PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES
SAP 클라우드 서비스에 관한 개인 정보 처리 계약

1. BACKGROUND
배경

1.1 Purpose and Application. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data processed by SAP and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP, and Customer shall not store Personal Data in such environments.

목적 및 적용. 본 정보 처리 계약 문서("**DPA**")는 본 계약에 통합되어 SAP 와 고객 간 서면(전자 형식 포함) 계약의 일부를 구성하며, 클라우드 서비스 제공과 관련하여 SAP 와 그 협력업체가 처리하는 개인 정보에 적용됩니다. 클라우드 서비스의 비운영 환경을 SAP 가 제공하는 경우, 본 DPA 는 해당 환경에 적용되지 않으며, 고객은 해당 환경에 개인 정보를 저장해서는 안 됩니다.

1.2 Structure. Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organizational measures.

구조. 부록 1 과 2 는 본 DPA 에 통합되어 그 일부를 구성합니다. 이들 문서는 합의된 주제 사안, 처리의 성격과 목적, 개인 정보의 유형, 정보 주체의 유형, 적용되는 기술적/조직적 조치를 명시합니다.

1.3 GDPR. SAP and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

GDPR. SAP 와 고객은 본 DPA 에 따라 처리되는 고객/컨트롤러의 개인 정보에 적용되는 경우 및 그 범위 내에서, 일반 정보 보호 법률 2016/679("**GDPR**"), 특히 GDPR 제 28 조, 제 32 조~제 36 조에 따라 컨트롤러와 처리자에 부과된 의무를 검토하고 채택할 책임이 각 당사자에 있다는 것에 동의합니다. 예를 들어 설명하자면, 부록 3 은 관련 GDPR 요건과 본 DPA 의 해당 조항을 나열합니다.

1.4 Governance. SAP acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SAP as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

거버넌스. SAP 는 처리자로서 역할을 하며, 고객 및 고객이 클라우드 서비스 사용을 허용한 법인은 DPA 에 따른 컨트롤러로 활동합니다. 고객은 단일 연락 담당자로서 역할을 하며, 처리자로서 SAP 를 이용하는 컨트롤러의 관련 승인을 비롯하여 본 DPA 에 따라 개인 정보 처리를 위한 해당 승인, 동의, 허가를 획득할 단독 책임이 있습니다. 고객이 승인, 동의, 지침 또는 허가를 제공하는 경우, 이들은 고객을 대신하여 제공될 뿐만 아니라 클라우드 서비스를 사용하는 다른 모든 컨트롤러를 대신하여 제공됩니다. SAP 가 고객에게 정보 또는 통지를 제공한 경우, 해당 정보 또는 통지는 고객이 클라우드 서비스 사용을 허가한 컨트롤러가 수령한 것으로 간주되며 고객에게는 해당 정보 및 통지를 해당 컨트롤러에게 전달할 책임이 있습니다.

2. SECURITY OF PROCESSING
정보 처리 보안

2.1 **Appropriate Technical and Organizational Measures.** SAP has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

관련 기술적, 조직적 조치. SAP 는 부록 2 에 명시된 기술적/조직적 조치를 시행했으며 이를 적용할 것입니다. 고객은 이러한 조치를 검토했으며 고객이 발주서에서 선택한 클라우드 서비스에 대해 해당 조치가 기술상태, 구현 비용, 개인 정보 처리의 성격, 범위, 맥락 및 목적을 적절히 고려하고 있다는 점에 동의합니다.

2.2 **Changes.** SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base hosted out of the same Data Center and receiving the same Cloud Service. SAP may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

변경. SAP 는 동일한 데이터 센터에서 호스팅되고 동일한 클라우드 서비스를 받는 SAP 의 전체 고객 기반에 부록 2 에 명시된 기술적/조직적 조치를 적용합니다. SAP 는 비슷하거나 그보다 높은 수준의 보안을 유지한다면 부록 2 에 명시된 조치를 통지 없이 언제든 변경할 수 있습니다. 개별 조치는, 개인 정보를 보호하는 보안 수준의 감소 없이, 동일한 목적의 새로운 조치로 대체될 수 있습니다.

3. SAP OBLIGATIONS
SAP 의무

3.1 **Instructions from Customer.** SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted).

고객의 지침. SAP 는 고객의 서면 지침에 따라서만 개인 정보를 처리합니다. 본 계약(본 DPA 포함)은 최초의 해당 서면 지침을 구성하며 이후 클라우드의 각 사용은 추가 지침을 구성합니다. SAP 는 정보 보호 법률에 따라 요구되고 기술적으로 가능하며 클라우드 서비스에 대한 변경을 요구하지 않는 한 모든 고객 지침을 따르기 위해 타당한 노력을 기울일 것입니다. 전술한 예외가 적용되거나 SAP 가 지침을 준수할 수 없거나 지침이 정보 보호 법률을 침해한다는 의견이 있는 경우, SAP 는 이를 즉시 고객에게 통지합니다(이메일 가능).

3.2 **Processing on Legal Requirement.** SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

법적 요건에 따른 처리. SAP 는 또한 관련 법률에서 요구하는 경우 개인 정보를 처리할 수 있습니다. 이 경우, 해당 법률이 공공 이익의 중대한 사유로 인해 해당 정보를 금지하는 경우가 아닌 한, SAP 는 처리하기 전에 법적 요건을 고객에게 알려야 합니다.

3.3 **Personnel.** To process Personal Data, SAP and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

인력. 개인 정보를 처리하기 위해, SAP 와 그 협력업체는 비밀 유지 준수를 약속한 승인된 인력에게만 액세스를 허가해야 합니다. SAP 와 그 협력업체는 관련 정보 보안 및 데이터 보호에 관해 개인 정보에 액세스하는 인력을 정기적으로 교육합니다.

3.4 Cooperation. At Customer's request, SAP will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data or any Personal Data Breach. SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SAP shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, SAP will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

협력. 고객이 요청할 경우, SAP 는 정보 주체의 요청을 처리하는 업무 또는 SAP 의 개인 정보 처리나 개인 정보 위반과 관련한 규제 당국의 업무에서 고객 및 컨트롤러와 합리적으로 협력합니다. SAP 는 개인 정보 처리와 관련하여 정보 주체로부터 받은 요청에 대해 합리적으로 가능한 즉시 고객에게 통지해야 하며, 고객의 추가 지침 없이는 해당 요청에 응답하지 않습니다(해당하는 경우). SAP 는 고객이 클라우드 서비스로부터 개인 정보를 수정 또는 삭제하거나 정보 보호 법률에 따라 처리를 제한할 수 있도록 지원하는 기능을 제공해야 합니다. 이러한 기능이 제공되지 않는 경우, SAP 는 고객의 지침과 정보 보호 법률에 따라 개인 정보를 수정 또는 삭제하거나 처리를 제한합니다.

3.5 Personal Data Breach Notification. SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP.

개인 정보 위반 통지. SAP 는 개인 정보 위반 사실을 알게 되면 이를 지체 없이 고객에게 통지하고, 정보 보호 법률이 요구하는 바에 따라 개인 정보 위반을 보고할 의무를 고객이 이행할 수 있도록 지원하기 위해 자신이 소유하고 있는 합리적인 정보를 제공합니다. 제공 가능한 경우 SAP 는 해당 정보를 단계별로 제공할 수 있습니다. 이러한 통지는 SAP 의 잘못 또는 책임을 인정하는 것으로 이해되거나 해석될 수 없습니다.

3.6 Data Protection Impact Assessment. If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

정보 보호 영향 평가. 정보 보호 법률에 따라 고객(또는 고객의 컨트롤러)이 정보 보호 영향 평가를 수행하거나 기관과 협의해야 하는 경우, 고객의 요청이 있을 시, SAP 는 클라우드 서비스를 위해 일반적으로 제공하는 해당 문서를 제공합니다(예: 본 DPA, 본 계약, 감사 보고서 또는 인증서). 모든 추가 지원은 당사자들 간에 상호 합의되어야 합니다.

4. DATA EXPORT AND DELETION

데이터 내보내기 및 삭제

4.1 Export and Retrieval by Customer. During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SAP and Customer will find a reasonable method to allow Customer access to Personal Data.

고객에 의한 내보내기 및 가져오기. 등록 기간 중 본 계약에 따라, 고객은 언제든지 자신의 개인 정보에 액세스할 수 있습니다. 고객은 자신의 개인 정보를 표준 형식으로 내보내거나 가져올 수 있습니다. 내보내기 및 가져오기에는 기술적 제한이 있을 수 있으며, 이 경우 SAP 와 고객은 고객이 개인 정보에 액세스할 수 있도록 해주는 합리적인 방법을 마련합니다.

4.2 Deletion. Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby

instructs SAP to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.

삭제. 등록 기간 만료 전, 고객은 클라우드 서비스로부터 개인 정보를 최종적으로 내보내기 위해 SAP 의 셀프 서비스 내보내기 도구(이용 가능한 대로)를 사용할 수 있습니다(개인 정보의 "반환"을 구성함). 등록 기간 종료 시, 관련 법률에 따라 보관이 요구되지 않는 한, 고객은 클라우드 서비스를 호스팅하는 서버에 남아 있는 개인 정보를 정보 보호 법률에 따라 합리적인 기간 내에(6 개월 이하) 삭제하도록 SAP 에 지시합니다.

5. CERTIFICATIONS AND AUDITS

인증 및 감사

5.1 Customer Audit. Customer or its independent third party auditor reasonably acceptable to SAP (which shall not include any third party auditors who are either a competitor of SAP or not suitably qualified or independent) may audit SAP's control environment and security practices relevant to Personal Data processed by SAP only if:

고객 감사. 고객 또는 SAP 가 타당하게 수용할 수 있는 독립적인 제 3 자 감사인은(SAP 의 경쟁업체이거나 적합한 자격을 갖추지 않았거나 독립적이지 않은 제 3 자 감사인은 제외됨) 다음의 경우에만 SAP 가 처리한 개인 정보와 관련하여 SAP 의 제어 환경과 보안 관행에 대한 감사를 실시할 수 있습니다.

(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 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or SAP;

(I) ISO 27001 또는 기타 표준에 따른 인증서(범위는 인증서에 정의) 또는 (ii) 유효한 ISAE3402 및/또는 ISAE3000 또는 기타 SOC1-3 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 감사 보고서 또는 ISO 인증서를 이용할 수 있습니다.

(b) A Personal Data Breach has occurred;

개인 정보 위반이 발생한 경우

(c) An audit is formally requested by Customer's data protection authority; or

고객의 정보 보호 당국이 정식으로 감사를 요청한 경우

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

의무적인 정보 보호 법률이 고객에게 직접 감사 권한을 규정하고 있는 경우. 의무적인 정보 보호 법률이 더 많은 횟수의 감사를 요구하지 않는 한 고객이 12 개월의 기간 동안 1 회만 감사를 수행합니다.

5.2 Other Controller Audit. Any other Controller may audit SAP's control environment and security practices relevant to Personal Data processed by SAP in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

다른 컨트롤러 감사. 다른 모든 컨트롤러는 제 5.1 항에 명시된 사례가 해당 컨트롤러에 적용될 경우에 한해 제 5.1 항에 따라 SAP 가 처리한 개인 정보와 관련하여 SAP 의 제어 환경과 보안 관행에 대한 감사를 실시할 수 있습니다. 정보 보호 법률에 따라 다른 컨트롤러가 스스로 감사를 수행해야 하는 경우를 제외하고, 이러한 감사는 제 5.1 항에 명시된 바에 따라 고객을 통해 그리고 고객이 수행할 수 있습니다. 본 계약에 따라 SAP 가 처리하는 개인 정보를 가지고 있는 여러 컨트롤러가 감사를 요구하는 경우, 고객은 복수의 감사를 피할 수 있는 모든 합리적인 수단을 사용해 감사를 통합해야 합니다.

5.3 Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP.

감사 범위. 고객은 의무적인 정보 보호 법률 또는 관련 정보 보호 당국이 더 짧은 기간의 통지를 요구하지 않는 한 모든 감사에 대해 적어도 60 일의 사전 통지를 제공해야 합니다. 감사의 빈도와 범위는 합리적이고 성실하게 행동하는 당사자들 간에 상호 합의되어야 합니다. 고객 감사는 최대 3 근무일의 기간으로 제한됩니다. 이러한 제한사항 외에도, 당사자들은 기존 인증서 또는 다른 감사 보고서를 이용해 감사 중복을 최소화합니다. 고객은 모든 감사 결과를 SAP 에 제공합니다.

5.4 Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by SAP of this DPA, then SAP shall bear its own expenses of an audit. If an audit determines that SAP has breached its obligations under the DPA, SAP will promptly remedy the breach at its own cost.

감사 비용. 고객은 모든 감사 비용을 부담해야 합니다. 단, 감사 결과 SAP 의 중대한 위반이 밝혀진 경우는 예외로 하며, 이 경우 SAP 가 자신의 감사 비용을 부담해야 합니다. 감사 결과 SAP 가 본 DAP 에 따른 의무를 위반한 것으로 드러나는 경우, SAP 는 자체 비용으로 해당 위반 사항을 즉시 구제합니다.

6. SUBPROCESSORS
협력업체

6.1 Permitted Use. SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

허가된 사용. SAP 는 개인 정보 처리를 협력업체에 하청할 수 있는 일반적인 권한을 부여받으며, 다음과 같은 조건이 적용됩니다.

(a) SAP or SAP SE on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SAP shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

SAP 또는 SAP 를 대신하는 SAP SE 는 협력업체의 개인 정보 처리와 관련하여 본 DPA 의 조건을 준수하는 서면(전자 형식 포함) 계약을 체결하여 협력업체를 고용해야 합니다. SAP 는 본 계약 조건에 따라 협력업체의 모든 위반에 대해 책임져야 합니다.

(b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

SAP 는 본 DPA 가 요구하는 개인 정보 보호 수준을 제공할 수 있음을 규명하기 위해 협력업체를 선택하기 전에 협력업체의 보안, 개인정보 보호 및 비밀 유지 관행을 평가합니다.

(c) SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the Cloud Service.

SAP 는 본 계약의 효력 발생일에 존재하는 SAP 의 협력업체 목록을 공개하거나 고객 요청 시 제공하며, 여기에는 SAP 가 클라우드 서비스를 제공하기 위해 사용하는 각 협력업체의 이름, 주소 및 역할이 포함되어 있습니다.

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

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

(a) SAP will inform Customer in advance (by email or by posting on the support portal available through SAP Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

SAP 는 신규 협력업체의 이름, 주소, 역할을 비롯하여 협력업체 목록에 의도적인 추가 또는 교체가 있는 경우 사전에 (이메일 또는 지원 포털에 게시를 통해) 고객에게 알립니다.

(b) Customer may object to such changes as set out in Section 0.
고객은 이러한 변경에 대해 제 0 항에 명시된 바에 따라 이의를 제기할 수 있습니다.

6.3 Objections to New Subprocessors.
신규 협력업체에 대한 이의 제기.

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.
정보 보호 법률에 따라 고객에게 신규 협력업체의 개인 정보 처리와 관련한 이의 제기에 합법적인 사유가 있는 경우, 고객은 서면 통지를 SAP 에 제공하여 본 계약(신규 협력업체 사용이 의도된 클라우드 서비스에 한함)을 해지할 수 있습니다. 이러한 해지는 고객이 결정한 시점에 효력이 발생되지만, SAP 가 고객에게 신규 협력업체에 관해 통지한 날로부터 30 일을 초과할 수 없습니다. 고객이 해당 30 일 이내에 해지하지 않는 경우, 고객은 새로운 협력업체를 허용하는 것으로 간주됩니다.

(b) Within the thirty day period from the date of SAP's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect SAP's right to use the new Subprocessor(s) after the thirty day period.
SAP 가 고객에게 신규 협력업체에 관해 통지한 날로부터 30 일 이내에, 고객은 당사자들이 이의 제기에 대한 해결책을 함께 성실하게 논의할 것을 요청할 수 있습니다. 이러한 논의는 해지 기간을 연장하지 않으며 해당 30 일 기간 종료 후 신규 협력업체를 사용할 SAP 의 권한에 영향을 미치지 않습니다.

(c) Any termination under this Section 0 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.
본 제 0 항에 따른 해지는 일방 당사자에 의한 귀책 사유 없는 해지로 간주되며 본 계약 조건이 적용됩니다.

6.4 Emergency Replacement. SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 0 applies accordingly.
긴급 교체. SAP 는 변경의 사유가 SAP 의 합리적 통제를 벗어난 경우 보안 또는 다른 긴급한 이유로 인해 신속한 교체가 요구되는 경우, 사전 통지 없이 협력업체를 변경할 수 있습니다. 이 경우, SAP 는 교체 임명 후 가능한 빨리 고객에게 협력업체 교체를 통지합니다. 제 0 항이 이에 따라 적용됩니다.

7. INTERNATIONAL PROCESSING
국제적 처리

7.1 Conditions for International Processing. SAP shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.
국제적 처리의 조건. SAP 는 정보 보호 법률에서 허용된 바에 따라 고객이 위치한 국가 외부에서 본 DPA 에 의거하여 협력업체 사용을 포함하여 개인 정보를 처리할 권한이 있습니다.

7.2 Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of

the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

표준 계약 조항. (i) EEA 또는 스위스에 위치한 컨트롤러의 개인 정보가 EEA, 스위스 및 GDPR 제 45 조에 따른 적절한 수준의 정보 보호가 이루어지는 안전한 국가로 유럽연합이 인정하는 국가, 단체, 지역 외부의 국가에서 처리되는 경우, 또는 (ii) 다른 컨트롤러의 개인 정보가 국제적으로 처리되고 해당 국제 처리에 컨트롤러의 국가 법률에 따라 적절한 수단이 요구되며 요구되는 적절한 수단이 표준 계약 조항을 체결하여 이행될 수 있는 경우,

(a) SAP and Customer enter into the Standard Contractual Clauses;
SAP 와 고객은 표준 계약 조항을 체결합니다.

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by SAP) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when SAP has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 0, or a notice to Customer; and/or
(i) 고객이 권리 및 의무의 독립적인 소유자로서 SAP 또는 SAP SE 및 협력업체가 체결한 표준 계약 조항에 동의하거나("동의 모델"), (ii) 협력업체(SAP 가 대리함)가 고객과 표준 계약 조항을 체결함으로써("대리 모델"), 고객은 각 해당 협력업체와 표준 계약 조항을 체결합니다. 대리 모델은 SAP 가 제 6.1 항 제(c)호에 따라 제공되는 협력업체 목록을 통해 또는 고객 통지를 통해 협력업체가 자격을 갖추고 있음을 명백히 확인한 경우 적용됩니다.

(c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 0 0 and 0 above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.
본 계약에 따라 고객이 클라우드 서비스 사용을 승인한 다른 컨트롤러는 상기 제 0 항 제 0 호 및 제 0 호에 따라 고객과 동일한 방식으로 SAP 및/또는 해당 협력업체와 표준 계약 조항을 체결할 수 있습니다. 이 경우, 고객은 다른 컨트롤러를 대신하여 표준 계약 조항을 체결합니다.

7.3 Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.
본 계약과 표준 계약 조항의 관계. 본 계약의 어떠한 내용도 표준 계약 조항의 상충하는 조항에 우선하는 것으로 해석되지 않습니다. 좀 더 명확히 하자면, 본 DPA 에서 제 5 조 및 제 6 조에 명시된 감사 및 협력업체 규정이 추가로 명시되는 경우, 해당 명시 내용도 표준 계약 조항과 관련하여 적용됩니다.

7.4 Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.
표준 계약 조항의 준거법. 표준 계약 조항에는 해당 컨트롤러 법인이 설립된 국가의 법률이 적용됩니다.

8. DOCUMENTATION; RECORDS OF PROCESSING
문서, 처리의 기록

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.
각 당사자는 각자의 문서화 요건, 특히 정보 보호 법률에 따라 요구되는 경우 처리 기록 유지 요건에 대해 책임을 집니다. 각 당사자는 상대 당사자가 합리적으로 요청하는 방법으로(전자 시스템 사용 등) 상대 당사자에게 필요로

하는 정보를 제공하는 등 문서화 요건에 대해 상대 당사자를 합리적으로 지원하여 상대 당사자가 처리 기록 유지와 관련된 의무를 이행할 수 있도록 합니다.

9. EU ACCESS
EU 액세스

9.1 Optional Service. EU Access is an optional service that may be offered by SAP. If agreed in the Order Form for the eligible Cloud Service expressly identified there as being subject to EU Access, SAP shall provide the Cloud Service solely for production instances in accordance with this Section 9. Where EU Access is not agreed in the Order Form, this Section 9 shall not apply.
옵션 서비스. EU 액세스는 SAP 가 제공하는 옵션 서비스입니다. EU 액세스가 적용된다는 것이 명시적으로 파악된 적격 클라우드 서비스의 발주서에서 합의된 경우, SAP 는 본 제 9 조에 따라 운영 인스턴스에 대해서만 클라우드 서비스를 제공합니다. EU 액세스가 발주서에서 합의되지 않은 경우, 본 제 9 조는 적용되지 않습니다.

9.2 EU Access. SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service and SAP shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case by case basis; or as excluded under Section 0.
EU 액세스. SAP 는 클라우드 서비스의 개인 정보에 대한 액세스가 요구되는 지원을 제공하는 데 있어 유럽 지역의 협력업체만을 이용하고, SAP 는 고객이 각각 서면으로(이메일도 허용됨) 명시적으로 승인하거나 제 0 항의 예외사항을 제외하고는 EEA 또는 스위스 외부로 개인 정보를 내보낼 수 없습니다.

9.3 Data Center Location. Upon the effective date of the Agreement, 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.
데이터 센터 위치. 본 계약의 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.

9.4 Exclusions. The following Personal Data is not subject to 0 and 0:
예외. 제 0 항 및 제 0 항은 다음 개인 정보에 적용되지 않습니다.

(a) Contact details of the sender of a support ticket; and
지원 티켓 전송자의 세부 연락처 및

(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.
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.

10. DEFINITIONS
용어 정의

Capitalized terms not defined herein will have the meanings given to them in the Agreement.
본 문서에서 정의되지 않은 대문자로 시작되는 용어는 본 계약에서 해당 용어에 부여된 의미를 지닙니다.

10.1 "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; for the purposes of this DPA, where Customer acts as processor for another controller, it

shall in relation to SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

"컨트롤러"는 개인 정보의 처리 목적과 수단을 단독으로 또는 다른 기관과 공동으로 결정하는 자연인 또는 법인, 공공 기관, 단체 또는 기타 조직을 의미합니다. 본 DPA 의 목적상, 고객이 다른 컨트롤러의 처리자로서 역할을 하는 경우, 고객은 SAP 와 관련하여 본 DAP 에 따른 해당 컨트롤러 권한과 의무를 지닌 부가적이고 독립적인 컨트롤러로 간주됩니다.

10.2 **"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.

"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.

10.3 **"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 (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by SAP on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

"정보 보호 법률"은 개인의 기본 권리 및 자유와 본 계약에 따른 개인 정보 처리와 관련된 개인정보 보호 권리를 보호하는 관련 법률을 의미합니다(고객을 대신하는 SAP 의 개인 정보 처리와 관련된 당사자들 사이의 관계에 관한 한, 개인 정보에 대한 GDPR 적용 여부에 관계없이 GDPR 을 최소 기준으로 포함).

10.4 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

"정보 주체"는 정보 보호 법률에 규정된 식별되거나 식별 가능한 자연인을 의미합니다.

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

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

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

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

10.7 **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) 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 (as defined under the Agreement).

"개인 정보"는 정보 보호 법률에 따라 보호되는 정보 주체와 관련한 모든 정보를 의미합니다. DPA 의 목적상, 여기에는 (i) 고객 또는 고객의 공인 사용자가 입력하거나 이들의 클라우드 서비스 사용으로부터 기인하거나 (ii) SAP 또는 그 협력업체가 본 계약에 따른 지원을 제공하기 위해 제공받거나 액세스한 개인 정보만이 포함됩니다. 개인 정보는 고객 정보의 일부입니다(본 계약에 정의된 바에 따름).

10.8 **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

"개인 정보 위반"은 정보 보호 법률에 따라 컨트롤러가 관할 정보 보호 당국 또는 정보 주체에게 통지를 제공해야 하는 확인된 (1) 개인 정보의 우발적 또는 불법적 파괴, 손실, 변경, 무단 공개 또는 제 3 자의 무단 액세스 또는 (2) 개인 정보가 관련된 유사한 사고를 의미합니다.

10.9 **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.
"처리자"는 컨트롤러를 대신해서 개인 정보를 처리하는 자연인 또는 법인, 공공 기관, 단체 또는 기타 조직을 의미하며, 직접 컨트롤러의 처리자로서 역할을 하거나 컨트롤러를 대신하여 개인 정보를 처리하는 처리자의 협력업체로서 간접적으로 역할을 수행합니다.

10.10 **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses *current as of the effective date of the Agreement* are attached hereto as **Appendix 4**.
"표준 계약 조항"(또는 간혹 "EU 모델 조항"으로도 지칭됨)은 (표준 계약 조항(처리자)) 또는 유럽 위원회가 발행한 그 후속 버전(자동으로 적용됨)을 의미합니다.

10.11 **"Subprocessor"** means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP , SAP SE or SAP SE's Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.
"협력업체"는 SAP 계열사, SAP SE, SAP SE 계열사 및 본 클라우드 서비스와 관련하여 SAP, SAP SE 또는 SAP SE 의 계열사가 고용하여 본 DPA 에 따라 개인 정보를 처리하는 제 3 자를 의미합니다.

11. This DPA is executed in both korean and english language. in the event that there are differernt interpretations of the same provision or acutal contradictions between the two languages, the meanings of the english version shall prevail.
본 DPA 는 한국어와 영어로 체결됩니다. 양 언어간에 같은 조항을 두고 다른 해석을 하거나 실제 상이한 경우가 있는 경우, 영어가 우선합니다.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses
DPA 부록 1 및 (해당하는 경우) 표준 계약 조항

Data Exporter
데이터 엑스포터
The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.
데이터 엑스포터는 클라우드 서비스에 등록한 고객으로, 이를 통해 권한 있는 사용자가 개인 정보를 입력, 수정, 사용, 삭제 또는 처리할 수 있습니다. 다른 컨트롤러도 클라우드 서비스를 이용하도록 고객이 허용한 경우, 다른 컨트롤러도 데이터 엑스포터가 됩니다.

Data Importer
데이터 임포터
SAP and its Subprocessors provide the Cloud Service that includes the following support:
SAP 와 그 협력업체는 다음과 같은 지원이 포함된 클라우드 서비스를 제공합니다.

SAP SE 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:
SAP SE 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.

- Monitoring the Cloud Service
  클라우드 서비스 모니터링
- Backup & restoration of Customer Data stored in the Cloud Service
  클라우드 서비스에 저장된 고객 데이터의 백업 및 복구
- Release and development of fixes and upgrades to the Cloud Service
  클라우드 서비스의 수정 및 개선 사항의 발표 및 개발
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
  기본 클라우드 서비스 인프라 및 데이터베이스의 모니터링, 문제 해결 및 관리
- Security monitoring, network-based intrusion detection support, penetration testing
  보안 모니터링, 네트워크 기반 침입 감지 지원, 침투 테스트

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

Data Subjects
정보 주체
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.
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.

Data Categories
정보 범주
The transferred Personal Data concerns the following categories of data:
전송되는 개인 정보는 다음과 같은 범주의 데이터와 관련된 것입니다.

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 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.
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 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.

Special Data Categories (if appropriate)
특별 정보 범주(해당하는 경우)
The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.
전송되는 개인 정보는 해당하는 경우 본 계약(발주서 포함)에 명시된 바에 따른 다음과 같은 특별 범주의 정보와 관련된 것입니다.

Processing Operations / Purposes
처리 운영/목적
The transferred Personal Data is subject to the following basic processing activities:
전송되는 개인 정보는 다음과 같은 기본 처리 작업의 대상이 됩니다.

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
  클라우드 서비스를 설정, 운영, 모니터링, 제공하기 위한 개인 정보의 이용(조직적/기술적 지원 포함)
- provision of Consulting Services;
  컨설팅 서비스의 제공
- communication to Authorized Users
  권한 있는 사용자와의 통신
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
  전용 데이터 센터(멀티 테넌트 아키텍처)에 개인 정보 저장
- upload any fixes or upgrades to the Cloud Service
  수정 사항 업로드 및 클라우드 서비스 업그레이드
- back up of Personal Data
  개인 정보 백업
- computer processing of Personal Data, including data transmission, data retrieval, data access
  컴퓨터로 개인 정보 처리(데이터 전송, 데이터 검색, 데이터 액세스 포함)
- network access to allow Personal Data transfer
  개인 정보 전송을 허용하기 위한 네트워크 액세스
- execution of instructions of Customer in accordance with the Agreement.
  본 계약에 따른 고객 지침의 수행

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures
DPA 부록 2 및 (해당하는 경우) 표준 계약 조항 - 기술적/조직적 조치

This Appendix 2 comprises two sets of technical and organizational measures ("**TOMs**"):
이 DPA 부록 2 는 두 세트의 기술적 및 조직적 조치 ("**TOM**") 으로 구성되어 있습니다.

- **TOMs Set 1 (last updated April 2018, without change):** applies to all Cloud Services, except for the TOMs Set 2 Services defined below.
  TOM 세트 1 (2018 년 4 월 마지막 업데이트 후로 변경없음): 아래에 정의된 "TOM 세트 2 서비스"를 제외한 모든 클라우드 서비스에 적용됩니다.

- **TOMs Set 2**: applies to the TOMs Set 2 Services only. As of May 4, 2020, "**TOMs Set 2 Services**" means the following Cloud Services: SAP Analytics Cloud, SAP SuccessFactors and SAP Cloud Platform. SAP may remove a Cloud Service from the list of TOMs Set 2 Services from time to time, in which case such Cloud Service will be subject to TOMs Set 1.
  TOM 세트 2: TOM 세트 2 서비스에만 적용됩니다. 2020 년 5 월 4 일 기준으로, **"TOM 세트 2 서비스"**는 다음 클라우드 서비스를 의미합니다: SAP Analytics Cloud, SAP SuccessFactors, 및 SAP Cloud Platform. SAP 는 때때로 TOM 세트 2 서비스 목록에서 클라우드 서비스를 제외시킬 수 있으며, 이 경우 해당 클라우드 서비스는 TOM 세트 1 를 적용합니다.

TOMs SET 1
TOM 세트 1

Last Updated: April 2018
마지막 업데이트: 2018 년 4 월

1. TECHNICAL AND ORGANIZATIONAL MEASURES
기술적/조직적 조치

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.
다음 조항들은 SAP 의 현행 기술적/조직적 조치를 정의합니다. SAP 는 비슷하거나 그보다 높은 수준의 보안을 유지한다면 이를 통지 없이 언제든 변경할 수 있습니다. 개별 조치는, 개인 정보를 보호하는 보안 수준의 감소 없이, 동일한 목적의 새로운 조치로 대체될 수 있습니다.

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

Measures:
조치:

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
  SAP 는 SAP 보안 정책을 기반으로 적절한 수단을 사용하여 자산과 시설을 보호합니다.
- In general, buildings are secured through access control systems (e.g., smart card access system).
  일반적으로 건물은 액세스 제어 시스템(예: 스마트 카드 액세스 시스템)을 통해 보안됩니다.
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.

최소 요건으로, 건물의 가장 바깥쪽 출입 지점에는 현대식 활성 키 관리를 포함한 인증된 키 시스템을 장착해야 합니다.

- 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.
  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.
- 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.
  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 employees and external personnel must wear their ID cards at all SAP locations.
  SAP 직원 및 외부 인력은 모든 SAP 위치에서 ID 카드를 착용해야 합니다.

Additional measures for Data Centers:
데이터 센터의 추가 조치:

- 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 being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
  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 데이터 센터 시설 내부의 시스템과 인프라에 액세스합니다. 적절한 기능을 보호하기 위해, 물리적 보안 장비(예: 동작 센서, 카메라 등)의 정기적 유지보수를 수행합니다.
- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.
  SAP 와 모든 제 3 자 데이터 센터 공급업자는 데이터 센터 내의 SAP 사적 구역을 출입하는 승인된 인력의 이름과 시간을 기록합니다.

1.2 System Access Control. Data processing systems used to provide the Cloud Service must be prevented from being used without authorization.
시스템 액세스 제어. 클라우드 서비스를 제공하기 위해 사용되는 데이터 처리 시스템은 승인되지 않은 사용이 금지되어야 합니다.

Measures:
조치:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy
  개인 정보를 저장하고 처리하는 시스템을 포함하여 중요한 시스템의 경우 여러 인증 단계를 사용하여 액세스를 허가합니다. 인증은 SAP 보안 정책에 따라 규정된 과정을 통해 관리됩니다.
- All personnel access SAP's systems with a unique identifier (user ID).
  모든 인력은 고유 식별자(사용자 ID)를 이용해 SAP 시스템에 액세스합니다.
- SAP has procedures in place to so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.
  SAP 는 요청된 권한 변경이 SAP 보안 정책에 따라서만 실행되도록 보장하기 위한 절차를 갖추고 있습니다(예: 허가 없이는 어떤 권한도 부여되지 않음). 인력이 퇴직할 경우, 해당 인력의 액세스 권한은 철회됩니다.

- 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.
  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.
- The company network is protected from the public network by firewalls.
  회사 네트워크는 방화벽에 의해 공용 네트워크로부터 보호됩니다.
- 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.
  SAP 는 회사 네트워크로 진입하는 액세스 지점(이메일 계정)과 모든 파일 서버 및 모든 워크스테이션에 최신 바이러스 차단 소프트웨어를 사용합니다.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.
  보안 패치 관리가 관련 보안 업데이트의 정기적인 배포를 제공하기 위해 시행됩니다. SAP 회사 네트워크 및 중요한 인프라에 대한 완전한 원격 액세스는 강력한 인증에 의해 보호됩니다.

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.
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.

Measures:
조치:

- 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.
  SAP 보안 정책의 일환으로, 개인 정보는 SAP 정보 등급 표준에 따른 "비밀" 정보와 최소 동일한 수준의 보호가 요구됩니다.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
  개인 정보에 대한 액세스 권한은 알아야 할 필요가 있는 경우에만 부여됩니다. 인력은 업무 완수를 위해 필요한 정보에 대해 액세스 권한을 갖게 됩니다. SAP 는 부여 과정 및 각 계정(사용자 ID)에 대해 배정된 역할을 문서화하는 권한 부여 개념을 사용합니다. 모든 고객 정보는 SAP 보안 정책에 따라 보호됩니다.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.
  모든 운영 서버는 데이터 센터 또는 안전한 서버실 내에서 가동됩니다. 개인 정보 처리 애플리케이션을 보호하는 보안 조치에 대해 정기 점검이 이루어집니다. 이를 위해 SAP 는 자체 IT 시스템에 대한 내부 및 외부 보안 점검 및 침투 테스트를 수행합니다.
- SAP does not allow the installation of software that has not been approved by SAP.
  SAP 는 SAP 가 승인하지 않은 소프트웨어의 설치를 허용하지 않습니다.

- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.
  SAP 보안 표준은 더 이상 필요하지 않은 데이터 및 데이터 매체를 삭제 또는 파기하는 방법을 규정합니다.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at SAP to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

데이터 전송 제어. 본 계약에 따른 클라우드 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 제공하기 위해 적절한 조치가 SAP 에서 시행됩니다(예: 암호화, 납으로 차폐한 용기 등).

Measures:
조치:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
  SAP 내부 네트워크를 통한 개인 정보 전송은 SAP 보안 정책에 따라 보호됩니다.
- 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).
  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 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.

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.

Measures:
조치:

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
  SAP 는 승인된 인력에 한해 업무상 필요한 개인 정보에만 액세스할 수 있도록 허용합니다.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.
  SAP 는 가능한 기술적 범위의 클라우드 서비스 내에서 SAP 또는 그 협력업체에 의한 개인 정보의 입력, 수정 및 삭제 또는 차단을 위한 로그 시스템을 구현했습니다.

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 Agreement and related instructions of the customer.

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

Measures:
조치:

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
  SAP 는 제어 조치와 프로세스를 사용하여 SAP 와 고객, 협력업체 또는 기타 서비스 공급자 간의 계약 준수를 모니터링합니다.

- 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.
  SAP 보안 정책의 일환으로, 개인 정보는 SAP 정보 등급 표준에 따른 "비밀" 정보와 최소 동일한 수준의 보호가 요구됩니다.
- 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.
  모든 SAP 직원 및 하청 협력업체 또는 기타 서비스 제공자는 SAP 고객 및 파트너의 영업비밀 등 모든 민감한 정보를 비밀로 유지할 계약상의 책임이 있습니다.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.
가용성 제어. 우발적 또는 무단 파기 또는 손실로부터 개인 정보를 보호합니다.

Measures:
조치:

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
  SAP 는 정기 백업 절차를 활용하여 필요에 따라 비즈니스 핵심 시스템의 복구를 제공합니다.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
  SAP 는 무정전 전원공급장치(UPS, 배터리, 발전기 등)를 이용해 데이터 센터의 전원 공급을 보호합니다.
- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
  SAP 는 비즈니스 핵심 프로세스에 대한 비즈니스 비상 계획을 규정했으며, 문서에 자세히 명시된 바에 따라 또는 관련 클라우드 서비스의 발주서에 통합된 바에 따라 비즈니스 핵심 서비스를 위한 재해 복구 전략을 제공합니다.
- Emergency processes and systems are regularly tested.
  비상 절차 및 시스템에 대한 정기 테스트가 이루어집니다.

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.
데이터 분리 제어. 서로 다른 목적으로 수집된 개인 정보의 별도 처리가 가능합니다.

Measures:
조치:

- 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.
  SAP 는 여러 고객에서 비롯된 개인 정보를 분리하기 위해 배포된 소프트웨어(예: 다중 테넌시 또는 별도 시스템 환경)의 기술적 능력을 사용합니다.
- Customer (including its Controllers) has access only to its own data.
  고객(고객의 컨트롤러 포함)은 자신의 정보에만 액세스할 수 있습니다.
- If Personal Data is required to handle a support incident from 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.
  고객 정보가 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 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.
데이터 무결성 제어. 개인 정보는 프로세스 처리 활동 중에 온전성, 정확성, 최신성이 유지됩니다.

Measures:

조치:

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

SAP 는 무단 수정에 대한 보호로서 다중 방어 단계를 구현했습니다.

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

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

- Firewalls;
  방화벽
- Security Monitoring Center;
  보안 모니터링 센터
- Antivirus software;
  바이러스 방지 소프트웨어
- Backup and recovery;
  백업 및 복구
- External and internal penetration testing;
  외부 및 내부 침투 테스트
- Regular external audits to prove security measures.
  보안 조치를 증명할 정기적인 외부 감사

TOMs SET 2
TOM 세트 2

(*applies to TOMs Set 2 Services defined above*)
(위에 정의된 TOM 세트 2 서비스에 적용함**)**

LAST UPDATED: MAY 4, 2020
마지막 업데이트: 2020 년 5 월 4 일

1. TECHNICAL AND ORGANIZATIONAL MEASURES
기술적/조직적 조치

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.
다음 조항들은 SAP 의 현행 기술적/조직적 조치를 정의합니다. SAP 는 비슷하거나 그보다 높은 수준의 보안을 유지한다면 이를 통지 없이 언제든 변경할 수 있습니다. 개별 조치는, 개인 정보를 보호하는 보안 수준의 감소 없이, 동일한 목적의 새로운 조치로 대체될 수 있습니다.

1.1 Physical Access Control. 물리적 액세스 제어.

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
  SAP 는 SAP 보안 정책을 기반으로 적절한 수단을 사용하여 자산과 시설을 보호합니다.
- In general, buildings are secured through access control systems (e.g., smart card access system).
  일반적으로 건물은 액세스 제어 시스템(예: 스마트 카드 액세스 시스템)을 통해 보안됩니다.
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
  최소 요건으로, 건물의 가장 바깥쪽 출입 지점에는 현대식 활성 키 관리를 포함한 인증된 키 시스템을 장착해야 합니다.
- 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.
  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.
- 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.
  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 employees and external personnel must wear their ID cards at all SAP locations.
  SAP 직원 및 외부 인력은 모든 SAP 위치에서 ID 카드를 착용해야 합니다.

Additional measures for Data Centers:
데이터 센터의 추가 조치:

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

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

- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.
  SAP 와 모든 제 3 자 데이터 센터 공급업자는 데이터 센터 내의 SAP 사적 구역을 출입하는 승인된 인력의 이름과 시간을 기록합니다.

1.2 System Access Control. 시스템 액세스 제어.

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy
  개인 정보를 저장하고 처리하는 시스템을 포함하여 중요한 시스템의 경우 여러 인증 단계를 사용하여 액세스를 허가합니다. 인증은 SAP 보안 정책에 따라 규정된 과정을 통해 관리됩니다.
- All personnel access SAP's systems with a unique identifier (user ID).
  모든 인력은 고유 식별자(사용자 ID)를 이용해 SAP 시스템에 액세스합니다.
- SAP has policies designed to provide that no rights are granted without authorization and in case personnel leaves the company their access rights are revoked.
  SAP 는 허가 없이는 어떠한 권한도 주어지지 않고 인력이 퇴직할 경우 해당 인력의 액세스 권한이 철회되도록 고안된 정책을 갖추고 있습니다.
- 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.
  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.
- The company network is protected from the public network by firewalls.
  회사 네트워크는 방화벽에 의해 공용 네트워크로부터 보호됩니다.
- 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.
  SAP 는 회사 네트워크로 진입하는 액세스 지점(이메일 계정)과 모든 파일 서버 및 모든 워크스테이션에 최신 바이러스 차단 소프트웨어를 사용합니다.
- Security patch management processes to deploy relevant security updates on a regular and periodic basis.
  정기적으로 관련 보안 업데이트 배포하기 위한 보안 패치 관리 과정.
- Full remote access to SAP's corporate network and critical infrastructure is protected by authentication.
  SAP 회사 네트워크 및 중요 기반 시설에 대한 원격 접속은 인증에 의해 보호됩니다.

1.3 Data Access Control. 데이터 액세스 제어.

- 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.

SAP 보안 정책의 일환으로, 개인 정보는 SAP 정보 등급 표준에 따른 "비밀" 정보와 최소 동일한 수준의 보호가 요구됩니다.

- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
  개인 정보에 대한 액세스 권한은 알아야 할 필요가 있는 경우에만 부여됩니다. 인력은 업무 완수를 위해 필요한 정보에 대해 액세스 권한을 갖게 됩니다. SAP 는 부여 과정 및 각 계정(사용자 ID)에 대해 배정된 역할을 문서화하는 권한 부여 개념을 사용합니다. 모든 고객 정보는 SAP 보안 정책에 따라 보호됩니다.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and/or penetration tests on its IT systems.
  모든 운영 서버는 데이터 센터 또는 안전한 서버실 내에서 가동됩니다. 개인 정보 처리 애플리케이션을 보호하는 보안 조치에 대해 정기 점검이 이루어집니다. 이를 위해 SAP 는 자체 IT 시스템에 대한 내부 및 외부 보안 점검 및/또는 침투 테스트를 수행합니다.
- SAP has processes and policies to detect the installation of unapproved software on production systems.
  SAP 는 운영 시스템에 승인되지 않은 소프트웨어의 설치를 감지하기 위한 과정과 정책을 갖추고 있습니다.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.
  SAP 보안 표준은 더 이상 필요하지 않은 데이터 및 데이터 매체를 삭제 또는 파기하는 방법을 규정합니다.

1.4 Data Transmission Control. 데이터 전송 제어.

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
  SAP 내부 네트워크를 통한 개인 정보 전송은 SAP 보안 정책에 따라 보호됩니다.
- 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).
  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 Data Input Control. 데이터 입력 제어.

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
  SAP 는 승인된 인력에 한해 업무상 필요한 개인 정보에만 액세스할 수 있도록 허용합니다.
- SAP has in most cases implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.
  SAP 는 대부분의 경우 가능한 기술적 범위의 클라우드 서비스 내에서 SAP 또는 그 협력업체에 의한 개인 정보의 입력, 수정 및 삭제 또는 차단을 위한 로그 시스템을 구현했습니다.

1.6 Job Control. 작업 제어.

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
  SAP 는 제어 조치와 프로세스를 사용하여 SAP 와 고객, 협력업체 또는 기타 서비스 공급자 간의 계약 준수를 모니터링합니다.

- 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.
  SAP 보안 정책의 일환으로, 개인 정보는 SAP 정보 등급 표준에 따른 "비밀" 정보와 최소 동일한 수준의 보호가 요구됩니다.
- 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.
  모든 SAP 직원 및 하청 협력업체 또는 기타 서비스 제공자는 SAP 고객 및 파트너의 영업비밀 등 모든 민감한 정보를 비밀로 유지할 계약상의 책임이 있습니다.

1.7 Availability Control. 가용성 제어.

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
  SAP 는 정기 백업 절차를 활용하여 필요에 따라 비즈니스 핵심 시스템의 복구를 제공합니다.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
  SAP 는 무정전 전원공급장치(UPS, 배터리, 발전기 등)를 이용해 데이터 센터의 전원 공급을 보호합니다.
- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
  SAP 는 비즈니스 핵심 프로세스에 대한 비즈니스 비상 계획을 규정했으며, 문서에 자세히 명시된 바에 따라 또는 관련 클라우드 서비스의 발주서에 통합된 바에 따라 비즈니스 핵심 서비스를 위한 재해 복구 전략을 제공합니다.
- Emergency processes and systems are regularly tested.
  비상 절차 및 시스템에 대한 정기 테스트가 이루어집니다.

1.8 Data Separation Control. 데이터 분리 제어.

- 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.
  SAP 는 여러 고객에서 비롯된 개인 정보를 분리하기 위해 배포된 소프트웨어(예: 다중 테넌시 또는 별도 시스템 환경)의 기술적 능력을 사용합니다.
- Customer (including its Controllers) has access only to its own data.
  고객(고객의 컨트롤러 포함)은 자신의 정보에만 액세스할 수 있습니다.
- If Personal Data is required to handle a support incident from 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.
  고객 정보가 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 Data Integrity Control. 데이터 무결성 제어.

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.
SAP 는 무단 수정에 대한 보호로서 다중 방어 단계를 구현했습니다.
In particular, SAP uses the following to implement the control and measure sections described above:
SAP 는 위에 설명된 관리 및 조치 조항을 실행하기 위해 특히 다음을 사용합니다.

- Firewalls;
  방화벽
- Security Monitoring Center;
  보안 모니터링 센터
- Antivirus software;

바이러스 방지 소프트웨어

- Backup and recovery;
  백업 및 복구
- External and internal penetration testing and/or regular external audits to prove security measures.
  외부 및 내부 침투 테스트 및/또는 보안 조치를 증명할 정기적인 외부 감사

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses
DPA 부록 3 및 (해당하는 경우) 표준 계약 조항

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.
다음 표는 GDPR 관련 조항과 DPA 해당 조건을 명시합니다(예시용으로만 작성됨)

Article of GDPF	**Section of DPA**	**Click on link to see Section**
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures
28(2), 28(3) (d) and 28 (4)	6	Subprocessors
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application Structure
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures
28(3) (e)	3.4	Cooperation
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data export and Deletion.
28(3) (h)	5	Certifications and Audits
28 (4)	6	Subprocessor
30	8	Documentation; Records of processing.
46(2) (c)	7.2	Standard Contractual Clauses.

Appendix 4
부록 4

The Standard Contractual Clauses set out in this Appendix 4 are current as at 31 March 2018, and the Korean translation is provided as a matter of convenience only. The English language version controls. These Standard Contractual Clauses are automatically subject to all updates by the European Commission and as subsequently published by the European Commission. Customer should always access the URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 for the current versions of the Standard Contractual Clauses. Customer's local language may not be supported at the European Commission, or at its URL. It will be Customer's responsibility to ensure that it is aware of the current version/s of the Standard Contractual Clauses and to manage for itself and its Controllers all required translations of the updated Standard Contractual Clauses.

본 부록 4 에 명시된 표준계약조항은 2018 년 3 월 31 일 현재 버젼으로 한국어 번역은 오로지 편의상 제공되고, 영어 버젼이 우선합니다. 이들 표준계약조항은 유럽위원회에 의해 전부 자동적으로 업데이트된 후 게재합니다. 고객은 표준계약조항의 현재 버젼 확인을 위해 URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 에 접속해야 합니다. 유럽위원회에서 또는 이 URL 에서 고객의 현지 언어가 지원되지 않을 수 있습니다. 표준계약조항의 현재 버전을 인지하고, 고객과 컨트롤러를 위해 업데이트된 표준계약조항의 모든 필요한 번역본을 관리할 책임은 고객에게 있습니다.

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]
표준 계약 조항(처리자)[2]

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection
적절한 수준의 정보 보호를 보장하지 않는 제 3 국에 있는 처리자로 개인 정보를 전송하는 것에 대한 Directive 95/46/EC 제 26 조 제(2)항(또는 2018 년 5 월 25 일 이후, 규정 2016/79 제 44 조 이하)의 목적상,

Customer also on behalf of the other Controllers
(in the Clauses hereinafter referred to as the '**data exporter'**)
다른 컨트롤러 또한 대신하는 고객
(이하 조항에서 '**데이터 엑스포터**')

and
당사자 2:

SAP
(in the Clauses hereinafter referred to as the **'data importer'**)
SAP
(이하 조항에서 '**데이터 임포터**')

each a 'party'; together 'the parties',
각각 '당사자', 통칭하여 '당사자들'은

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

[2] 2010년 2월 5일자 위원회 결정(2010/87/EU)에 의거

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.
부록 1 에 규정된 개인 정보를 데이터 엑스포터가 데이터 임포터에게 전송하는 것에 대한 개인 정보 보호와 개인의 기본 권리 및 자유와 관련된 적절한 안전 장치를 제시할 수 있도록 다음의 계약 조항(조항)에 합의했습니다.

Clause 1
조항 1

Definitions
용어 정의

For the purposes of the Clauses:
조항의 목적상

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
'개인 정보', '특별 데이터 범주', '처리', '컨트롤러', '처리자', '정보 주체' 및 '감독 기관'은 개인 정보의 처리 및 자유로운 이동과 관련된 개인 보호에 대한 유럽 의회 및 위원회의 1995 년 10 월 24 일자 지침 95/46/EC 에서의 의미와 동일한 의미를 갖습니다.

(b) 'the data exporter' means the controller who transfers the personal data;
'데이터 엑스포터'는 개인 정보를 전송하는 컨트롤러를 의미합니다.

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
'데이터 임포터'는 데이터 엑스포터로부터 개인 정보를 전송받은 후 데이터 엑스포터의 지침 및 조항의 조건에 따라 데이터 엑스포터를 대신하여 개인 정보를 처리하기로 동의한 처리자를 의미하며 지침 95/46/EC 의 제 25 조 제(1)항의 의미 내에서 적절한 보호를 보장하는 제 3 국 제도가 적용되지 않습니다.

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
'협력업체'는 데이터 엑스포터로부터 개인 정보를 전송받은 후 데이터 엑스포터의 지침, 조항의 조건 및 하청 계약서의 조건에 따라 데이터 엑스포터를 대신하여 오직 처리 활동만을 하기로 동의한 업체로, 데이터 임포터 또는 데이터 임포터의 다른 협력업체에 의해 참여하게 된 처리자를 의미합니다.

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'해당 정보 보호 법률'은 개인의 기본 권리와 자유, 특히 데이터 엑스포터가 설립된 회원 국가의 컨트롤러에 적용할 수 있는 개인 정보의 처리와 관련된 개인정보 보호 권리를 보호하는 법률을 의미합니다.

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

'기술적, 조직적 보안 조치'란 특히 처리가 네트워크를 통한 데이터 전송과 관련된 경우 우발적 또는 불법적 파괴, 우발적 손실, 변경, 무단 공개 또는 액세스와 기타 모든 불법적 형태의 처리로부터 개인 정보를 보호하기 위한 조치를 의미합니다.

Clause 2
조항 2

Details of the transfer
전송 세부 사항

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.
전송 세부 사항과 특히 특별 개인 데이터 범주(해당되는 경우)는 본 조항의 중요한 부분을 구성하는 부록 1 에 명시되어 있습니다.

Clause 3
조항 3

Third-party beneficiary clause
제 3 자 수혜자 조항

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

정보 주체는 제 3 자 수혜자로서 데이터 엑스포터를 대상으로 본 조항, 조항 4(b)~(i), 조항 5(a)~(e) 및 (g)~(j), 6(1) 및 (2), 조항 7, 조항 8(2), 조항 9~12 를 시행할 수 있습니다.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7,Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

데이터 엑스포터가 사실상 없어지거나 법적으로 소멸된 경우 정보 주체는 데이터 임포터를 대상으로 본 조항, 조항 5(a)~(e) 및 (g), 조항 6, 조항 7, 조항 8(2), 조항 9~12 를 시행할 수 있습니다. 단, 후임 법인이 계약 또는 법률 운용에 따른 데이터 엑스포터의 모든 법적 책임을 지고 데이터 엑스포터의 권리와 의무를 맡게 된 경우, 정보 주체는 해당 법인을 대상으로 이를 시행할 수 있습니다.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and

obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

데이터 엑스포터와 데이터 임포터 둘 다 사실상 없어지거나 법적으로 소멸되거나 파산한 경우 정보 주체는 협력업체를 대상으로 본 조항, 조항 5(a)~(e) 및 (g), 조항 6, 조항 7, 조항 8(2), 조항 9~12 를 시행할 수 있습니다. 단, 후임 법인이 계약 또는 법률 운용에 따른 데이터 엑스포터의 모든 법적 책임을 지고 데이터 엑스포터의 권리와 의무를 맡게 된 경우, 정보 주체는 해당 법인을 대상으로 이를 시행할 수 있습니다. 이러한 협력업체의 제 3 자 책임은 본 조항에 따른 자체 처리 작업으로 제한됩니다.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

당사자들은 정보 주체가 명시적으로 원하고 국가 법으로 허용되는 경우 협회 또는 기타 단체가 정보 주체를 대표하는 것에 반대하지 않습니다.

Clause 4
조항 4

Obligations of the data exporter
데이터 엑스포터의 의무

The data exporter agrees and warrants:
데이터 엑스포터는 다음 내용에 동의하고 이를 보증합니다.

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

전송 자체를 포함하여 개인 정보의 처리는 해당 정보 보호 법률의 관련 조항에 따라 수행되어 왔고 지속적으로 수행될 것이며(해당되는 경우, 데이터 엑스포터가 설립된 회원 국가의 관련 당국에 통지됨) 해당 국가의 관련 조항을 위반하지 않습니다.

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

개인 정보 처리 서비스 전체 기간 동안 해당 정보 보호 법률 및 본 조항에 따라 오직 데이터 엑스포터를 대신해서만 전송된 개인 정보를 처리하도록 데이터 임포터에게 지시해왔고 지시할 것입니다.

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

데이터 임포터는 본 계약서의 부록 2 에 명시된 기술적, 조직적 보안 조치에 관하여 충분한 보장을 제공할 것입니다.

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

해당 정보 보호 법률의 요건에 대한 평가 후, 네트워크를 통한 데이터 전송과 관련된 처리의 경우, 보안 조치가 우발적 또는 불법적 파괴, 우발적 손실, 변경, 무단 공개 또는 액세스 및 기타 모든 불법적 형태의 처리로부터 개인 정보를 보호하기에 적합하며, 이러한 조치가 처리로 인해 제시되는 위험과 구현 비용 및 기술 상태를 고려한 보호 대상 정보의 특성에 적합한 보안 수준임을 확인합니다.

(e) that it will ensure compliance with the security measures;
보안 조치를 준수할 것입니다.

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
특별 데이터 범주와 관련된 전송의 경우, 정보 주체는 지침 95/46/EC 의 의미 내에서 적절한 보호 수단을 제공하지 않는 제 3 국으로 자신의 데이터가 전송될 수 있음을 전송되기 전 또는 전송된 후에 최대한 빨리 통지 받게 될 것입니다.

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
데이터 엑스포터가 전송을 계속하거나 중단을 해제하기로 결정한 경우, 데이터 임포터 또는 협력업체로부터 받은 모든 통지를 조항 5(b) 및 조항 8(3)에 따라 데이터 보호 감독 기관에 전달합니다.

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
정보 주체가 조항 사본을 요청하면 부록 2 를 제외하고 보안 조치 요약 설명과 본 조항에 따라 체결된 하청 서비스 계약서 사본을 제공합니다. 단, 조항 또는 계약서에 상업 정보가 포함되어 있는 경우 해당 상업 정보는 제거할 수 있습니다.

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
하청의 경우, 본 조항에 의거해 데이터 임포터인 정보 주체의 권리 및 개인 정보에 대한 보호 수준과 동일한 수준의 보호를 제공하는 협력업체가 조항 11 에 따라 처리 활동을 수행합니다.

(j) that it will ensure compliance with Clause 4(a) to (i).
조항 4(a)~(i)를 준수할 것입니다.

Clause 5
조항 5

Obligations of the data importer
데이터 임포터의 의무

The data importer agrees and warrants:
데이터 임포터는 다음 내용에 동의하고 이를 보증합니다.

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

데이터 엑스포터의 지시 및 본 조항에 따라 오직 데이터 엑스포터를 대신해서만 개인 정보를 처리합니다. 어떤 이유로든 해당 준수를 제공할 수 없을 경우에는 이를 즉시 데이터 엑스포터에게 알릴 것에 동의하며, 이 경우 데이터 엑스포터는 데이터 전송을 중단하거나 계약을 해지할 수 있습니다.

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

데이터 임포터에게 적용되는 법률은 데이터 엑스포터로부터 받은 지침과 계약에 따른 의무 이행을 방해하지 않습니다. 이 법률이 변경되어 본 조항을 통해 제공되는 본 의무와 보증에 상당한 역효과를 미칠 가능성이 높은 경우에는 이러한 사실을 인지하는 즉시 데이터 엑스포터에게 통지할 것이며, 이 경우 데이터 엑스포터는 데이터 전송을 중단하거나 계약을 해지할 수 있습니다.

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

전송된 개인 정보를 처리하기 전에 부록 2 에 명시된 기술적, 조직적 보안 조치를 시행했습니다.

(d) that it will promptly notify the data exporter about:

다음의 경우 데이터 엑스포터에게 즉시 통지할 것입니다.

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

법 집행기관에 의한 법적으로 구속력 있는 개인 정보 공개 요청(단, 법적 조사의 비밀 정보의 유지를 위한 형법에 따른 금지 등과 같이 달리 금지된 경우는 제외)

(ii) any accidental or unauthorised access; and

우발적 또는 무단 액세스

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

정보 주체로부터 받은 직접 요청. 이 경우 이에 대한 응답 없이 통지(그렇게 하도록 달리 승인을 받은 경우는 제외)

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

전송 대상인 개인 정보의 처리와 관련하여 데이터 엑스포터로부터 받은 모든 질의를 즉시 적절하게 처리하고, 전송된 정보의 처리와 관련된 감독 기관의 조언을 준수합니다.

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required

professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

본 조항에 포함되는 처리 활동의 감사를 위해 데이터 엑스포터가 요청하면 데이터 처리 시설을 제공합니다. 이러한 감사는 데이터 엑스포터 또는 비밀 유지 의무에 구속되는 필수 전문 자격을 소유하고 있고 데이터 엑스포터가 선정한 독립적 회원으로 구성된 검사 기관에 의해 수행되며, 해당되는 경우 감독 기관과 협의합니다.

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

정보 주체가 요청하면 본 조항의 사본 또는 하청에 대한 기존 계약서를 제공합니다. 단, 조항 또는 계약서에 상업 정보가 포함되어 있는 경우 해당 상업 정보는 제거할 수 있습니다. 정보 주체가 데이터 엑스포터로부터 사본을 얻을 수 없는 경우 부록 2 는 보안 조치에 대한 요약 설명으로 대체됩니다.

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

하청을 하게 되는 경우, 데이터 엑스포터에게 미리 알리고 사전 서면 동의를 얻습니다.

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

협력업체에 의한 처리 서비스는 조항 11 에 따라 수행될 것입니다.

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

본 조항에 의거하여 체결한 모든 하청 계약의 사본을 데이터 엑스포터에게 즉시 보냅니다.

Clause 6
조항 6

Liability
책임

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

당사자들은 일방 당사자 또는 협력업체가 조항 3 또는 조항 11 관련 의무를 위반하여 정보 주체가 손해를 입은 경우 정보 주체는 해당 손해에 대해 데이터 엑스포터로부터 보상을 받을 수 있음에 동의합니다.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

데이터 엑스포터가 사실상 없어졌거나 법적으로 소멸되었거나 파산했기 때문에 데이터 임포터 또는 그 협력업체의 조항 3 또는 조항 11 관련 의무 위반으로 인해 발생한 손해에 대해 정보 주체가 데이터

엑스포터에게 위 1 항에 따른 보상을 청구할 수 없는 경우, 데이터 임포터는 정보 주체가 데이터 임포터가 마치 데이터 엑스포터인 것처럼 데이터 임포터에게 보상을 청구할 수 있음에 동의합니다. 단, 후임 법인이 계약 또는 법률 운용에 따른 데이터 엑스포터의 모든 법적 책임을 지게 된 경우, 정보 주체는 해당 법인을 대상으로 이 권리를 시행할 수 있습니다.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
데이터 임포터는 협력업체의 의무 위반을 구실로 자신의 책임을 회피할 수 없습니다.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

데이터 엑스포터 또는 데이터 임포터가 사실상 없어졌거나 법적으로 소멸되었거나 파산했기 때문에 협력업체의 조항 3 또는 조항 11 관련 의무 위반으로 인해 발생한 손해에 대해 정보 주체가 데이터 엑스포터 또는 데이터 임포터에게 1 항 및 2 항에 따른 보상을 청구할 수 없는 경우, 협력업체는 정보 주체가 협력업체가 마치 데이터 엑스포터 또는 데이터 임포터인 것처럼 협력업체에 보상을 청구할 수 있음에 동의합니다. 단, 후임 법인이 계약 또는 법률 운용에 따른 데이터 엑스포터 또는 데이터 임포터의 모든 법적 책임을 지게 된 경우, 정보 주체는 해당 법인을 대상으로 이 권리를 시행할 수 있습니다. 협력업체의 책임은 본 조항에 따른 자체 처리 작업으로 제한됩니다.

Clause 7
조항 7

Mediation and jurisdiction
중재 및 관할권

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

데이터 임포터는 정보 주체가 제 3 자 수혜자 권리를 적용하거나 본 조항에 따라 손해 보상을 청구하는 경우 다음과 같은 정보 주체의 결정을 받아들일 것에 동의합니다.

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

독립적 개인 또는 감독 기관(해당되는 경우)에 분쟁에 대한 중재를 회부합니다.

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

데이터 엑스포터가 설립된 회원 국가의 법원에 분쟁에 대한 판결을 회부합니다.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

당사자들은 정보 주체의 선택이 국내법 또는 국제법의 기타 규정에 따라 구제책을 모색하기 위한 실질적, 절차적 권한을 침해하지 않을 것에 동의합니다.

Clause 8
조항 8

Cooperation with supervisory authorities
감독 기관과의 협력

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
데이터 엑스포터는 해당 정보 보호 법률에 따라 요구되거나 감독 기관의 요청이 있는 경우 감독 기관에 본 계약서의 사본을 보관할 것에 동의합니다.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
당사자들은 해당 데이터 보호법에 따라 데이터 엑스포터의 감사에 적용되는 것과 동일한 범위 및 동일한 조건으로 데이터 임포터 및 그 협력업체에 대한 감사를 수행할 권한이 감독 기관에 있다는 것에 동의합니다.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).
데이터 임포터는 상기 2 항에 따라 감사에 적용되는 법률이 있거나 데이터 임포터 또는 협력업체에 대한 감사의 수행을 막는 협력업체가 있을 경우 이를 즉시 데이터 엑스포터에게 알립니다. 이 경우 데이터 엑스포터는 조항 5(b)에 예견된 조치를 취할 수 있습니다.

Clause 9
조항 9

Governing law
준거법

The Clauses shall be governed by the law of the Member State in which the data exporter is established.
본 조항에는 데이터 엑스포터가 설립된 회원 국가의 법률이 적용됩니다.

Clause 10
조항 10

Variation of the contract
계약 변경

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

당사자들은 본 조항을 변경하거나 수정하지 않습니다. 이는 당사자들이 필요한 경우 본 조항과 모순되지 않는 범위 내에서 업무 관련 문제에 대한 조항을 추가하는 것을 제한하지 않습니다.

Clause 11
조항 11

Sub-processing
처리 작업의 하청

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

데이터 임포터는 데이터 엑스포터의 사전 서면 동의 없이 본 조항에 따라 데이터 엑스포터를 대신하여 수행하는 처리 작업을 하청하지 않습니다. 데이터 임포터가 데이터 엑스포터의 동의를 받은 후 본 조항에 따른 의무를 하청하는 경우, 이는 본 조항에 따라 데이터 임포터에 부과되는 것과 동일한 의무를 협력업체에 부과하는 서면 계약을 협력업체와 체결해야만 가능합니다. 협력업체가 해당 서면 계약에 따른 데이터 보호 의무를 완수하지 못한 경우 데이터 임포터는 해당 계약에 따른 협력업체의 의무 수행과 관련하여 데이터 엑스포터에 대한 모든 책임을 집니다.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

데이터 엑스포터 또는 데이터 임포터가 사실상 없어졌거나 법적으로 소멸되었거나 파산했고 계약 또는 법률 운용에 따른 데이터 엑스포터 또는 데이터 임포터의 모든 법적 책임을 지는 후임 법인이 없기 때문에 정보 주체가 데이터 엑스포터 또는 데이터 임포터에게 조항 6 의 1 항에 언급된 보상 청구를 제기할 수 없는 경우, 데이터 임포터와 협력업체 간 사전 서면 계약은 또한 조항 3 에 규정된 바와 같이 제 3 자 수혜자 조항을 제공합니다. 이러한 협력업체의 제 3 자 책임은 본 조항에 따른 자체 처리 작업으로 제한됩니다.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

제 1 항에 언급된 계약의 하청에 대한 데이터 보호 측면과 관련된 조항에는 데이터 엑스포터가 설립된 회원 국가의 법률이 적용됩니다.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

데이터 엑스포터는 본 조항에 따라 체결되고 조항 5(j)에 따라 데이터 임포터가 통지한 하청 계약 목록을 보관하며 1년에 한 번 이상 업데이트합니다. 데이터 엑스포터의 데이터 보호 감독 기관은 이 목록을 이용할 수 있습니다.

Clause 12
조항 12

Obligation after the termination of personal data-processing services
개인 정보 처리 서비스의 해지 후 의무

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

당사자들은 데이터 처리 서비스 제공의 해지 시 데이터 임포터 및 협력업체는 데이터 엑스포터의 선택에 따라 전송된 모든 개인 정보 및 그 사본을 데이터 엑스포터에게 반납하거나 모든 개인 정보를 파기하고 이를 데이터 엑스포터에게 증명할 것에 동의합니다. 단, 법률에 따라 데이터 임포터가 전송된 개인 정보의 전부 또는 일부를 반납하거나 파기할 수 없는 경우는 제외합니다. 이러한 경우 데이터 임포터는 전송된 개인 정보의 비밀 유지를 보장하고 전송된 개인 정보를 더 이상 적극적으로 처리하지 않을 것임을 보증합니다.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

데이터 임포터와 협력업체는 데이터 엑스포터 및/또는 감독 기관이 요청할 경우 1항에 언급된 조치의 감사를 위해 데이터 처리 시설을 제공할 것을 보증합니다.