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.

This document has been executed in the English and Slovak language. In the case of ambiguity or discrepancies between the two versions, the English version shall prevail.

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).

ZMLUVA O SPRACOVANÍ OSOBNÝCH ÚDAJOV PRE CLOUDOVÉ SLUŽBY SAP

1. POZADIE

1.1 Účel.

Tento dokument je zmluvou o spracovaní údajov („**ZSU**") medzi spoločnosťou SAP a Zákazníkom a vzťahuje sa na Osobné údaje, ktoré poskytne Zákazník a každý Prevádzkovateľ v súvislosti so svojím používaním Cloudovej služby. Určuje technické a organizačné opatrenia, ktoré spoločnosť SAP využíva pri ochrane Osobných údajov, ktoré sú uložené v produktívnom systéme Cloudovej služby.

Tento dokument je vyhotovený v anglickom a slovenskom jazyku. V prípade nejednoznačností alebo nezrovnalostí medzi oboma verziami, je rozhodujúca anglická verzia.

1.2 Uplatňovanie Štandardných zmluvných doložiek.

Ak súčasťou spracovania Osobných údajov je aj Medzinárodný prenos, uplatňujú sa Štandardné zmluvné doložky, ako sú uvedené v Článku 5 a zahrnuté formou odkazu.

1.3 Dozor.

Okrem prípadov uvedených v Článku 5.2 za správu všetkých požiadaviek od ostatných Prevádzkovateľov zodpovedá výlučne Zákazník. Zákazník musí všetkých ostatných Prevádzkovateľov, ktorým povolí používať Cloudovú službu, zmluvne zaviazať k dodržiavaniu podmienok tejto ZSU.

2. DODATKY

Účely zhromažďovania a spracovania Osobných údajov v Cloudovej službe určujú Zákazník a jeho Prevádzkovatelia. Príloha 1 obsahuje podrobné informácie o spracovaní, ktoré spoločnosť SAP bude poskytovať prostredníctvom Cloudovej služby. Príloha 2 obsahuje technické a organizačné opatrenia, ktoré spoločnosť SAP uplatňuje na Cloudovú službu, ak v Zmluve nie je uvedené inak.

3. POVINNOSTI SPOLOČNOSTI SAP

3.1 Pokyny od Zákazníka.

Spoločnosť SAP bude dodržiavať pokyny, ktoré v súvislosti s Osobnými údajmi prijme od Zákazníka (v jeho mene alebo v mene jeho Prevádzkovateľov), (i) ak nie sú v rozpore so zákonom alebo (ii) ak nevyžadujú vykonanie zásadných zmien v Cloudovej službe. Spoločnosť SAP môže opravovať alebo odstraňovať Osobné údaje v súlade s pokynmi Zákazníka. Ak spoločnosť SAP nemôže vyhovieť týmto pokynom, ihneď na to upozorní

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.

(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.

Zákazníka (na tento účel sa môže použiť aj e-mail).

3.2 Dôvernosť údajov.
Na spracovanie Osobných údajov spoločnosť SAP a jej Subdodávatelia budú používať iba personál, ktorý má záväznú povinnosť zachovávať dôvernosť údajov a telekomunikačných operácií v súlade so Zákonom o ochrane údajov. Spoločnosť SAP a jej Subdodávatelia poskytnú jednotlivcom, ktorí majú prístup k Osobným údajom, riadne školenie o opatreniach na zabezpečenie a ochranu údajov.

3.3 Technické a organizačné opatrenia.

(a) Spoločnosť SAP bude používať primerané technické a organizačné opatrenia, ktoré sú uvedené v Prílohe 2.

(b) Príloha 2 sa vzťahuje na produktívny systém Cloudovej služby. Zákazník nesmie uchovávať žiadne Osobné údaje v iných než produktívnych prostrediach.

(c) Spoločnosť SAP poskytuje Cloudovú službu celej zákazníckej základni spoločnosti SAP, ktorá je hostovaná z rovnakého dátového centra a ktorá odoberá rovnakú Cloudovú službu. Zákazník súhlasí s tým, že spoločnosť SAP bude zdokonaľovať opatrenia uvedené v Prílohe 2, ktoré sa týkajú ochrany Osobných údajov, ak to nepovedie k zníženiu úrovne ochrany údajov.

3.4 Upozorňovanie na porušenie dôvernosti.
Ak spoločnosť SAP zistí, že došlo k Porušeniu dôvernosti, ihneď o tom informuje Zákazníka.

3.5 Spolupráca.
Spoločnosť SAP bude na žiadosť Zákazníka poskytovať Zákazníkovi alebo Prevádzkovateľovi primeranú podporu pri spracovaní požiadaviek Dotknutých osôb alebo dozorných orgánov, ktoré sa týkajú spracovania Osobných údajov spoločnosťou SAP.

4. SUBDODÁVATELIA

4.1 Povolené používanie.

(a) Zákazník a Prevádzkovatelia oprávňujú spoločnosť SAP na využívanie služieb Subdodávateľov pri spracovaní Osobných údajov. Za všetky porušenia Zmluvy zo strany svojich Subdodávateľov zodpovedá spoločnosť SAP.

(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 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.

(b) Subdodávatelia majú v súvislosti s ich spracovávaním Osobných údajov rovnaké povinnosti, aké má aj spoločnosť SAP ako Spracovateľ (alebo Subdodávateľ).

(c) Spoločnosť SAP pred výberom Subdodávateľa vykoná jeho hodnotenie z hľadiska uplatňovania zabezpečenia, ochrany a dôvernosti. Subdodávatelia môžu mať bezpečnostné certifikáty, ktoré osvedčujú, že používajú primerané bezpečnostné opatrenia. Ak ich nemajú, spoločnosť SAP bude pravidelne hodnotiť bezpečnostné postupy Subdodávateľa, ktoré sa týkajú manipulácie s údajmi.

(d) Spoločnosť SAP na požiadanie Zákazníka informuje Zákazníka o názve, adrese a role každého Subdodávateľa, ktorého využíva pri poskytovaní Cloudovej služby.

4.2 Noví subdodávatelia.
Spoločnosť SAP využíva služby Subdodávateľov podľa vlastného uváženia, musí však pri tom splniť tieto podmienky:

(a) Spoločnosť SAP vopred upozorní Zákazníka (e-mailom alebo zverejnením na portáli Support Portal) na akékoľvek zmeny v zozname aktívnych Subdodávateľov k Dátumu nadobudnutia účinnosti (ak nejde o Núdzové výmeny alebo odstránenia Subdodávateľov bez náhrady).

(b) Ak má Zákazník opodstatnené výhrady voči spracovaniu Osobných údajov Subdodávateľmi, Zákazník môže namietať voči využívaniu služieb Subdodávateľa spoločnosťou SAP tak, že to písomne oznámi spoločnosti SAP do tridsiatich dní od prijatia oznámenia od spoločnosti SAP. Ak Zákazník namieta voči používaniu služieb Subdodávateľa, strany sa stretnú, aby v dobrej viere prediskutovali možné riešenie. Spoločnosť SAP sa môže rozhodnúť, že: (i) nepoužije služby Subdodávateľa alebo (ii) vykoná nápravné opatrenia, ktoré Zákazník požaduje vo svojich námietkach, a použije služby Subdodávateľa. Ak nie je možné využiť ani jednu z týchto možností a Zákazník naďalej namieta z opodstatneného dôvodu, ktorákoľvek zo strán môže do tridsiatich dní vypovedať Zmluvu na základe písomného oznámenia. Ak Zákazník nevznesie žiadne námietky do

(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

(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

tridsiatich dní od prijatia oznámenia, považuje sa to za prijatie nového Subdodávateľa zo strany Zákazníka.
(c) Ak námietka Zákazníka zostane nevyriešená aj po šesťdesiatich dňoch od vznesenia a spoločnosti SAP nebude doručené žiadne oznámenie o vypovedaní, považuje sa to za prijatie Subdodávateľa zo strany Zákazníka.

4.3 Núdzová výmena.
Spoločnosť SAP môže vymeniť Subdodávateľa v prípade, že dôvod na výmenu je odôvodnene mimo kontroly spoločnosti SAP. Ak je to tak, spoločnosť SAP čo najskôr informuje Zákazníka o výmene Subdodávateľa. Zákazník si zachováva právo namietať voči Subdodávateľovi v súlade s Článkom 4.2(b).

5. MEDZINÁRODNÉ PRENOSY

5.1 Obmedzenia Medzinárodného prenosu.
Osobné údaje od Prevádzkovateľov z EHP alebo zo Švajčiarska môžu byť exportované alebo sprístupnené spoločnosti SAP alebo jej Subdodávateľom mimo EHP alebo Švajčiarska (**„Medzinárodný prenos"**):

(a) len za predpokladu, že Príjemca alebo krajina či územie, kde spracúva Osobné údaje alebo pristupuje k Osobným údajom, poskytuje primeranú úroveň ochrany práv a slobôd Dotknutých osôb v súvislosti so spracovaním Osobných údajov, ako to určuje Európska komisia, alebo
(b) v súlade s Článkom 5.2.

5.2 Štandardné zmluvné doložky a viacvrstvová štruktúra.
(a) V prípadoch Medzinárodného prenosu do krajiny, ktorá nezaručuje adekvátnu úroveň ochrany práv a slobôd Dotknutých osôb v súvislosti so spracovaním Osobných údajov, ako to určuje Európska komisia, sa uplatňujú Štandardné zmluvné doložky.

(b) V prípade Subdodávateľov z tretej krajiny spoločnosť SAP musí pred spracovaním Osobných údajov Subdodávateľom zaviazať Subdodávateľa k dodržiavaniu nezmenenej verzie Štandardných zmluvných doložiek. Zákazník týmto (vo svojom mene, ako aj v mene každého Prevádzkovateľa) vyjadruje svoj súhlas so Štandardnými

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

(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.

zmluvnými doložkami medzi spoločnosťou SAP a Subdodávateľom z tretej krajiny. Spoločnosť SAP bude presadzovať Štandardné

zmluvné doložky voči Subdodávateľovi v mene Prevádzkovateľa, ak možnosť priameho presadzovania na základe Zákona o ochrane údajov nie je k dispozícii.

(c) Žiadne články v tejto ZSU sa nesmú interpretovať ako niečo, čo má prednosť pred akýmkoľvek konfliktným ustanovením Štandardných zmluvných doložiek.

6. CERTIFIKÁCIE A AUDITY

6.1 Audity Zákazníka.

Zákazník alebo jeho treťostranný nezávislý audítor môže vykonať audit riadiaceho prostredia a bezpečnostných postupov spoločnosti SAP v rozsahu relevantnom pre Osobné údaje, ktoré spracúva spoločnosť SAP, len v prípade, ak:

(a) spoločnosť SAP dostatočne nepreukázala konanie v súlade s technickými a organizačnými opatreniami na ochranu produkčných systémov Cloudovej služby predložením: (i) osvedčenia o súlade so štandardom ISO 27001 alebo inými štandardmi (v rozsahu definovanom v certifikáte) alebo (ii) platnú správu o atestácii ISAE3402 alebo ISAE3000, pričom správy z auditov SOC alebo certifikácie ISO sú na vyžiadanie Zákazníka k dispozícii od treťostranného audítora alebo od spoločnosti SAP,

(b) došlo k Porušeniu zabezpečenia,

(c) Zákazník alebo iný Prevádzkovateľ má odôvodnené podozrenie, že spoločnosť SAP nekoná v súlade s povinnosťami, ktoré jej vyplývajú z tejto ZSU,

(d) o audit formálne požiada orgán na ochranu údajov Zákazníka alebo iného Prevádzkovateľa, alebo

(e) záväzný Zákon o ochrane údajov poskytuje Zákazníkovi právo na priamy audit.

Počas auditu prostredia spoločnosti SAP zo strany Zákazníka bude spoločnosť SAP poskytovať Zákazníkovi primeranú podporu pri jeho procesoch auditu.

6.2 Obmedzenia auditu.

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.

Periodicita auditu Zákazníka bude obmedzená na jeden audit za obdobie dvanástich mesiacov a obmedzená na maximálne 3 pracovné dni a na primeraný rozsah, ktorý si strany vopred dohodnú. Audit je potrebné oznámiť v primeranom predstihu minimálne šesťdesiatich dní, ak Zákon o ochrane údajov nevyžaduje skorší audit. Spoločnosť SAP a Zákazník využijú aktuálne certifikácie alebo iné správy z auditov na obmedzenie opakovania auditov. Zákazník aj spoločnosť SAP budú sami znášať svoje vlastné náklady na audit, s výnimkou prípadov, keď Zákazník vykonáva audit na základe Článku 6.1 (c) (a ak z auditu nevyplynie, že došlo k porušeniu zo strany spoločnosti SAP, a v takom prípade svoje vlastné náklady na audit bude znášať spoločnosť SAP), 6.1 (d) alebo 6.1 (e). V takýchto prípadoch bude Zákazník znášať svoje vlastné náklady aj náklady na interné prostriedky spoločnosti SAP, ktoré boli potrebné na uskutočnenie auditu. Ak z auditu vyplynie, že spoločnosť SAP porušila svoje povinnosti, ktoré jej vyplývajú zo Zmluvy, spoločnosť SAP okamžite zabezpečí nápravu porušenia na vlastné náklady.

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;

7. EU ACCESS

7.1 Voliteľná služba.

Ak je prístup EU Access zahrnutý v Objednávke, spoločnosť SAP súhlasí s jej poskytovaním pre oprávnenú Cloudovú službu, ako je uvedené v tomto Článku 7.

7.2 EU Access.

Spoločnosť SAP bude používať výhradne Európskych subdodávateľov na poskytovanie podpory pri požadovaní prístupu k Osobným údajom v Clloudovej službe.

7.3 Umiestnenie Dátových centier.

Dátové centrá, ktoré budú hostiteľmi Cloudovej služby, sa budú od Dátumu nadobudnutia účinnosti Objednávky nachádzať v EHP alebo vo Švajčiarsku. Spoločnosť SAP nebude bez predchádzajúce písomného súhlasu Zákazníka (na tento účel sa môže použiť aj e-mail) migrovať inštanciu Zákazníka do Dátového centra mimo EHP alebo Švajčiarska. Ak spoločnosť SAP plánuje migrovať inštanciu Zákazníka do dátového centra v EHP alebo vo Švajčiarsku, spoločnosť SAP to písomne oznámi Zákazníkovi (na tento účel sa môže použiť aj e-mail) nie neskôr ako tridsať dní pred plánovanou migráciou.

7.4 Výluky.

Požiadavky v Článkoch 7.2 a 7.3 sa nevzťahujú na nasledujúce Osobné údaje:

(a) kontaktné detaily odosielateľa hlásenia podpory,

(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. **"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

(b) ľubovoľné iné Osobné údaje, ktoré Zákazník odošle pri vypĺňaní hlásenia podpory (Zákazník sa môže rozhodnúť neodoslať Osobné údaje pri vypĺňaní hlásenia podpory a ak tieto údaje sú potrebné

pri spracovaní v rámci správy incidentov, Zákazník sa môže rozhodnúť pre anonymizáciu týchto Osobných údajov pred prenosom hlásenia o incidente do spoločnosti SAP),

(c) Osobné údaje v iných než produktívnych systémoch.

8. DEFINÍCIE

Význam pojmov s veľkými počiatočnými písmenami, ktoré nie sú definované v tomto dokumente, je definovaný v Zmluve. **„Dátové centrum"** znamená miesto, ktoré je hostiteľom produktívnej inštancie Cloudovej služby pre Zákazníka v jeho regióne, ako je to publikované na stránke http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html alebo oznámené Zákazníkovi, prípadne inak odsúhlasené v Objednávke.

8.2 „Prevádzkovateľ" znamená fyzickú alebo právnickú osobu, orgán verejnej správy, agentúru alebo akýkoľvek iný orgán, ktorý sám alebo spoločne s inými určuje účel a prostriedky spracovania Osobných údajov,

8.3 „Spracovateľ" znamená fyzickú alebo právnickú osobu, orgán verejnej správy, agentúru alebo akýkoľvek iný orgán, ktorý spracováva osobné údaje v mene prevádzkovateľa.

8.4 „Zákon o ochrane údajov" znamená príslušné právne predpisy na ochranu základných práv a slobôd osôb a ich práva na súkromie v súvislosti so spracovaním Osobných údajov podľa Zmluvy.

8.5 „Dotknutá osoba" znamená identifikovanú alebo identifikovateľnú fyzickú osobu.

8.6 „EHP" znamená Európsky hospodársky priestor, čiže členské štáty Európskej únie a Island, Lichtenštajnsko a Nórsko.

8.7 „Európsky subdodávateľ" znamená Subdodávateľa, ktorý fyzicky spracúva Osobné údaje v EHP alebo vo Švajčiarsku.

8.8 „Osobné údaje" znamená ľubovoľné informácie, ktoré sa týkajú Dotknutej osoby. Na účely tejto ZSU zahŕňajú len osobné údaje, ktoré Zákazník alebo jeho Oprávnení

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 subset of Customer Data.

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.

používatelia zadali do Cloudovej služby alebo odvodili od svojho používania Cloudovej služby. Patria sem aj osobné údaje, ktoré boli poskytnuté spoločnosti SAP alebo jej Subdodávateľom alebo ku ktorým spoločnosť SAP alebo jej Subdodávatelia získali prístup, aby mohli poskytovať podporu na základe Zmluvy. Osobné údaje sú podmnožinou Údajov Zákazníka.

8.9 „Porušenie zabezpečenia" znamená potvrdené (1) náhodné alebo nezákonné zničenie, stratu, zmenu alebo zverejnenie Osobných údajov alebo Dôverných údajov Zákazníka, alebo (2) podobný incident v súvislosti s Osobnými údajmi, na ktoré Spracovateľ v súlade s príslušnými zákonmi musí upozorniť Prevádzkovateľa.

8.10 „Štandardné zmluvné doložky", ktoré sa niekedy označujú aj ako „Modelové doložky EÚ", znamenajú (Štandardné zmluvné doložky (spracovatelia)) alebo ich ľubovoľnú následnú verziu, ktorú vydala Komisia (a ktoré sa začnú automaticky uplatňovať). Aktuálne Štandardné zmluvné doložky sú k dispozícii na stránke http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc.

Obsahujú Prílohy 1 a 2 pripojené k tejto ZSU.

8.11 „Subdodávateľ" znamená Ovládané osoby spoločnosti SAP a tretie strany, ktoré si spoločnosť SAP alebo Ovládané osoby spoločnosti SAP najali na spracovanie osobných dát.

8.12 „Subdodávateľ z tretej krajiny" znamená Subdodávateľa nachádzajúceho sa mimo EHP a mimo ľubovoľnej krajiny, pre ktorú Európska komisia publikovala rozhodnutie o adekvátnosti, ako je uvedené na stránke http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

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

Príloha 1 k Zmluve o spracovaní údajov a Štandardným zmluvným doložkám

Exportér údajov
Exportér údajov s predplatenou Cloudovou službou, ktorá umožňuje Oprávneným používateľom zadávať, pozmeňovať, používať, odstraňovať alebo inak spracovávať Osobné údaje.

Importér údajov
Spoločnosť SAP a jej Subdodávatelia poskytujú Cloudovú službu, ktorá zahŕňa nasledujúcu podporu:
Ovládané osoby spoločnosti SAP podporujú dátové centrá Cloudovej služby na diaľku zo zariadení spoločnosti SAP v St. Leon/Rot (Nemecko), Indii a na ďalších miestach, kde spoločnosť SAP zamestnáva personál na pozíciách súvisiacich s prevádzkovaním a dodávkou Cloudových služieb. Podpora zahŕňa:

- monitorovanie Cloudovej služby,
- zálohovanie a obnovu Údajov Zákazníka, ktoré sú uložené v Cloudovej službe,
- vydávanie a vývoj opráv a inovácií pre Cloudovú službu,
- monitorovanie a správu súvisiacej infraštruktúry a databázy Cloudovej služby a riešenie s nimi súvisiacich problémov,
- monitorovanie zabezpečenia, podporu pre zisťovanie neoprávnených vniknutí cez sieť a testovanie nepreniknuteľnosti.

Ovládané osoby spoločnosti SAP poskytujú podporu, keď Zákazník odošle hlásenie podpory z dôvodu nedostupnosti Cloudovej služba pre niektorých alebo všetkých Oprávnených používateľov alebo ak Cloudová služba nefunguje podľa očakávaní. Spoločnosť SAP odpovedá na telefonáty, vykonáva základné riešenie problémov a spracúva hlásenia podpory v sledovacom systéme, ktorý je oddelený od produktívnej inštancie Cloudovej služby.

Dotknuté osoby
Ak Exportér údajov neuvedie inak, prenesené Osobné údaje sa týkajú nasledujúcich kategórií dotknutých osôb: zamestnanci, zmluvní dodávatelia, obchodní partneri alebo iní jednotlivci, ktorých Osobné údaje sú uložené v Cloudovej službe.

Kategórie údajov
Prenesené Osobné údaje sa týkajú nasledujúcich kategórií údajov:
Zákazník určuje kategórie údajov podľa predplatenej Cloudovej služby. Zákazník môže konfigurovať dátové polia počas implementácie Cloudovej služby alebo tak, ako umožňuje Cloudová služba. Prenesené Osobné údaje sa

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.

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

zvyčajne týkajú nasledujúcich kategórií údajov: mená, telefónne čísla, e-mailové adresy, časové pásma, údaje o adresách, údaje o prístupe k systémom, používaní systémov a oprávneniach pre systémy, názvy spoločností, zmluvné údaje, fakturačné údaje a akékoľvek údaje špecifické pre určité aplikácie, ktoré Oprávnení používatelia zadajú do Cloudovej služby, a môžu zahŕňať údaje o bankových účtoch a kreditných alebo debetných kartách.

Prípadné špeciálne kategórie údajov
Prenesené Osobné údaje sa týkajú nasledujúcich špeciálnych kategórií údajov: ako je uvedené v Objednávke (ak je uvedené v Objednávke).

Operácie spracovania
Prenesené Osobné údaje sa spracúvajú v nasledujúcich základných operáciách:

- použitie Osobných údajov na nastavenie, prevádzkovanie, monitorovanie a poskytovanie Cloudovej služby (vrátane Prevádzkovej a technickej podpory),
- poskytovanie Poradenských služieb,
- komunikácia s Oprávnenými používateľmi,
- uchovávanie Osobných údajov vo vyhradených Dátových centrách (architektúra s viacerými klientmi),
- nahrávanie opráv alebo inovácií do Cloudovej služby,
- zálohovanie Osobných údajov,
- počítačové spracovanie Osobných údajov vrátane prenosu údajov, vyhľadávania údajov, prístupu k údajom,
- sieťový prístup na umožnenie prenosu Osobných údajov,
- realizácia pokynov Zákazníka v súlade s touto Zmluvou.

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:

Príloha 2 – Technické a organizačné opatrenia

1. TECHNICKÉ A ORGANIZAČNÉ OPATRENIA

Nasledujúce články definujú aktuálne bezpečnostné opatrenia spoločnosti SAP. Spoločnosť SAP ich môže kedykoľvek a bez upozornenia zmeniť pri zachovaní porovnateľnej alebo vyššej úrovne zabezpečenia. Môže to znamenať, že jednotlivé opatrenia sa nahradia novými opatreniami, ktoré plnia rovnaký účel, bez zníženia úrovne zabezpečenia.

1.1 Kontrola fyzického prístupu.

Neoprávneným osobám je zabránené získať fyzický prístup k priestorom, budovám alebo miestnostiam, kde sa nachádzajú systémy na spracovanie údajov, ktoré spracúvajú alebo používajú Osobné údaje.

Opatrenia:

- Spoločnosť SAP používa na ochranu svojho majetku a zariadení primerané prostriedky na základe klasifikácie zabezpečenia, ktorú vypracovalo oddelenie pre interné zabezpečenie.
- Budovy sú vo všeobecnosti zabezpečené prostredníctvom systémov kontroly prístupu (napr. systém kontroly prístupu cez karty smart card).
- Požaduje sa, aby aspoň vonkajšie vchody budov boli vybavené certifikovaným systémom kľúča, ktorý zahŕňa modernú a aktívnu správu kľúčov.
- V závislosti od bezpečnostnej klasifikácie môžu byť jednotlivé budovy, samostatné plochy a okolité priestory chránené ďalšími opatreniami. Tieto zahŕňajú špecifické prístupové profily, dohľad prostredníctvom videa, systémy na varovanie pred vniknutím a biometrické systémy riadenia prístupu.
- Prístupové práva sa udeľujú oprávneným osobám na individuálnej báze podľa opatrení na kontrolu prístupu k systémom a údajom (pozri Články 1.2 a 1.3 nižšie). Toto sa vzťahuje aj na prístup návštevníkov. Mená hostí a návštevníkov v budovách spoločnosti SAP sa musia registrovať na recepcii a hostia a návštevníci musia byť sprevádzaní autorizovaným personálom spoločnosti SAP.
- Zamestnanci spoločnosti SAP a externý personál musia nosiť identifikačné karty vo všetkých priestoroch spoločnosti SAP.

Ďalšie opatrenia pre Dátové centrá:

- 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 ensure proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

- Všetky Dátové centrá musia dodržiavať prísne procedúry zabezpečenia presadzované prostredníctvom personálu bezpečnostných služieb, bezpečnostných kamier, detektorov pohybu, mechanizmov na kontrolu prístupu a ďalšími opatreniami na predchádzanie ohrozeniu zariadení a Dátových centier. Prístup k systémom a infraštruktúre v zariadeniach Dátových centier majú iba oprávnení zástupcovia. Na zaistenie správnej funkčnosti sa vykonáva pravidelná údržba fyzických bezpečnostných zariadení (napr. snímačov pohybu, kamier atď.).

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

- Spoločnosť SAP a všetci poskytovatelia služieb Dátových centier tretej strany zapisujú mená a časy prístupu osôb vstupujúcich do vyhradených priestorov spoločnosti SAP v rámci Dátových centier.

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

1.2 Kontrola prístupu k systému.

Systémy na spracovanie údajov slúžiace na poskytovanie služieb SAP musia byť chránené pred použitím bez oprávnenia.

Opatrenia:

- Pri udeľovaní prístupu k citlivým systémom vrátane systémov uchovávajúcich a spracúvajúcich Osobné údaje sa uplatňujú viaceré úrovne oprávnení. Uplatňujú sa procesy, ktoré zaručujú, aby oprávnení používatelia mali správne oprávnenia na pridávanie, odstraňovanie alebo modifikovanie používateľov.
- Všetci používatelia pristupujú k systémom spoločnosti SAP s jedinečným identifikátorom (ID používateľa).
- Spoločnosť SAP uplatňuje postupy na zabezpečenie implementácie požadovaných zmien oprávnení iba v súlade s pravidlami (ako je napríklad neudeľovanie práv bez oprávnenia). Ak používateľ opustí spoločnosť, jeho prístupové práva sa zrušia.
- Spoločnosť SAP stanovila pravidlá pre heslá, ktoré zakazujú zdieľanie hesiel, určujú postupy v prípade odhalenia hesla a vyžadujú pravidelnú zmenu hesiel a zmenu predvolených hesiel. Na overenie sa priraďujú prispôsobené ID používateľa. Všetky heslá musia spĺňať definované minimálne požiadavky a sú uložené v šifrovanej forme. V prípade doménových hesiel systém vynucuje zmenu hesla každých šesť mesiacov a v súlade s požiadavkami na zložitosť hesla. Každý

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.

- 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.

počítač má šetrič obrazovky chránený heslom.
- Podniková sieť je chránená pred verejnou sieťou bránami firewall.

- Spoločnosť SAP používa aktuálny antivírusový softvér v prístupových bodoch do podnikovej siete (pre e-mailové kontá), ako aj vo všetkých súborových serveroch a všetkých pracovných staniciach.

- Implementovaná je aj správa opráv zabezpečenia, ktorá zaisťuje riadne a pravidelné nasadzovanie relevantných aktualizácií zabezpečenia.
- Úplný vzdialený prístup k podnikovej sieti a kritickej infraštruktúre spoločnosti SAP je chránený účinným overovaním.

1.3 Kontrola prístupu k údajom.

Osoby oprávnené na používanie systémov na spracovanie údajov musia mať prístup iba k Osobným údajom, ku ktorým majú právo na prístup, a Osobné údaje sa počas spracovania, používania a uchovávania nesmú bez oprávnenia čítať, kopírovať, upravovať ani odstraňovať.

Opatrenia:

- V rámci pravidiel zabezpečenia spoločnosti SAP sa pre Osobné údaje vyžaduje minimálne rovnaká úroveň ochrany ako v prípade „dôverných" informácií podľa štandardu klasifikácie informácií spoločnosti SAP.
- Prístup k osobným, dôverným alebo citlivým informáciám sa udeľuje na báze potreby prístupu k informáciám. Inak povedané, zamestnanci alebo externé tretie strany majú prístup k informáciám, ktoré potrebujú na vykonávanie svojej práce. Spoločnosť SAP používa koncepty oprávnení, ktoré dokumentujú, ako sa oprávnenia priraďujú a komu sa priraďujú aké oprávnenia. Všetky osobné, dôverné alebo inak citlivé dáta sú chránené v súlade so štandardmi a pravidlami zabezpečenia spoločnosti SAP. Dôverné informácie sa musia spracovávať ako dôverné.
- Všetky produkčné servery sú prevádzkované v Dátových centrách alebo zabezpečených serverových miestnostiach. Bezpečnostné opatrenia, ktoré ochraňujú aplikácie spracúvajúce osobné, dôverné alebo iné citlivé informácie, sa pravidelne kontrolujú. Na tento účel spoločnosť SAP uskutočňuje

- 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 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

interné a externé kontroly zabezpečenia a testy nepreniknuteľnosti k svojim IT systémom.

- Spoločnosť SAP nepovoľuje inštaláciu osobného softvéru ani iného softvéru, ktorý nebol schválený spoločnosťou SAP.
- Bezpečnostný štandard spoločnosti SAP určuje, ako sa odstraňujú alebo ničia údaje a dátové nosiče, ktoré už nie sú potrebné.

1.4 Kontrola prenosu údajov.

S výnimkou nevyhnutnou na poskytovanie Služieb v súlade s príslušnou zmluvou o poskytovaní služieb sa Osobné údaje nesmú počas prenosu čítať, kopírovať, modifikovať ani odstraňovať bez povolenia. Pri fyzickej preprave nosičov dát sa v spoločnosti SAP uplatňujú primerané opatrenia na zabezpečenie odsúhlasenej úrovne služby (napríklad šifrovanie alebo kontajnery poskytujúce ochranu proti elektromagnetickému žiareniu).

- Osobné údaje prenášané cez interné siete spoločnosti SAP sú v súlade s pravidlami zabezpečenia spoločnosti SAP chránené rovnako ako akékoľvek iné dôverné údaje.
- Pri prenose údajov medzi spoločnosťou SAP a jej zákazníkmi sú ochranné opatrenia pre prenášané Osobné údaje vzájomne odsúhlasené a začlenené do príslušnej Zmluvy. Toto sa vzťahuje na fyzický aj na sieťový prenos údajov. Po prenesení údajov mimo systémy ovládané spoločnosťou SAP (napr. po prenesení údajov von z brány firewall Dátového centra spoločnosti SAP) preberá za všetky prenosy údajov zodpovednosť Zákazník.

1.5 Kontrola údajových vstupov.

Musí byť možné spätne preskúmať a zistiť, či v systémoch spracovania údajov spoločnosti SAP došlo k zadaniu, modifikovaniu alebo odstráneniu údajov a kto vykonal daný krok.

Opatrenia:

- Spoločnosť SAP poskytuje oprávneným osobám prístup k Osobným údajom tak, ako je to potrebné pre ich prácu.
- Spoločnosť SAP implementuje systém na zaznamenávanie zadávania, modifikovania a odstraňovania alebo na blokovanie Osobných údajov spoločnosťou SAP alebo jej Subdodávateľmi v rámci Produktov a Služieb spoločnosti SAP v maximálnom možnom rozsahu.

1.6 Kontrola vykonávania úloh.

Osobné údaje spracovávané na základe poverenia (t. j. Osobné údaje spracovávané v mene zákazníka) sa spracúvajú výlučne v

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.
- 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.

súlade s príslušnou zmluvou a súvisiacimi pokynmi zákazníka.

Opatrenia:

- Spoločnosť SAP používa kontroly a procesy na zabezpečenie súladu so zmluvami medzi spoločnosťou SAP a jej zákazníkmi, subdodávateľmi alebo inými poskytovateľmi služieb.
- V rámci pravidiel zabezpečenia spoločnosti SAP sa pre Osobné údaje vyžaduje minimálne rovnaká úroveň ochrany ako v prípade „dôverných" informácií podľa štandardu klasifikácie informácií spoločnosti SAP.
- Všetci zamestnanci spoločnosti SAP a jej zmluvní subdodávatelia alebo iní poskytovatelia služieb sú zmluvne zaviazaní rešpektovať dôvernosť všetkých citlivých informácií vrátane obchodných tajomstiev zákazníkov a partnerov spoločnosti SAP.
- Na účely služieb podpory v mieste prevádzky spoločnosť SAP poskytuje špeciálne navrhnuté a zabezpečené zariadenie pre hlásenia podpory, v ktorom spoločnosť SAP poskytuje špeciálny priestor na prenos údajov o prístupoch a hesiel, ktorý je chránený proti prístupu a má monitorované zabezpečenie. Zákazníci spoločnosti SAP majú po celý čas kontrolu nad svojimi pripojeniami na poskytovanie podpory na diaľku. Zamestnanci spoločnosti SAP nemôžu získať prístup do systému zákazníka bez vedomia alebo úplnej aktívnej spoluúčasti zákazníka.

1.7 Kontrola dostupnosti.

Osobné údaje musia byť chránené pred náhodným alebo neúmyselným zničením alebo stratou.

Opatrenia:

- Spoločnosť SAP využíva procesy zálohovania a ďalšie opatrenia, ktoré zaisťujú rýchle obnovenie kľúčových podnikových systémov tak, ako a kedy je to potrebné.
- Spoločnosť SAP používa zdroje neprerušovaného napájania (napríklad UPS, batérie, generátory atď.) na zaistenie dostupnosti napájania pre Dátové centrá.
- Spoločnosť SAP má vypracované kontingenčné plány, ako aj a stratégie na obnovenie prevádzky a obnovenie po katastrofe pre poskytované služby.
- Procesy a systémy pre prípad núdze sa pravidelne testujú.

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 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.

1.8 Kontrola oddelenia údajov.
Osobné údaje zhromažďované na odlišné účely môžu byť spracované oddelene. Opatrenia:

- Spoločnosť SAP využíva technické možnosti nasadeného softvéru (napríklad oddelené systémové infraštruktúry alebo systémové infraštruktúry s viacerými klientmi) na zaistenie oddelenia Osobných údajov jedného zákazníka od Osobných údajov ostatných zákazníkov.
- Zákazníci (vrátane svojich Ovládaných osôb) majú prístup iba k svojim vlastným údajom.
- Ak sú Osobné údaje potrebné na spracovanie incidentu podpory konkrétneho zákazníka, priradia sa k danému konkrétnemu hláseniu a použijú sa len na spracovanie tohto hlásenia a nepristupuje sa k nim účely spracovania iných hlásení. Tieto údaje sú uložené vo vyhradených podporných systémoch.

1.9 Kontrola integrity údajov.
Osobné údaje zostanú počas spracovania nedotknuté, úplné a aktuálne.
Opatrenia:
Spoločnosť SAP má implementovanú viacvrstvovú obrannú stratégiu na ochranu pred neoprávnenými modifikáciami.
Na uplatňovanie riadenia a opatrení popísaných v článkoch vyššie spoločnosť SAP používa nasledujúce prostriedky.

Ide najmä o tieto súčasti:

- brány firewall,
- centrum monitorovania zabezpečenia,
- antivírusový softvér,
- zálohovanie a obnovenie,
- testovanie externého a interného vniknutia,
- pravidelné externé audity na overenie bezpečnostných opatrení.