본 조항의 목적상

(a) '개인 정보(personal data)', 특별한 범주의 정보(special categories of data)', '처리(process/processing)', '통제자(controller)', '처리업체(processor)', '정보 주체(data subject)' 및 '감독 기관(supervisory authority)'은 1995년 10월 24일 자 유럽 의회 및 위원회의 개인 정보의 처리 및 해당 정보의 자유로운 이전과 관련된 개인 보호에 관한 지침 95/46/EC와 동일한 의미를 가진다.

(b) '정보 송신자'란 개인 정보를 통제하는 자로, 개인 정보를 전송한다.

(c) '정보 수신자'란 정보 송신자로부터 개인 정보를 전송 받은 후 정보 송신자의 지시 및 본 조항의 조건에 따라 정보 송신자를 대신해 개인 정보를 처리하는 데 합의한 정보 처리업체를 의미하며, EU

개인정보 보호지침 95/46/EC의 제25조(1)항의 의미 내에서 적절한 보호를 보장하는 제3국 제도에 적용을 받지 아니하는 자이다.

(d) '하청업체'란 정보 수신자 또는 정보 수신자의 다른 하청업체로부터 정보 송신자의 개인 정보를 전송받은 후 정보 송신자의 지시, 본 조항의 조건 및 서면 하청 계약서의 조건에 따라 정보 송신자를 위해 정보 처리 작업만 하기로 합의한 업체로, 정보 수신자 또는 정보 수신자의 다른 하청업체에 의해 고용된 처리업체를 의미한다.

(e) '해당 개인정보 보호법'이란 개인의 기본 권리 및 자유, 특히 정보 송신자가 있는 회원 국가의 정보 통제자에게 적용되는 개인 정보 처리와 관련된 사생활권을 보호하는 법을 의미한다.

(f) '기술적, 체계적 보안 조치'란 특히, 정보 처리가 네트워크를 통한 전송과 관련된 경우 우발적 또는 불법적 파기, 우발적 손실, 변경, 무단 공개 또는 액세스 및 기타 모든 불법적 형태의 처리로부터 개인 정보를 보호하기 위한 조치를 의미한다.

제2절. 전송 세부 사항

전송 세부 사항 및 특히, 특별한 범주의 개인 정보(해당되는 경우)는 본 조항과 일체를 이루는 부록 1에 명시되어 있다.

제3절. 제3자 수혜자 조항

1. 정보 주체는 제3자 수혜자로서 정보 송신자에 대하여 본 조항, 제4(b)~(i)항, 제5(a)~(e)항 및 (g)~(j)항, 제6(1)항 및 (2)항, 제7항, 제8(2)항, 제9~12항을 적용할 수 있다.

2. 정보 주체는 정보 수신자에 대하여 정보 송신자가 사실상 사라졌거나 법률적으로 더 이상 존재하지 않을 경우에 본 조항, 제5(a)~(e)항 및 (g)항, 제6항, 제7항, 제8(2)항, 제9~12항을 적용할 수 있다. 단, 후임 업체가 계약 또는 법적 규정에 의해 정보 송신자의 모든 법적 책임을 지고 정보 송신자의 권리와 의무를 지게 된 경우, 정보 주체는 해당 업체에게 이러한 조항을 적용할 수 있다.

3. 정보 송신자와 정보 수신자 둘 다 사실상 없어지거나 법적으로 더 이상 존재하지 않거나 파산한 경우, 정보 주체는 하청업체에게 본 조항, 제5(a)~(e)항 및 (g)항, 제6항, 제7항, 제8(2)항, 제9~12항을 적용할 수 있다. 단, 후임 업체가 계약 또는 법적 규정에 의해 정보 송신자의 모든 법적 책임을 지고 정보 송신자의 권리와 의무를 떠맡게 된 경우, 정보 주체는 해당 업체에게 이러한 조항을 적용할 수 있다. 이러한 하청업체의 제3자 책임은 본 조항에 따른 해당 업체의 자체 처리 작업에 제한된다.

4. 양당사자는 정보 주체가 명백하게 원하고, 국내법이 허용한다면, 협회 또는 기타 단체가 정보 주체를 대리하는 것에 반대하지 아니한다.

제4절. 정보 송신자의 의무

정보 송신자는 다음 사항에 동의하고 보증한다.

(a) 전송 자체를 포함하는 개인 정보의 처리는 해당 정보 보호 법률의 관련 조항에 따라 수행되어 왔고 계속 수행될 것이며(해당하는 경우, 정보 송신자가 설립된 회원국의 관련 당국에 통지되어 왔고), 해당 국가의 관련 규정을 위반하지 아니한다.

(b) 정보 수신자에게 오직 정보 송신자를 위하여 전송된 개인 정보를 해당 정보 보호 법률과 본 조항들에 따라 처리하도록 지시하여 왔고, 개인 정보 처리 서비스의 기간 동안에 그렇게 계속 지시할 것이다.

(c) 정보 수신자가 본 계약의 부록 2에 명시된 기술적, 체계적 보안 조치에 관해 충분한 보장을 제공한다.

(d) 해당 정보 보호 법률의 요구 사항을 평가한 후, 보안 조치는 특히 네트워크를 통한 정보 전송을 수반하는 처리의 경우 우발적이거나 불법적인 파괴나 우발적 손실, 변경, 무단 공개 혹은 액세스에 대하여, 그리고 모든 불법적 형태의 처리에 대하여 개인 정보를 보호하기에 적합하며, 이러한 조치들은, 첨단 기술과 구현 비용에 있어서, 처리에 의한 리스크와 보호될 정보의 특성에 적합한 보안 수준임을 보장한다.

(e) 보안 조치를 준수한다.

(f) 전송이 정보의 특별 범주를 수반하는 경우, 정보 주체는 지침 95/46/EC의 의미에서 적절한 보호를 제공하지 않는 제3국으로 해당 정보가 전송되기 전 혹은 전송된 직후 최대한 신속하게 그러한 정보 전송에 대해 통보를 받아 왔거나 또는 통보를 받게 될 것이다.

(g) 정보 송신자가 전송을 계속하거나 중지를 해제하기로 결정한 경우, 제5(b)항 및 제8(3)항에 따라 정보 수신자 또는 하청업체로부터 받은 통지를 정보 보호 감독 당국에 전달한다.

(h) 정보 주체가 요구할 경우 본 조항들의 사본을 이용할 수 있도록 하되, 부록 2, 보안 조치의 요약 설명 및 본 조항들에 따라 만들어야 하는 하청 처리 서비스를 위한 계약은 예외로 한다. 단, 본 조항들 혹은 계약이 상업적 정보를 포함한 경우는 그러한 상업적 정보를 삭제할 수 있다.

(i) 하청 처리의 경우, 본 조항들에 따른 정보 수신자로서 처리 행위는 제11조에 따라 개인 정보와 정보 주체의 권한에 대해 최소한 동일한 수준의 보호를 제공하는 하청업체에 의하여 수행된다.

(j) 제4(a)~(i)항에 따른 준수를 보장한다.

제5절. 정보 수신자의 의무

정보 수신자는 다음 사항에 동의하고 이를 보증한다.

(a) 오직 정보 송신자를 위하여 그 지시와 본 조항들에 따라 개인 정보를 처리하며, 여하한 이유로 준수할 수 없을 경우, 즉각 이를 정보 송신자에게 통보하며, 이 경우 정보 송신자는 정보의 전송 중지 및/또는 계약을 종료할 권한을 가진다.

(b) 정보 수신자에게 적용되는 법은 정보 송신자로부터 받은 지시와 본 계약에 따른 의무 이행을 방해하지 않는다. 해당 법이 변경되어 본 조항에 명시된 의무와 보증에 상당한 역효과를 미칠 가능성이 높은 경우 이 사실을 인지하는 즉시 정보 송신자에게 통지할 것이며, 이 경우 정보 송신자는 정보의 전송 중지 및/또는 계약을 종료할 권한을 가진다.

(c) 전송된 개인 정보를 처리하기 전에 부록 2에 규정된 기술적, 체계적 보안 조치들을 실시하였다.

(d) 다음의 경우 정보 송신자에게 즉시 통지한다.

(i) 법집행 기관에 의한 법적으로 구속력 있는 개인 정보 공개 요청(단, 형사 조사 시 기밀 정보를 유지해야 하는 형법에 따른 금지 등과 같이 달리 금지된 경우는 제외)
(ii) 우발적 또는 무단 액세스
(iii) 정보 주체로부터 직접 받은 요청(요청에 응할 수 있도록 허가 받은 경우가 아니어서 요청에 응하지 아니한 경우)

(e) 전송 대상인 개인 정보의 처리와 관련하여 정보 송신자로부터 받은 모든 질의를 즉시 적절하게 처리하고, 전송된 정보의 처리와 관련된 감독 기관의 조언을 준수한다.

(f) 본 조항에 따른 처리 작업의 감사를 위해 정보 송신자가 요청할 경우, 정보 처리 시설을 제공한다. 이러한 감사는 정보 송신자 또는 기밀 유지 의무가 있는 전문 자격을 소유하고 있고 정보 송신자가 선정한 외부 회원으로 구성된 검사 기관에 의해 실시되며, 해당될 경우 감독 기관과 협의한다.

(g) 정보 주체가 요청할 경우 본 조항의 사본 또는 하청에 대한 기존 계약서를 제공한다. 단, 본 조항들이나 계약에 상업적 정보가 포함된 경우, 그러한 상업적 정보는 삭제할 수 있으며, 정보 주체가 정보 송신자로부터 사본을 얻을 수 없는 경우 부록 2는 보안 조치 요약본으로 대체한다.

(h) 하청 처리를 할 경우, 정보 송신자에게 사전에 통보하고 사전 서면 동의를 획득한다.

(i) 하청업체에 의한 처리 서비스는 제11항에 따라 수행된다.

(j) 정보 송신자에게 본 조항들에 따라 체결한 하청업체 계약의 사본을 신속하게 송부한다.

제6절. 책임

1. 양당사자는 제3항 혹은 제11항에 언급된 의무를 한 당사자 혹은 하청업체가 위반한 결과, 손해를 입은 정보 주체가 겪은 손해에 대하여 정보 송신자로부터 보상을 받을 권한이 있다는 데 동의한다.

2. 정보 송신자가 사실상 없어졌거나 법적으로 더 이상 존재하지 않거나 파산했기 때문에 정보 수신자 또는 그 하청업체가 제3항 또는 제11항과 관련된 의무를 위반하여 발생한 손해에 대해 정보 주체가 정보 송신자에게 상기 1항에 따른 보상을 청구할 수 없는 경우, 정보 수신자는 정보 주체가 정보 수신자가 정보 송신자인 것처럼 정보 수신자에게 보상을 청구할 수 있음에 동의한다. 단, 후임 업체가 계약 또는 법적 규정에 의해 정보 송신자의 모든 법적 책임을 지게 된 경우, 정보 주체는 이러한 권리를 해당 업체에게 행사할 수 있다.

   정보 수신자는 하청업체의 의무 위반을 핑계로 자신의 책임을 회피할 수 없다.

3. 정보 송신자와 정보 수신자 둘 다 사실상 없어졌거나 법적으로 더 이상 존재하지 않거나 파산했기 때문에 하청업체가 제3항 또는 제11항과 관련된 의무를 위반하여 발생한 손해에 대해 정보 주체가 정보 송신자 또는 정보 수신자에게 상기 1항 및 2항에 따른 보상을 청구할 수 없는 경우, 하청업체는 정보 주체가 하청업체가 정보 송신자 또는 정보 수신자인 것처럼 하청업체에게 본 조항에 따른 하청업체의 자체 처리 작업과 관련해 보상을 청구할 수 있음을 동의한다. 단, 후임 업체가 계약 또는 법적 규정에 의해 정보 송신자 또는 정보 수신자의 모든 법적 책임을 지게 된 경우, 정보 주체는 이러한 권리를 해당 업체에게 행사할 수 있다. 하청 처리업체의 책임은 본 조항에 따른 업체의 자체 처리 작업으로 제한된다.

제7절. 조정 및 관할권

1. 정보 수신자는 정보 주체가 정보 수신자에 대해 제3자 수혜권 및/또는 본 조항에 따른 청구 보상을 제기할 경우, 정보 수신자가 아래와 같은 정보 주체의 결정을 수락할 것에 동의한다.

(a) 독립적 제3자 또는 감독 기관(해당될 경우)에 분쟁에 대한 조정을 회부한다.

(b) 정보 송신자가 있는 회원 국가의 법원에 분쟁을 회부한다.

2. 양당사자는 정보 주체에 의한 선택이 국내 또는 국제 법률의 다른 규정에 따라 구제를 추구할 실질적 또는 절차적 권리를 침해하지 않을 것에 동의한다.

제8절. 감독 기관과의 협력

1. 정보 송신자는 해당 정보 보호법에 따라 요구되거나 요청이 있는 경우, 해당 감독 기관에 본 계약의 사본을 맡길 것에 동의한다.

2. 양당사자는 감독 기관이 정보 송신자 및 그 하청업체에 대하여 감사를 실시할 권리가 있음에 동의하고, 이러한 감사는 해당 정보 보호법에 따라 정보 송신자의 감사에 적용되는 것과 동일한 범위를 가지며, 그와 동일한 조건을 적용한다.

3. 정보 수신자는 제2항에 따라 정보 수신자 혹은 하청업체의 감사 수행을 금지하는 그 자신 또는 하청업체에게 적용될 법률의 존재에 관하여 정보 송신자에게 신속하게 통보하여야한다. 이러한 경우에 정보 송신자는 제5(b)항에서 규정된 조치를 취할 권리를 가진다.

제9절. 준거법

본 조항들에는 정보 송신자가 설립된 회원국의 법을 적용한다.

제10절. 계약의 변경

당사자는 본 조항들을 변경 혹은 수정하지 않을 것에 약속한다. 이는 당사자들이 필요한 경우 본 조항과 모순되지 않는 범위에서 업무와 관련한 조항을 추가하는 것을 제한하지 아니한다.

제11절. 하청 처리

1. 정보 수신자는 정보 송신자의 사전 서면 동의 없이 본 조항들에 따라 정보 송신자를 위하여 수행하는 처리 작업을 하청하지 아니한다. 정보 수신자가 본 조항들에 따라 정보 송신자의 동의를 얻어 의무를 하청하는 경우, 본 조항들에 따라 정보 수신자에게 부과되는 것과 동일한 의무를 하청업체에게 부과하는 서면 계약을 하청업체와 체결하는 방식으로 하도록 한다. 하청업체가 그러한 서면 계약에 따른 정보 보호 의무를 이행하지 못하는 경우, 정보 수신자는 그러한 계약에 따른 하청업체의 수행에 대하여 정보 송신자에게 완전히 책임을 져야 한다.

2. 정보 송신자 또는 정보 수신자가 사실상 없어졌거나 법적으로 더 이상 존재하지 않거나 파산했으며, 계약 또는 법적 규정에 의해 정보 송신자 또는 정보 수신자의 모든 법적 책임을 지는 후임 업체가 없기 때문에 정보 주체가 정보 송신자 또는 정보 수신자에게 제6(1)항에 따른 보상을 청구할 수 없는 경우, 정보 수신자와 하청업체 간 사전 서면 계약은 또한 제3항에 규정된 제3자 수혜자 조항을 제공한다. 이러한 하청업체의 제3자 책임은 본 조항에 따른 업체의 자체 처리 작업으로 제한된다.

3. 제1항에 언급된 계약의 하청 처리에 대한 정보 보호 측면에 관한 규정은 정보 송신자가 설립된 회원국의 법을 적용한다.

4. 정보 송신자는 본 조항에 의하여 체결되고 제5(j)항에 따라 정보 수신자에 의하여 통보된 하청 처리 계약의 목록을 보관하며, 적어도 일년에 한 번 업데이트한다. 이 목록은 정보 송신자의 정보 보호 감독 기관이 사용할 수 있어야 한다.

제12절. 개인 정보 처리 서비스 해지 후 의무

1. 양당사자들은 정보 처리 서비스 제공의 종료 시 정보 송신자의 선택에 따라 정보 수신자 및 하청업체는 전송된 모든 개인 정보와 그에 대한 사본을 정보 송신자에게 반환하거나, 모든 개인 정보를 파기하고 그렇게 했음을 정보 송신자에게 증명하는 데 동의한다. 단, 정보 송신자에게 부과된 법률이 전송된 개인 정보의 전부 혹은 부분을 반환 혹은 파기하는 것을 금지하는 경우는 예외로 한다. 이 경우, 정보 수신자는 전송된 개인 정보의 기밀성을 보장하며, 전송된 개인 정보를 더 이상 적극적으로 처리하지 아니할 것을 보증한다.

2. 정보 수신자 및 하청업체는 정보 송신자 및/또는 감독 기관의 요청에 따라, 제1항에 언급된 조치의 감사를 위한 정보 처리 시설을 제출할 것을 보증한다.

표준 계약 조항 부록 1

정보 송신자
정보 송신자는 다음과 같다(정보 전송과 관련한 작업에 대해 여기에 간단히 기재):

고객은 SISW에 의해 제공되는 클라우드 서비스의 구독자로서, 고객에 의해 승인된 최종 사용자는 고객 정보를 입력, 수정, 사용, 삭제, 다운로드 및 다른 방식으로 처리할 수 있으며, 이러한 정보에는 본 계약과 클라우드 서비스를 위한 관련 서류에 명시된 개인 정보가 포함된다.

정보 수신자
정보 수신자는 다음과 같다(정보 전송과 관련한 작업에 대해 여기에 간단히 기재):

Siemens Product Lifecycle Management Software Inc.는 자사 및/또는 그 하청업체에 의하여 다음이 포함되는 클라우드 서비스를 제공한다. 클라우드 서비스가 운영되는 미국 및 유럽 연합에 컴퓨팅 인프라를 유지하며, 고객에 의해 클라우드 서비스에 업로드되는 고객 정보를 인프라에 저장하고, 클라우드 서비스 및 인프라 시설의 가용성 및 현재 운영 상황을 모니터링하며, 본 계약서 및 클라우드 서비스를 위한 관련 문서에 명시된 인프라의 보안을 유지한다.

정보 주체
전송되는 개인 정보는 다음과 같은 범주의 정보 주체와 관련되어 있다(구체적으로 명시):

정보 송신자에 의하여 명시적으로 서면에 의해 지정되지 않은 경우, 정보주체는 클라우드 서비스를 사용하도록 고객에 의하여 권한을 부여받은 최종 사용자와 클라우드 서비스에 개인정보가 저장된 고객의 다른 직원을 포함한다.

정보 범주
전송되는 개인 정보는 다음과 같은 범주의 정보와 관련되어 있다(구체적으로 명시):

클라우드 서비스에 저장된 구체 정보 범주는 고객에 의한 중요설정에 따르지만, 클라우드 서비스에 저장될 수 있는 일반적인 정보 범주의 비제한적 예시는 다음과 같다: 이름, 이메일 주소, 회사명, 전화 번호, 직장 위치, 국적 또는 시민권, 클라우드 서비스의 접근 및 사용에 관한 정보. 클라우드 서비스의 고객 설정에 따라, 기타 많은 정보 범주가 고객 정보에 존재할 수 있다.

특별한 범주의 정보(해당되는 경우)
전송된 개인 정보는 다음과 같은 특별한 범주의 정보와 관련되어 있다(구체적으로 명시):

클라우드 서비스에 저장될 특별 정보 범주는 본 계약 또는 주문서에서 양 당사자 사이에 합의된 대로이거나, 클라우드 서비스의 제공의 일환으로 고객에게 제공되는 전문 서비스를 위한 업무기술서에 명시된 대로 한다.

처리 작업

전송되는 개인 정보에는 다음과 같은 기본 처리 작업이 적용된다(구체적으로 명시):

개인 정보는 다음과 같이 처리될 수 있다. 클라우드 서비스의 정상 동작의 일부로서, 고객의 설정에 따라 처리, 단일 테넌트 또는 멀티 테넌트 환경에서 정보 송신자에 의해 유지되는 컴퓨팅 인프라에 저장 및/또는 보관을 통하여 처리; 혹은 클라우드 서비스를 사용하는 고객이 지정한 최종 사용자에 의해 클라우드 서비스에 발행된 지시에 따라 액세스되거나 또는 전송되어 처리; 정보 송신자에 의해 수행되는 클라우드 서비스 유지 보수 작업의 일환으로 처리.

표준 계약 조항 부록 2

일부 클라우드 서비스 제공은 해당되는 경우 주문서에 명시된 다른 조건에 따라 제공된다. 그렇지 않으면, 정보 수신자는 제4(d)항 및 제5(c)항에 따라, 시스템에 저장된 개인 정보에 대하여 아래 명시한 기술적, 체계적 조치를 취한다.

제4(d)항 및 제5(c)항에 따른 정보 수신자에 의해 실행되는 기술적, 체계적 보안 조치의 설명:

1. 물리적 액세스 제어. 승인되지 않은 사람은 개인 정보를 처리 및/또는 사용하는 정보 처리 시스템이 위치한 소재지, 건물이나 공간에 물리적 접근이 금지된다.

   조치: 모든 정보 센터는 보안 요원, 감시 장치, 모션 감지기, 액세스 제어 메커니즘 및 장비와 정보 센터 설비가 기능을 제대로 발휘할 수 있도록 하는 기타 조치에 의해 실행되는 보안 절차를 엄격하게 준수한다. 승인된 담당자만 정보 센터 시설 내 시스템과 인프라에 대한 액세스를 할 수 있다. 적절한 기능을 보장하기 위하여, 물리적 보안 설비(예: 모션 센서, 카메라 등)는 정기적으로 유지보수 한다. 구체적으로는, 다음의 물리적 보안 조치가 모든 정보 센터에서 구현된다.

   a. 일반적으로, 건물은 액세스 제어 시스템(스마트 카드 액세스 시스템)을 통해 보안된다.
   b. 전자 액세스 배지(직원, 벤더, 또는 계약자마다 고유함) 및 PIN 등의 인증 자격 증명이 정보 센터 시설에 물리적으로 액세스하기 위하여 승인된 직원에게 제공된다.
   c. 시스템 경계 내에서 정보 센터에 물리적으로 액세스하는 것은 전자 액세스 제어 시스템에 의해 집행되며, 빌딩과 룸 입구에는 카드 리더기와 PIN 패드를 설치하고, 빌딩과 룸 출구에는 카드 리더기만을 설치한다.
   d. 보안 분류에 따라, 건물, 개별 지역 및 주변 부지는 추가 조치에 의해 더 보호된다. 여기에는 특정 액세스 프로필, 비디오 감시, 침입자 경보 시스템과 생체 인식 액세스 제어 시스템이 포함된다.
   e. 액세스 권한은 아래에 명시된 시스템 및 정보 액세스 제어 조치에 따라 개별적으로 승인된 직원에게 부여된다. 이는 또한 방문자 액세스에도 적용된다. SISW 빌딩의 손님과 방문객은 리셉션에 이름을 등록하고 승인된 SISW 직원을 동반해야 한다. SISW 및 모든 제3자 정보 센터 서비스 제공자는 정보 센터 내에서 SISW의 사적 영역에 진입하는 사람의 이름과 시간을 기록한다.
   f. SISW 직원 및 외부 인사는 모든 SISW 위치에서 자신의 ID 카드를 착용해야한다.

2. 시스템 액세스 제어. 클라우드 서비스를 제공하기 위해 사용되는 정보 처리 시스템은 승인없이 사용되는 것이 금지되어야 한다.

   조치:

   a. SISW 또는 그 하청업체는 NIST SP 800-53 Rev 4 액세스 제어(AC) 및 식별과 인증(IA) 요건을 준수하도록 환경을 관리한다.
   b. 복수의 인증 수준을 사용하여 개인 정보를 저장 및 처리하는 것을 포함하는 민감한 시스템에 대한 액세스를 부여한다. 승인된 사용자만 사용자를 추가, 삭제 또는 수정할 수 있도록 하는 적절한 권한을 가지도록 보장하는 프로세스가 준비되어 있다.
   c. 모든 사용자는 고유한 사용자 이름 및 특정한 최소 복잡성 기준을 충족하는 암호로 SISW의 시스템에 액세스한다.
   d. SISW 및 그 하청업체는 요청된 승인 변경을 가이드라인(예: 승인없이 어떠한 권한도 부여 불가)에 따라 실행하도록 보장하는 적절한 절차를 가지고 있다. SISW 사용자가 직책을 변경하거나 회사를 떠날 때, 환경에 대한 액세스 권한을 취소하는 과정이 수행된다.
   e. SISW 및 하청업체는 암호 공개를 금지하고, 암호가 공개될 경우 어떻게 해야 하는지 정하며, 모든 사용자의 암호를 정기적으로 변경하도록 요구하고 기본 설정 암호를 변경하도록 요구하는 암호 정책을 수립하였다. 개인화된 사용자 ID가 인증을 위해 할당된다. 모든 암호는 최소 복잡성 요구 사항을 충족해야 하며 암호화 된 형태로 저장된다. 도메인 암호의 경우, 시스템은 최소

복잡성 요구 사항을 준수하여 60일마다 암호 변경을 강제한다. 각 SISW 컴퓨터는 암호로 보호된 화면 보호기가 있다.

f. SISW 또는 그 하청업체는 자동으로 다음 계정 이벤트를 감사한다. 즉, 생성, 수정, 활성화, 비활성화 및 제거이다. 시스템 관리자는 로그를 주기적으로 검토한다.
g. SISW 및 그 하청업체의 네트워크는 방화벽에 의해 공개 인터넷으로부터 보호된다.
h. SISW 및 그 하청업체는 회사 네트워크, 전자 메일 계정 및 모든 파일 서버와 워크 스테이션에 대한 액세스 포인트에 최신 안티 바이러스 소프트웨어를 사용한다.
i. SISW 및 그 하청업체는 관련 보안 업데이트의 배포를 보장하기 위해 보안 패치 관리를 실행한다.
j. SISW의 기업 네트워크 및 중요 인프라에 대한 완전한 원격 액세스는 강력한 다중 요소 인증에 의해 보호된다.

3. 정보 액세스 제어. 정보 처리 시스템을 사용할 권한이 있는 직원은 액세스 권한이 있는 개인 정보에 대해서만 액세스하며, 처리, 사용 및 저장의 과정에서 개인 정보를 승인 없이 읽거나, 복사하거나, 수정하거나 삭제해서는 안 된다.

조치:

a. 개인, 기밀 혹은 민감 정보에 대한 액세스는 알 필요가 있는가의 기준으로 부여한다. 즉, 직원 또는 외부 제3자는 그들의 작업을 완료하기 위해 필요한 정보에 액세스한다. SISW는 어떻게 권한이 할당되고 어떤 권한이 할당되는가를 문서화하는 인증 개념을 사용한다. 모든 개인, 기밀 또는 다른 민감 정보는 SISW 보안 정책 및 표준에 따라 보호된다.
b. SISW 클라우드 서비스의 모든 제품 서버는 해당 정보 센터에서 운영된다. 개인, 기밀 혹은 기타 민감 정보를 처리하는 응용 프로그램을 보호하는 보안 조치가 정기적으로 점검된다. 이를 위해, SISW는 이러한 조치가 적절한 방식으로 적용되는지 확인하는 정기적인 외부 감사를 수행한다.
c. SISW는 SISW에 의해 승인받지 않은 개인 소프트웨어 혹은 기타 소프트웨어를 클라우드 서비스를 위해 사용되는 시스템에 설치하도록 허용하지 않는다.
d. 정보 저장 매체의 고장으로 인해 정보를 이전해야 할 필요가 있을 경우, 그러한 이전이 완료된 후, 고장난 저장 매체는 자장을 제거하거나(자기 저장장치의 경우) 혹은 파쇄한다(고체 또는 광 스토리지의 경우).

4. 정보 전송 제어. 개인 정보는 전송 중 승인없이 읽거나, 복사, 수정 혹은 삭제할 수 없다.

조치:

a. SISW 또는 그 하청업체는 NIST SP 800-53 Rev 4 시스템 및 통신 보호(SC) 요구사항을 준수하기 위해 인프라 및 설정을 관리한다. 여기에는 인프라의 외부 경계에서 악성 통신을 방지하기 위한 시스템 경계에서의 네트워크 기반 침입 차단 시스템(NIPS) 및 방화벽이 포함된다. NIPS 및 방화벽은 DISA STIG 표준에 따라 구성된다. 정보는 FIPS 140-2를 준수하는 암호화 모듈을 사용하여 전송 중에 암호화된다.
b. 정보 캐리어가 물리적으로 전송되는 경우, 합의된 서비스 수준(예: 암호화, 및 납내장 컨테이너)을 보장하기 위하여 적절한 조치가 SISW에서 구현된다.
c. SISW 내부 네트워크에서 개인 정보의 전송은 SISW의 보안 정책에 따른 기타 기밀 정보와 동일한 방식으로 보호된다.
d. 정보가 SISW 및 고객 간에 전송되는 경우, 전송된 개인 정보를 위한 보호 조치는 본 계약 또는 클라우드 서비스에 대한 관련 문서에 명시된 대로 한다. 이것은 물리적 및 네트워크 기반의 정보 전송에 모두 적용된다. 고객은 SISW의 분계점에서부터 정보 전송에 대한 책임을 진다(예: 클라우드 서비스를 호스팅하는 정보 센터의 송신 방화벽).

5. 정보 입력 제어. 클라우드 서비스는 클라우드 서비스를 제공하기 위하여 사용된 인프라에서 개인정보가 입력, 수정 혹은 제거되는지의 여부 및 누구에 의하여 이루어지는가를 소급적으로 확인할 수 있도록 허용한다.

조치:

a. SISW는 승인된 직원만 그들의 작업의 과정에서 필요에 따라 개인 정보에 액세스하도록 허용한다. SISW는 클라우드 서비스에 의하여 지원될 수 있는 최대 범위까지 SISW 또는 하청업체에 의한 개인 정보의 입력, 수정 및 삭제 혹은 블록킹을 위한 로깅 시스템을 실행하였다.
b. 허가받지 않은 활동이나 오작동이 발생하거나 의심되는 경우 사건의 재구성을 촉진하는 데 필요한 충분한 세부 사항을 감사 추적을 통해 제공한다. 각 운영 시스템 이벤트 로그 기록에는 이벤트 유형, 타임 스탬프, 이벤트 소스, 이벤트 위치, 이벤트의 결과 및 그 이벤트와 관련된 사용자가 포함된다.

6. 작업 제어. 개인 정보는 전적으로 계약 조항 및 고객이 제공하는 관련 지시에 따라 처리된다.

조치:
a. SISW는 SISW와 고객, 하청업체, 또는 다른 서비스 제공자 사이의 계약 준수를 보장할 수 있는 제어 및 프로세스를 사용한다.
b. 고객 정보에는 SISW 정보 분류 기준에 따라 최소한 기밀 정보와 동일한 보호 수준이 적용된다.
c. 모든 SISW 직원과 계약 파트너는 SISW 고객 및 파트너의 영업 비밀을 포함한 모든 민감한 정보의 기밀성을 존중하도록 계약적으로 구속된다.

7. 가용성 관리. 개인 정보는 실수로 또는 무단으로 파괴 또는 손실되는 것으로부터 보호된다.

조치:
a. SISW는 필요한 경우 비즈니스 중요 시스템의 신속한 복구를 보장하는 백업 프로세스와 다른 조치를 채용한다.
b. SISW는 정보 센터에 전력 가용성을 보장하기 위해 글로벌 클라우드 서비스 제공자에 의존한다.
c. SISW는 클라우드 서비스를 위한 비상 계획뿐만 아니라 비즈니스 및 재해 복구 전략을 마련하였다.

8. 정보 분리 제어. 다른 목적을 위해 수집된 개인 정보는 별도로 처리될 수 있다.

조치:
a. 적용 가능한 경우, SISW는 고객의 개인 정보와 기타 고객의 개인 정보 사이에 정보 분리를 실현하기 위하여 배포된 소프트웨어(예: 멀티 테넌시 또는 개별 시스템 랜드스케이프)의 기술 능력을 사용한다.
b. SISW는 각 고객에 대한 전용 인스턴스(논리적 또는 물리적 분리)를 유지한다.
c. 고객(고객의 계열사 포함)은 자신의 고객 인스턴스에 액세스할 수 있다.

9. 정보 완전성 제어. 처리 활동을 하는 동안, 개인정보가 그대로, 완전하게 현재 상태로 유지되는 것을 보장한다.

조치: SISW는 무단 변경에 대한 보호를 위한 여러 계층의 방어 전략을 구현하였다. 이는 전술한 제어 및 조치 부분에서 언급한 제어를 말한다. 방화벽의 설정은 공공 및 민간 액세스를 분리하는 복수의 네트워크 세그먼트에서 발생한다. 각 방화벽 규칙 세트는 이러한 세그먼트 사이에 허용된 통신을 명시하여 특정 액세스를 제어한다.

a. 보안 모니터링 센터: 자동 침입 탐지 소프트웨어는 다른 보안 예방 및 포렌직 소프트웨어 및 프로세스와 함께 사용되어, 알림, 조사 및 필요할 경우, 보안 사고의 복원을 위한 통지 및 지원을 하게 된다.
b. 안티 바이러스 소프트웨어: 모든 시스템은 바이러스, 웜, 트로이 목마 및 다른 형태의 맬웨어로부터 보호하기 위해 구성된 최신 바이러스 백신을 구현한다.
c. 백업 및 복구: 모든 시스템은 기본 수준의 정보와 구성에 대한 백업 스냅샷을 제공한다. 해당하는 경우, SISW 및 하청업체는 정보가 서로 충분한 거리의 두 개의 별개의 정보 센터에 저장되도록 보장하는 높은 가용성 구성을 통해 고객의 인스턴스를 운영한다.
d. 보안 조치를 증명하는 정기적인 외부 감사. SISW 및 하청업체는 위의 보안 조치를 테스트하기 위해 정기적인 외부 감사를 받는다.