PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

1. BACKGROUND

1.1 Purpose.

This document is a data processing agreement ("**DPA**") between SAP and Customer and applies to Personal Data provided by Customer and each Data Controller in connection with their use of the Cloud Service. It states the technical and organizational measures SAP uses to protect Personal Data that is stored in the production system of the Cloud Service.

1.2 Application of the Standard Contractual Clauses Document.

If processing of Personal Data involves an International Transfer, the Standard Contractual Clauses apply as stated in Section 5 and are incorporated by reference.

1.3 Governance.

Except as provided in Section 5.2, Customer is solely responsible for administration of all requests from other Data Controllers. Customer will bind any other Data Controller it permits to use the Cloud Service to the terms of this DPA.

2. APPENDICES

Customer and its Data Controllers determine the purposes of collecting and processing Personal Data in the Cloud Service. Appendix 1 states the details of the processing SAP will provide via the Cloud Service. Appendix 2 states the technical and organizational measures SAP applies to the Cloud Service, unless the Agreement states otherwise.

3. SAP OBLIGATIONS

3.1 Instructions from Customer.

SAP will follow instructions received from Customer (on its own behalf or on behalf of its Data Controllers) with respect to Personal Data, unless they are (i) legally prohibited or (ii) require material changes to the Cloud Service. SAP may correct or remove any Personal Data in accordance with the Customer's instruction. If SAP cannot comply with an instruction, it will promptly notify Customer (email permitted).

3.2 Data Secrecy.

To process Personal Data, SAP and its Subprocessors will only use personnel who are bound to observe data and telecommunications secrecy under the Data Protection Law. SAP and its Subprocessors will regularly train individuals having access to Personal Data in data security and data privacy measures.

3.3 Technical and Organizational Measures.

SAP 클라우드 서비스에 관한 개인 정보 처리 계약

1. 배경

1.1 목적.

본 문서는 SAP 와 고객 간의 정보 처리 계약("**DPA**")으로, 고객과 각 정보 컨트롤러가 그들의 클라우드 서비스 이용과 관련하여 제공하는 개인 정보에 적용됩니다. 이는 SAP 가 클라우드 서비스의 운영 시스템에 저장된 개인 정보를 보호하기 위해 사용하는 기술적/조직적 조치를 기술합니다.

1.2 표준 계약 조항 문서의 적용.

개인 정보의 처리에 국제 전송이 포함되는 경우, 제 5 항에 명시되어 있고 참조로 통합되어 있는 바와 같이 표준 계약 조항이 적용됩니다.

1.3 거버넌스.

제 5.2 조에 명시된 바를 제외하고, 고객은 다른 데이터 컨트롤러의 모든 요청을 전적으로 관리할 책임이 있습니다. 고객은 자신이 본 DPA 조건에 따라 클라우드 서비스를 이용하도록 허용하는 다른 데이터 컨트롤러에 대해 구속력을 지닙니다.

2. 부록

고객과 그 데이터 컨트롤러는 본 클라우드 서비스에 저장되는 개인 정보를 수집, 처리 및 다른 방식으로 사용하는 목적을 결정합니다. 부록 1 은 SAP 가 클라우드 서비스를 통해 제공하는 처리의 세부 사항을 기술합니다. 부록 2 는 계약에 달리 명시되어 있지 않는 한, SAP 가 클라우드 서비스에 적용하는 기술적/조직적 조치를 기술합니다.

3. SAP 의무

3.1 고객의 지침.

SAP 는 해당 지침이 (i) 법적으로 금지되어 있거나, (ii) 클라우드 서비스에 중요한 변경을 요하지 않는 한 (자신 또는 그 데이터 컨트롤러를 대신하여) 고객으로부터 받은 지침을 준수합니다. SAP 는 고객의 지침에 따라 개인 정보를 수정하거나 제거할 수 있습니다. 지침을 준수할 수 없는 경우, SAP 는 고객에게 신속하게 통지합니다(이메일도 허용됨).

3.2 정보 비밀 유지.

개인 정보를 처리하기 위해 SAP 와 그 협력업체는 정보 보호 법률에 따른 정보 및 통신 비밀 유지를 준수할 책임이 있는 인력만을 이용합니다. SAP 와 그 협력업체는 정보 보안 및 데이터 보호에 관해 개인 정보에 액세스하는 개인을 정기적으로 교육합니다.

3.3 기술적, 조직적 조치.

(a) SAP will use the appropriate technical and organizational measures stated in Appendix 2.

(b) Appendix 2 applies to the production system of the Cloud Service. Customer should not store any Personal Data in non-production environments.

(c) SAP provides the Cloud Service to SAP's entire customer base hosted out of the same data center and receiving the same Cloud Service. Customer agrees SAP may improve the measures taken in Appendix 2 in protecting Personal Data so long as it does not diminish the level of data protection.

3.4 Security Breach Notification.

SAP will promptly inform Customer if it becomes aware of any Security Breach.

3.5 Cooperation.

At Customer's request, SAP will reasonably support Customer or any Data Controller in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data.

4. SUBPROCESSORS

4.1 Permitted Use.

(a) Customer and Data Controllers authorize SAP to subcontract the processing of Personal Data to Subprocessors. SAP is responsible for any breaches of the Agreement caused by its Subprocessors.

(b) Subprocessors will have the same obligations as SAP does as a Data Processor (or Subprocessor) with regard to their processing of Personal Data.

(c) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection. Subprocessors may have security certifications that evidence their use of appropriate security measures. If not, SAP will regularly evaluate each Subprocessor's security practices as they relate to data handling.

(d) If Customer requests, SAP will inform Customer of the name, address and role of each Subprocessor it uses to provide the Cloud Service.

4.2 New Subprocessors.

SAP's use of Subprocessors is at its discretion, provided that:

(a) SAP 는 부록 2 에 기술되어 있는 적절한 기술적/조직적 조치를 이용합니다.

(b) 부록 2 는 클라우드 서비스의 운영 시스템에 적용됩니다. 고객은 개인 정보를 비운영 환경에 저장해서는 안 됩니다.

(c) SAP 는 동일한 데이터 센터에서 호스팅되고 동일한 클라우드 서비스를 받는 SAP 의 전체 고객 기반에 클라우드 서비스를 제공합니다. 고객은 정보 보호의 수준을 약화시키지 않는 한, 개인 정보를 보호함에 있어 SAP 가 부록 2 에서 취하는 조치를 개선할 수 있다는 점에 동의합니다.

3.4 보안 위반 통지.

SAP 는 보안 위반을 알게 된 경우 즉시 이를 고객에게 통지합니다.

3.5 협력.

고객이 요청할 경우, SAP 는 고객 또는 데이터 컨트롤러가 정보 주체의 요청을 처리하는 업무 또는 SAP 의 개인 정보 처리와 관련한 규제 당국의 업무를 합리적으로 지원합니다.

4. 협력업체

4.1 허가된 사용.

(a) 고객과 데이터 컨트롤러는 개인 정보의 처리를 협력업체에 하청할 수 있는 권한을 SAP 에 부여합니다. SAP 는 자신의 협력업체로 인해 발생하는 본 계약의 위반에 대해 책임이 있습니다.

(b) 협력업체는 개인 정보의 처리와 관련하여 데이터 처리자(또는 협력업체)로서 SAP 가 지닌 것과 동일한 의무를 지닙니다.

(c) SAP 는 협력업체를 선택하기 전에 협력업체의 보안, 개인정보 보호 및 비밀 유지 관행을 평가합니다. 협력업체에는 그들이 적절한 보안 조치를 사용한다는 것을 증명하는 보안 인증서가 있을 수 있습니다. 인증서가 없을 경우, 각 협력업체의 보안 관행이 데이터 처리와 관련되기 때문에 SAP 는 이러한 관행을 정기적으로 평가합니다.

(d) 고객이 요청할 경우, SAP 는 클라우드 서비스를 제공하기 위해 사용하는 각 협력업체의 이름, 주소 및 역할을 고객에게 통지합니다.

4.2 신규 협력업체.

SAP 의 협력업체 이용은 SAP 의 재량에 따라 결정되며, 다음과 같은 조건이 적용됩니다.

(a) SAP will notify Customer in advance (by email or by posting on the Support Portal) of any changes to the list of Subprocessors in place on the Effective Date (except for Emergency Replacements or deletions of Subprocessors without replacement).

(b) If Customer has a legitimate reason that relates to the Subprocessors' processing of Personal Data, Customer may object to SAP's use of a Subprocessor, by notifying SAP in writing within thirty days after receipt of SAP's notice. If Customer objects to the use of the Subprocessor, the parties will come together in good faith to discuss a resolution. SAP may choose to: (i) not use the Subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the Subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the Agreement on thirty days' written notice. If Customer does not object within thirty days of receipt of the notice, Customer is deemed to have accepted the new Subprocessor.

(c) If Customer's objection remains unresolved sixty days after it was raised, and SAP has not received any notice of termination, Customer is deemed to accept the Subprocessor.

4.3 Emergency Replacement.

SAP may change a Subprocessor where the reason for the change is outside of SAP's reasonable control. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible. Customer retains its right to object to a replacement Subprocessor under Section 4.2(b).

5. INTERNATIONAL TRANSFERS

5.1 Limitations on International Transfer.

Personal Data from an EEA or Swiss Data Controller(s) may only be exported or accessed by SAP or its Subprocessors outside the EEA or Switzerland (**"International Transfer"**):

(a) If the recipient, or the country or territory in which it processes or accesses Personal Data, ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission; or

(a) SAP 는 효력 발생일에 실행 중인 협력업체 목록에 변경을 하는 경우 사전에 (이메일 또는 지원 포털에 게시를 통해) 고객에게 통지합니다(긴급 교체 또는 교체 없이 협력업체와의 계약을 해지하는 경우 제외).

(b) 고객에게 협력업체의 개인 정보 처리와 관련한 합법적인 사유가 있는 경우, 고객은 SAP 로부터 통지를 받은 후 30 일 이내에 SAP 에 서면으로 통지하여 SAP 가 협력업체를 이용하는 것에 이의를 제기할 수 있습니다. 고객이 협력업체 이용에 이의를 제기하는 경우, 당사자들은 함께 성실하게 해결책을 논의합니다. SAP 는 (i) 협력업체를 이용하지 않거나, (ii) 고객이 이의를 제기하면서 요청한 시정 조치를 취한 후 협력업체를 이용하는 것 중에서 선택할 수 있습니다. 이러한 옵션들이 합리적으로 가능하지 않거나, 고객이 계속해서 합법적인 사유로 이의를 제기할 경우, 당사자 중 일방은 30 일 서면 통지를 통해 계약을 해지할 수 있습니다. 고객이 통지를 받은 후 30 일 이내에 이의를 제기하지 않는 경우, 고객은 새로운 협력업체를 허용하는 것으로 간주됩니다.

(c) 고객의 이의가 제기된 후 60 일까지 해결되지 않은 상태로 남아 있고, SAP 가 해지 통지를 받지 않은 경우, 고객은 협력업체를 허용하는 것으로 간주됩니다.

4.3 긴급 교체.

SAP 는 변경의 사유가 SAP 의 합리적 통제를 벗어난 경우 협력업체를 변경할 수 있습니다. 이 경우, SAP 는 가능한 빨리 고객에게 협력업체 교체를 통지합니다. 고객은 제 4.2(b)항에 따라 교체 협력업체에 대한 이의를 제기할 권한이 있습니다.

5. 국제 전송

5.1 국제 전송의 제한사항.

EEA 또는 스위스 데이터 컨트롤러의 개인 정보는 다음과 같은 경우 EEA 또는 스위스 밖에서 SAP 또는 그 협력업체에 의해서만 수출 또는 액세스할 수 있습니다(**"국제 전송"**).

(a) 수혜자 또는 개인 정보를 처리하거나 개인 정보에 액세스하는 국가나 지역이 유럽위원회의 결정에 따라 개인 정보의 처리와 관련하여 데이터 주체의 권리와 자유가 적절한 수준임을 확인하는 경우

(b) in accordance with Section 5.2

5.2 Standard Contractual Clauses and Multi-tier Framework.

(a) The Standard Contractual Clauses apply where there is an International Transfer to a country that does not ensure an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data as determined by the European Commission.

(b) For Third Country Subprocessors, SAP has entered into the unchanged version of the Standard Contractual Clauses prior to the Subprocessor's processing of Personal Data. Customer hereby (itself as well as on behalf of each Data Controller) accedes to the Standard Contractual Clauses between SAP and the Third Country Subprocessor. SAP will enforce the Standard Contractual Clauses against the Subprocessor on behalf of the Data Controller if a direct enforcement right is not available under Data Protection Law.

(c) Nothing in this DPA will be construed to prevail over any conflicting clause of the Standard Contractual Clauses.

6. CERTIFICATIONS AND AUDITS

6.1 Customer Audits.

Customer or its independent third party auditor may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:

(a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 attestation report. Upon Customer's request -SOC Audit reports or ISO certifications are available through the third party auditor or SAP;

(b) A Security Breach has occurred;

(c) Customer or another Data Controller has reasonable grounds to suspect that SAP is not in compliance with its obligations under this DPA;

(d) An audit is formally requested by Customer's or another Data Controller's data protection authority; or

(b) 제 5.2 항에 따른 경우

5.2 표준 계약 조항 및 다층 프레임워크.

(a) 유럽위원회의 결정에 따라 개인 정보의 처리와 관련하여 데이터 주체의 권리와 자유가 적절한 수준임을 확인하지 않는 국가로 국제 전송을 하는 경우 표준 계약 조항이 적용됩니다.

(b) 제 3 국 협력업체의 경우, SAP 는 협력업체가 개인 정보를 처리하기 전에 변경되지 않은 버전의 표준 계약 조항을 체결했습니다. 이에 고객(본인 및 각 데이터 컨트롤러를 대신하여)은 SAP 와 제 3 국 협력업체 간 표준 계약 조항에 응합니다. 정보 보호 법률에 따라 직접적인 집행권을 행사할 수 없는 경우, SAP 는 데이터 컨트롤러를 대신하여 협력업체에 대해 표준 계약 조항을 집행합니다.

(c) 본 DPA 의 어떠한 내용도 표준 계약 조항의 상충하는 조항에 우선하는 것으로 해석되지 않습니다.

6. 인증 및 감사

6.1 고객 감사.

고객 또는 독립적인 제 3 자 감사인은 다음의 경우에만 SAP 가 처리한 개인 정보와 관련하여 SAP 의 제어 환경과 보안 관행에 대한 감사를 실시할 수 있습니다.

(a) (i) ISO 27001 또는 기타 표준에 따른 인증서(범위는 인증서에 정의) 또는 (ii) 유효한 ISAE3402 및/또는 ISAE3000 인증 보고서 제출을 통해 클라우드 서비스의 운영 시스템을 보호하는 기술적/조직적 조치의 준수 여부에 대한 충분한 증거를 SAP 가 제시하지 않은 경우. 고객의 요청 시, 제 3 자 감사인 또는 SAP 를 통해 SOC 감사 보고서 또는 ISO 인증서를 이용할 수 있습니다.

(b) 보안 위반 발생 시

(c) SAP 가 본 DPA 에 따른 의무를 준수하지 않았다고 의심할만한 합리적 근거를 고객이나 다른 데이터 관리자가 가진 경우

(d) 고객 또는 다른 데이터 컨트롤러의 데이터 보호 당국이 정식으로 감사를 요청한 경우

(e) Mandatory Data Protection Law provides Customer with a direct audit right.

Where Customer audits SAP's environment, SAP will reasonably support Customer in its audit processes.

6.2 Audit Restrictions.

The Customer audit will be limited to once in any twelve month period, and limited in time to a maximum of 3 business days and scope as reasonably agreed in advance between the parties. Reasonable advance notice of at least sixty days is required, unless Data Protection Law requires earlier audit. SAP and Customer will use current certifications or other audit reports to minimize repetitive audits. Customer and SAP will each bear their own expenses of audit, unless the Customer is auditing under Section 6.1 (c) (unless such audit reveals a breach by SAP in which case SAP shall bear its own expenses of audit), 6.1 (d) or 6.1 (e). In those cases, Customer will bear its own expense and the cost of SAP's internal resources required to conduct the audit. If an audit determines that SAP has breached its obligations under the Agreement, SAP will promptly remedy the breach at its own cost.

7. EU ACCESS

7.1 Optional Service.

If included in the Order Form, SAP agrees to provide EU Access for the eligible Cloud Service as stated in this Section 7.

7.2 EU Access.

SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service.

7.3 Data Center Location.

Upon the Order Form Effective Date, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. SAP will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If SAP plans to migrate the Customer instance to a data center within the EEA or to Switzerland, SAP will notify Customer in writing (email permitted) no later than thirty days before the planned migration.

7.4 Exclusions.

The following Personal Data is not subject to the requirements in 7.2-7.3:

(a) Contact details of the sender of a support ticket;

(e) 의무적 정보 보호 법률에 따라 고객에게 직접 감사권이 부여된 경우

고객이 SAP 의 환경을 감사하는 경우, SAP 는 고객의 감사 절차를 합리적으로 지원합니다.

6.2 감사 제한사항.

고객 감사는 12 개월에 한 번으로 제한되며, 최대 3 영업일 및 당사자들 간에 사전에 합리적으로 합의한 범위로 제한됩니다. 정보 보호 법률에서 더 빨리 감사를 실시할 것을 요구하지 않는 한, 최소 60 일의 합리적인 사전 통지를 해야 합니다. SAP 와 고객은 기존 인증서 또는 다른 감사 보고서를 이용해 감사 중복을 최소화합니다. 고객과 SAP 는 각자 자신의 감사 비용을 부담합니다. 단, 고객이 제 6.1 항(단, 감사 결과 SAP 가 위반했음이 밝혀진 경우 SAP 가 자신의 감사 비용을 부담해야 함), 제 6.1(d)항 또는 제 6.1(e)항에 따라 감사를 하는 경우에는 예외로 합니다. 이러한 경우, 고객은 감사 수행에 필요한 자신의 비용과 SAP 의 내부 자원 비용을 부담합니다. 감사 결과 SAP 가 계약 의무를 위반한 것으로 드러나는 경우, SAP 는 자체 비용으로 해당 위반 사항을 즉시 구제합니다.

7. EU 액세스

7.1 옵션 서비스.

발주서에 포함된 경우, SAP 는 본 제 7 항에 명시된 대로 적격 클라우드 서비스에 대한 EU 액세스를 제공하는 데 동의합니다.

7.2 EU 액세스.

SAP 는 클라우드 서비스의 개인 정보에 대한 액세스가 필요한 지원을 제공하는 데 있어 유럽 지역의 협력업체만을 이용합니다.

7.3 데이터 센터 위치.

발주서 효력 발생일부터 클라우드 서비스에서 개인 정보를 호스팅하는 데 사용된 데이터 센터는 EEA 또는 스위스에 위치합니다. SAP 는 고객의 사전 서면 동의(이메일도 허용됨) 없이 EEA 또는 스위스 밖의 데이터 센터로 고객 인스턴스를 마이그레이션하지 않습니다. SAP 가 EEA 또는 스위스 내에 있는 데이터 센터로 고객 인스턴스를 마이그레이션하고자 하는 경우, SAP 는 예정된 마이그레이션의 최소 삼십일 전 고객에게 서면(이메일도 허용됨)으로 통지합니다.

7.4 예외.

다음 개인 정보에는 제 7.2 항~제 7.3 항의 요건이 적용되지 않습니다.

(a) 지원 티켓 전송자의 세부 연락처

(b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to SAP;

(c) Personal Data in non-production systems.

8. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

8.1 **"Data Center"** means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at**:** http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html or notified to Customer or otherwise agreed in an Order Form.

8.2 **"Data Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

8.3 **"Data Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

8.4 **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

8.5 **"Data Subject"** means an identified or identifiable natural person.

8.6 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Lichtenstein and Norway.

8.7 **"European Subprocessor"** means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

8.8 **"Personal Data"** means any information relating to a Data Subject For the purposes of this DPA, it includes only personal data entered by Customer or its Authorized Users into or derived from their use of the Cloud Service. It also includes personal data supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data.

(b) 지원 티켓 접수 시 고객이 제출한 기타 모든 개인 정보. 고객은 지원 티켓 접수 시 개인 정보를 전송하지 않도록 선택할 수 있습니다. 이 정보가 문제점 관리 프로세스에 필수적인 경우, 고객은 문제점 메시지를 SAP 에 전송하기 전에 해당 개인 정보를 익명화할 수 있습니다.

(c) 비운영 시스템의 개인 정보

8. 용어 정의

본 문서에서 정의되지 않은 대문자로 시작되는 용어는 본 계약에서 해당 용어에 부여된 의미를 지닙니다.

8.1 **"데이터 센터"**는 클라우드 서비스의 제품 인스턴스가 해당 지역의 고객을 위해 호스팅되는 지역을 의미하며 http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html 에 게시되어 있거나 고객에게 통보되었거나 발주서에서 달리 동의됩니다.

8.2 **"데이터 컨트롤러"**는 개인 정보의 처리 목적과 수단을 단독으로 또는 다른 기관과 공동으로 결정하는 자연인 또는 법인, 공공 기관, 단체 또는 기타 조직을 의미합니다.

8.3 **"데이터 처리자"**는 컨트롤러를 대신해서 개인 정보를 처리하는 자연인 또는 법인, 공공 기관, 단체 또는 기타 조직을 의미합니다.

8.4 **"정보 보호 법률"**은 개인의 기본 권리 및 자유와 본 계약에 따른 개인 정보 처리와 관련된 개인정보 보호 권리를 보호하는 관련 법률을 의미합니다.

8.5 **"데이터 주체"**는 식별되거나 식별 가능한 자연인을 의미합니다.

8.6 **"EEA"**는 유럽경제지역(European Economic Area)을 의미하며, 아일랜드, 리히텐슈타인, 노르웨이를 포함하여 유럽연합 회원국을 말합니다.

8.7 **"유럽 협력업체"**는 EEA 나 스위스에서 개인정보를 실제로 처리하는 협력업체를 의미합니다.

8.8 **"개인 정보"**는 본 DPA 의 목적상 데이터 주체와 관련한 모든 정보를 의미하며, 여기에는 고객 또는 그 권한 있는 사용자가 입력하거나, 이들의 클라우드 서비스 사용을 통해 파생된 개인 정보만 포함됩니다. 여기에는 본 계약에 따라 지원을 제공할 목적으로 SAP 나 그 협력업체에 제공되거나 SAP 나 그 협력업체가 액세스한 개인 정보도 포함됩니다. 개인 정보는 고객 정보의 일부입니다.

8.9 "Security Breach" means a confirmed (1) accidental or unlawful destruction, loss, alteration, or disclosure of Customer Personal Data or Confidential Data, or (2) similar incident involving Personal Data for which a Data Processor is required under applicable law to provide notice to the Data Controller.

8.10 "Standard Contractual Clauses" or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof released by the Commission (which will automatically apply). The current Standard Contractual Clauses are located at http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc. They include Appendices 1 and 2 attached to this DPA.

8.11 "Subprocessor" means SAP Affiliates and third parties engaged by SAP or SAP's Affiliates to process personal data.

8.12 "Third Country Subprocessor" means any Subprocessor incorporated outside the EEA and outside any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

8.9 "보안 위반"은 확인된 (1) 고객 개인 정보 또는 비밀 정보의 불법적 파괴, 손실, 변경이나 공개 또는 (2) 해당 법률에 따라 데이터 처리자가 데이터 컨트롤러에게 통지해야 하는 개인 정보가 관련된 유사한 사고를 의미합니다.

8.10 "표준 계약 조항"(또는 간혹 "EU 모델 조항"으로도 지칭됨)은 (표준 계약 조항(처리자)) 또는 위원회가 공개한 그 후속 버전(자동으로 적용됨)을 의미합니다. 현행 표준 계약 조항은 http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc 에 게시되어 있습니다. 여기에는 본 DPA 에 첨부된 부록 1 과 2 가 포함됩니다.

8.11 "협력업체"는 개인 정보 처리를 위해 SAP 또는 SAP 계열사가 고용한 SAP 계열사 및 제 3 자를 의미합니다.

8.12 "제 3 국 협력업체"는 EEA 외부 및 http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm 에 게시되어 있는 유럽 위원회가 적합 결정을 발표한 모든 국가 외부에 포함된 협력업체를 의미합니다.

Appendix 1 to Data processing agreement and Standard Contractual Clauses

Data Exporter

The Data Exporter subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data.

Data Importer

SAP and its Subprocessors provide the Cloud Service that includes the following support:

SAP Affiliates support the Cloud Service data centers remotely from SAP facilities in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

SAP Affiliates provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. SAP answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of data subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

Data Categories

The transferred Personal Data transferred concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, time

정보 처리 계약 및 표준 계약 조항의 부록 1

데이터 엑스포터

데이터 엑스포터는 클라우드 서비스에 등록되어 있으며, 이를 통해 권한 있는 사용자가 개인 정보를 입력, 수정, 사용, 삭제 또는 처리할 수 있습니다.

데이터 임포터

SAP 와 그 협력업체는 다음과 같은 지원이 포함된 클라우드 서비스를 제공합니다.

SAP 계열사는 St. Leon/Rot(독일), 인도 및 SAP 가 운영/클라우드 제공 기능을 담당하는 직원을 채용한 기타 지역의 SAP 시설에서 원격으로 클라우드 서비스 데이터 센터를 지원합니다. 지원에는 다음이 포함됩니다.

- 클라우드 서비스 모니터링
- 클라우드 서비스에 저장된 고객 데이터의 백업 및 복구
- 클라우드 서비스의 수정 및 개선 사항의 발표 및 개발
- 기본 클라우드 서비스 인프라 및 데이터베이스의 모니터링, 문제 해결 및 관리
- 보안 모니터링, 네트워크 기반 침입 감지 지원, 침투 테스트

클라우드 서비스를 사용할 수 없거나 일부 또는 모든 권한 있는 사용자에 대해 예상대로 작동하지 않아 고객이 지원 티켓을 제출한 경우 SAP 계열사는 지원을 제공합니다. SAP 는 전화에 응답하고, 기본적인 문제 해결을 수행하며, 클라우드 서비스의 운영 인스턴스에서 분리된 추적 시스템의 지원 티켓을 처리합니다.

정보 주체

데이터 엑스포터가 달리 규정하지 않는 한, 전송된 개인 정보는 직원, 계약자, 비즈니스 파트너 또는 클라우드 서비스에 개인 정보가 저장된 기타 개인의 정보 주체의 범주와 관련된 것입니다.

정보 범주

전송되는 개인 정보는 다음과 같은 범주의 데이터와 관련된 것입니다.

고객이 등록된 클라우드 서비스별로 데이터 범주를 결정합니다. 고객은 클라우드 서비스가 실행되는 동안 또는 클라우드 서비스에서 달리 정한대로 데이터 필드를 구성할 수 있습니다. 전송되는 개인 정보는 주로 이름, 전화번호, 이메일

zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data that Authorized Users enter into the Cloud Service and may include bank account data, credit or debit card data.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Order Form, if any.

Processing Operations

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with this Agreement

주소, 시간대, 주소 정보, 시스템 액세스/사용/권한 정보, 회사 이름, 계약 정보, 송장 정보 및 권한 있는 사용자가 클라우드 서비스에 입력하고 은행 계좌 정보, 신용/직불 카드 정보 등이 포함될 수 있는 애플리케이션 특정 데이터의 데이터 범주와 관련된 것입니다.

특별 데이터 범주(해당하는 경우)

전송되는 개인 정보는 해당하는 경우 발주서에 명시된 바에 따른 다음과 같은 특별 범주의 정보와 관련된 것입니다.

처리 작업

전송되는 개인 정보는 다음과 같은 기본 처리 작업의 대상이 됩니다.

- 클라우드 서비스를 설정, 운영, 모니터링, 제공하기 위한 개인 정보의 이용(조직적/기술적 지원 포함)
- 컨설팅 서비스의 제공
- 권한 있는 사용자와의 통신
- 전용 데이터 센터(멀티 테넌트 아키텍처)에 개인 정보 저장
- 수정 사항 업로드 및 클라우드 서비스 업그레이드
- 개인 정보 백업
- 컴퓨터로 개인 정보 처리(데이터 전송, 데이터 검색, 데이터 액세스 포함)
- 개인 정보 전송을 허용하기 위한 네트워크 액세스
- 본 계약에 따른 고객 지침의 수행

Appendix 2 – Technical and Organizational Measures

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define the SAP's current security measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

1.1 Physical Access Control.

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- SAP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from

부록 2 – 기술적/조직적 조치

1. 기술적, 조직적 조치

다음 조항들은 SAP 의 현재 보안 조치를 정의합니다. SAP 는 비슷하거나 그보다 향상된 수준의 보안을 유지하는 한 이를 통지 없이 언제든 변경할 수 있습니다. 이는 곧 개별 조치가 동일한 목적의 새로운 조치로 보안 수준의 감소 없이 대체될 수 있음을 의미합니다.

1.1 물리적 액세스 제어.

승인되지 않은 사람이 개인 정보를 처리하거나 사용하는 정보 처리 시스템이 위치해 있는 사업장, 건물, 실내에 대한 물리적 액세스를 확보하는 것을 방지합니다.

조치:

- SAP 는 보안 등급을 기반으로 적절한 수단을 사용하여 자산과 시설을 보호합니다. 내부 보안 부서가 이를 담당합니다.
- 일반적으로 건물은 액세스 제어 시스템(예: 스마트 카드 액세스 시스템)을 통해 보안됩니다.
- 최소 요건으로, 건물의 가장 바깥쪽 출입 지점에는 현대식 활성 키 관리를 포함한 인증된 키 시스템을 장착해야 합니다.
- 보안 등급에 따라 건물, 개별 구역 및 주변 지역은 추가 조치로 보안을 강화할 수 있습니다. 추가 조치에는 특정 액세스 프로필, 비디오 감시, 침입자 경보 시스템 및 생체 인식 액세스 제어 시스템이 포함됩니다.
- 시스템 및 데이터 액세스 제어 조치에 따라 개별적으로 승인된 사람에게 액세스 권한을 부여합니다(아래 제 1.2 항 및 제 1.3 항 참조). 이는 방문객 액세스에도 적용됩니다. SAP 건물을 방문하는 손님과 방문객은 접수처에서 이름을 등록해야 하며 승인된 SAP 직원과 동행해야 합니다.
- SAP 직원 및 외부 인력은 모든 SAP 위치에서 ID 카드를 착용해야 합니다.

데이터 센터의 추가 조치:

- 모든 데이터 센터는 보안 요원, 감시 카메라, 동작 감지기, 액세스 제어 장치 및 장비와 데이터 센터 시설이 손상되는 것을 방지할 기타 조치로 강화되는 엄격한 보안 절차를 유지합니다. 승인된 대리인만이

being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To ensure proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

- SAP and all third party Data Center providers log the names and times of persons entering SAP's private areas within the Data Centers.

1.2 System Access Control.

Data processing systems used to provide the SAP Services must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
- All users access SAP's systems with a unique identifier (user ID).
- SAP has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are revoked.
- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.

데이터 센터 시설 내부의 시스템과 인프라에 액세스합니다. 적절한 기능을 보장하기 위해, 물리적 보안 장비(예: 동작 센서, 카메라 등)의 정기적 유지보수를 수행합니다.

- SAP 와 모든 제 3 자 데이터 센터 공급업자는 데이터 센터 내의 SAP 사적 구역을 출입하는 개인의 이름과 시간을 기록합니다.

1.2 시스템 액세스 제어.

SAP 서비스를 제공하기 위해 사용되는 데이터 처리 시스템은 승인되지 않은 사용이 금지되어야 합니다.

조치:

- 개인 정보를 저장하고 처리하는 시스템을 포함하여 중요한 시스템의 경우 여러 인증 단계를 사용하여 액세스를 허가합니다. 적절한 권한이 있는 승인된 사용자가 사용자를 추가, 삭제 또는 수정할 수 있도록 보장하는 절차가 마련되어 있습니다.
- 모든 사용자는 고유 식별자(사용자 ID)를 이용해 SAP 시스템에 액세스합니다.
- SAP 는 요청된 권한 변경이 지침에 따라서만 실행되도록 보장하기 위한 절차를 갖추고 있습니다(예: 허가 없이는 어떤 권한도 부여되지 않음). 사용자가 퇴직할 경우 해당 사용자의 액세스 권한이 철회됩니다.
- SAP 는 비밀번호 공유를 금지하고 비밀번호가 공개된 경우 취해야 할 대응책을 명시하고 정기적으로 비밀번호를 변경하도록 규정하며 기본 비밀번호가 달라지는 비밀번호 정책을 수립하고 있습니다. 인증을 위해 개인별 사용자 ID 가 배정됩니다. 모든 비밀번호는 규정된 최소 요건을 충족하고 암호화된 형태로 저장되어야 합니다. 도메인 비밀번호의 경우 복잡한 비밀번호 요건을 충족하는 비밀번호 변경이 시스템에 의해 6 개월마다 강제됩니다. 모든 컴퓨터에서 비밀번호로 보호된 화면 보호기가 작동됩니다.
- 회사 네트워크는 방화벽에 의해 공용 네트워크로부터 보호됩니다.
- SAP 는 회사 네트워크로 진입하는 액세스 지점(이메일 계정)과 모든 파일 서버 및 모든 워크스테이션에 최신 바이러스 차단 소프트웨어를

- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.
- Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control .

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

Measures:

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. SAP uses authorization concepts that document how authorizations are assigned and which authorizations are assigned to whom. All personal, confidential, or otherwise sensitive data is protected in accordance with the SAP security policies and standards. Confidential information must be processed confidentially.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.
- SAP does not allow the installation of personal software or other software that has not been approved by SAP.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control.

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate

사용합니다.

- 보안 패치 관리가 관련 보안 업데이트의 정기적인 배포를 보장하기 위해 시행됩니다.
- SAP 회사 네트워크 및 중요한 인프라에 대한 완전한 원격 액세스는 강력한 인증에 의해 보호됩니다.

1.3 데이터 액세스 제어.

데이터 처리 시스템을 사용할 권한이 있는 사람은 액세스할 권한이 있는 개인 정보에 대한 액세스만 얻으며, 처리, 사용, 저장하는 중에 권한 없이 개인 정보를 읽거나 복사하거나 수정하거나 제거할 수 없습니다.

조치:

- SAP 보안 정책의 일환으로, 개인 정보는 SAP 정보 등급 표준에 따른 "비밀" 정보와 최소 동일한 수준의 보호가 요구됩니다.
- 개인 정보, 비밀 정보 또는 민감한 정보에 대한 액세스 권한은 알아야 할 필요가 있는 경우에만 부여됩니다. 다시 말해 직원이나 외부의 제 3 자는 업무 완수를 위해 필요한 정보에 대한 액세스 권한을 갖게 됩니다. SAP 는 어떤 권한이 누구에게 어떻게 배정되는지를 문서화하는 권한 부여 개념을 사용합니다. 모든 개인 정보, 비밀 정보 또는 기타 민감한 정보는 SAP 보안 정책 및 표준에 따라 보호됩니다. 비밀 정보는 비밀을 유지하며 처리되어야 합니다.
- 모든 운영 서버는 데이터 센터 또는 안전한 서버실 내에서 가동됩니다. 개인 정보, 비밀 정보 또는 기타 민감한 정보 처리용 애플리케이션을 보호하는 보안 조치에 대해 정기적 점검이 이루어집니다. 이를 위해 SAP 는 자체 IT 시스템에 대한 내부 및 외부 보안 점검 및 침투 테스트를 수행합니다.
- SAP 는 개인 소프트웨어나 SAP 가 승인하지 않은 기타 소프트웨어의 설치를 허용하지 않습니다.
- SAP 보안 표준은 더 이상 필요하지 않은 데이터 및 데이터 매체를 삭제 또는 파기하는 방법을 규정합니다.

1.4 데이터 전송 제어.

관련 서비스 계약에 따른 서비스의 제공을 위해 필요한 경우를 제외하고, 개인 정보를 전송하는 동안 이를 승인 없이 읽거나, 복사하거나, 수정하거나, 제거할 수 없습니다. 데이터 매체를 직접 운송하는 경우에는 합의된 서비스 수준을 보장하기 위해

measures are implemented at SAP to ensure the agreed-upon service levels (for example, encryption and lead-lined containers).

- Personal Data transfer over SAP internal networks are protected in the same manner as any other confidential data according to SAP Security Policy.
- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center).

1.5 Data Input Control.

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems.

Measures:

- SAP only allows authorized persons to access Personal Data as required in the course of their work.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within SAP's Products and Services to the fullest extent possible.

1.6 Job Control.

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the relevant agreement and related instructions of the customer.

Measures:

- SAP uses controls and processes to ensure compliance with contracts between SAP and its customers, subprocessors or other service providers.
- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.

적절한 조치가 SAP 에서 시행됩니다(예: 암호화, 납으로 차폐한 용기 등).

- SAP 내부 네트워크를 통한 개인 정보 전송은 SAP 보안 정책에 따라 기타 다른 비밀 정보와 같은 방식으로 보호됩니다.
- 데이터가 SAP 와 고객 간에 전송되는 경우, 전송되는 개인 정보를 위한 보호 조치가 상호 합의되며 관련 계약의 일부가 됩니다. 이는 물리적 데이터 전송과 네트워크 기반 데이터 전송에 모두 적용됩니다. 어떠한 경우에도 SAP 가 관리하는 시스템 외부에서 데이터 전송이 이루어진 경우(예: SAP 데이터 센터 방화벽 외부에서 전송된 데이터) 모든 데이터 전송에 대한 책임은 고객에게 있습니다.

1.5 데이터 입력 제어.

개인 정보가 SAP 정보 처리 시스템에서 입력, 수정 또는 제거되었는지 여부 및 이 작업의 수행 당사자를 소급하여 조사 및 확인할 수 있습니다.

조치:

- SAP 는 승인된 사람에 한해 업무상 필요한 개인 정보에만 액세스할 수 있도록 허용합니다.
- SAP 는 가능한 최대한의 범위에서 SAP 제품 및 서비스 내에서 SAP 또는 그 협력업체에 의한 개인 정보의 입력, 수정 및 삭제 또는 차단을 위한 로그 시스템을 구현했습니다.

1.6 작업 제어.

위탁 처리되는 개인 정보(예: 고객을 대신하여 처리된 개인 정보)는 관련 계약 및 고객의 관련 지침에 따라서만 처리됩니다.

조치:

- SAP 는 제어 조치와 프로세스를 사용하여 SAP 와 고객, 협력업체 또는 기타 서비스 공급자 간의 계약 준수를 보장합니다.
- SAP 보안 정책의 일환으로, 개인 정보는 SAP 정보 등급 표준에 따른 "비밀" 정보와 최소 동일한 수준의 보호가 요구됩니다.
- 모든 SAP 직원 및 하청 협력업체 또는 기타 서비스 제공자는 SAP 고객 및 파트너의 영업비밀 등 모든 민감한 정보를 비밀로 유지할 계약상의 책임이 있습니다.

- For on premise support services, SAP provides a specially designated, secure support ticket facility in which SAP provides a special access-controlled and monitored security area for transferring access data and passwords. SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer system without the knowledge or full active participation of the customer.

1.7 Availability Control.

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- SAP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.
- SAP has defined contingency plans as well as business and disaster recovery strategies for the provided Services.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control.

Personal Data collected for different purposes can be processed separately.

Measures:

- SAP uses the technical capabilities of the deployed software (for example: multi-tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customers (including their Affiliates) have access only to their own data.
- If Personal Data is required to handle a support incident from a specific customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 Data Integrity Control .

Personal Data will remain intact, complete and current during processing activities.

Measures:

SAP has implemented a multi-layered defense strategy

- 온 프레미스 지원 서비스의 경우, SAP 는 특별 지정된 보안 지원 티켓 시설을 제공하며, 이를 통해 SAP 는 액세스 데이터 및 비밀번호를 전송하기 위한 액세스 보호와 모니터링이 이루어지는 특별 보안 구역을 제공합니다. SAP 고객은 언제든지 원격 지원 연결에 대한 제어권을 가질 수 있습니다. SAP 직원은 고객이 모르고 있거나 적극적이며 전적인 참여를 제공하지 않는 상황에서 고객 시스템에 액세스할 수 없습니다.

1.7 가용성 제어.

우발적 또는 무단 파기 또는 손실로부터 개인 정보를 보호합니다.

조치:

- SAP 는 백업 절차 및 기타 조치를 활용하여 필요에 따라 비즈니스 핵심 시스템의 신속한 복구를 보장합니다.
- SAP 는 무정전 전원공급장치(UPS, 배터리, 발전기 등)를 이용해 데이터 센터의 전원 공급을 보장합니다.
- SAP 는 비상 계획과 제공되는 서비스를 위한 비즈니스 및 재해 복구 전략을 규정합니다.
- 비상 절차 및 시스템에 대한 정기적 테스트가 이루어집니다.

1.8 데이터 분리 제어.

서로 다른 목적으로 수집된 개인 정보의 별도 처리가 가능합니다.

조치:

- SAP 는 여러 고객에서 비롯된 개인 정보를 분리하기 위해 배포된 소프트웨어(예: 다중 테넌시 또는 별도 시스템 환경)의 기술적 능력을 사용합니다.
- 고객(계열사 포함)은 자신의 정보에만 액세스할 수 있습니다.
- 고객 정보가 특정 고객으로부터의 지원 인스턴스를 처리해야 하는 경우, 정보는 해당 특정 메시지에 할당되어 해당 메시지를 처리하기 위해서만 사용되며 다른 메시지를 처리하기 위해 액세스되지 않습니다. 이 정보는 전용 지원 시스템에 저장됩니다.

1.9 데이터 무결성 제어.

개인 정보는 프로세스 처리 활동 중에 온전성, 정확성, 최신성이 유지됩니다.

조치:

SAP 는 무단 수정에 대한 보호로서 다중 방어 단계를

as a protection against unauthorized modifications.

In particular, SAP uses the following to implement the control and measure sections described above. In particular:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

구현했습니다.

특히, SAP 는 위에 설명된 관리 및 조치 조항을 실행하기 위해 다음을 사용합니다. 특히 다음을 의미합니다.

- 방화벽
- 보안 모니터링 센터
- 바이러스 방지 소프트웨어
- 백업 및 복구
- 외부 및 내부 침투 테스트
- 보안 조치를 증명할 정기적인 외부 감사