

PŘÍLOHA

STANDARDNÍ SMLUVNÍ DOLOŽKY

ODDÍL I

Doložka 1

Účel a oblast působnosti

- a) Účelem těchto standardních smluvních doložek (dále jen „doložky“) je zajistit soulad s [vyberte příslušnou možnost: MOŽNOST 1: ustanoveními čl. 28 odst. 3 a 4 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů] / [MOŽNOST 2: ustanoveními čl. 29 odst. 3 a 4 nařízení Evropského parlamentu a Rady (ES) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů].
- b) Správci a zpracovatelé uvedení v příloze I schválili tyto doložky, aby zajistili soulad s čl. 28 odst. 3 a 4 nařízení (EU) 2016/679 a/nebo čl. 29 odst. 3 a 4 nařízení (EU) 2018/1725.
- c) Tyto doložky se uplatňují na zpracování osobních údajů, jak je upřesněno v příloze II.
- d) Přílohy I až IV jsou nedílnou součástí těchto doložek.
- e) Těmito doložkami nejsou dotčeny povinnosti, které správce musí plnit na základě nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.
- f) Tyto doložky samy o sobě nezajišťují soulad s povinnostmi týkajícími se mezinárodního předávání podle kapitoly V nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

Doložka 2

Neměnnost doložek

- a) Smluvní strany se zavazují, že doložky nebudou měnit, s výjimkou doplňování nebo aktualizace informací v přílohách.
- b) To stranám nebrání v možnosti zahrnout tyto standardní smluvní doložky stanovené v tomto rozhodnutí do širší smlouvy nebo k nim doplnit další doložky nebo další záruky, pokud tyto nejsou se standardními smluvními doložkami v přímém nebo nepřímém rozporu nebo pokud neomezují základní práva nebo svobody subjektů údajů.

Doložka 3

Výklad

- a) V případech, kdy tyto doložky používají pojmy definované v nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725, mají tyto pojmy stejný význam jako v uvedeném nařízení.
- b) Tyto doložky jsou chápány a vykládány v souladu s ustanoveními nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.
- c) Tyto doložky nesmí být vykládány způsobem, který by byl v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679 / nařízení (EU) 2018/1725, nebo který by omezoval základní práva nebo svobody subjektů údajů.

Doložka 4

Hierarchie

V případě rozporu mezi těmito doložkami a ustanoveními souvisejících dohod existujících mezi stranami v době, kdy jsou tyto doložky sjednány, nebo dohod uzavřených později mají přednost tyto doložky.

Doložka 5 – Nepovinná

Doložka o přistoupení

- a) Každý subjekt, který není smluvní stranou těchto doložek, může se souhlasem všech stran k těmto doložkám kdykoli přistoupit buď jako správce, nebo jako zpracovatel, a to tím, že vyplní přílohy a podepíše přílohu I.
- b) Po vyplnění a podpisu příloh uvedených v odst. a) je přistupující subjekt považován za smluvní stranu těchto doložek a má práva a povinnosti správce nebo zpracovatele v souladu s jeho určením v příloze I.
- c) Přistupujícímu subjektu z těchto doložek nevyplývají žádná práva ani povinnosti pro období před tím, než se stal smluvní stranou.

ODDÍL II – POVINNOSTI STRAN

Doložka 6

Popis zpracování

Podrobnosti týkající se operací zpracování, zejména kategorie osobních údajů a účely zpracování, pro něž jsou osobní údaje zpracovávány jménem správce, jsou uvedeny v příloze II.

Doložka 7

Povinnosti stran

7.1 Pokyny

- a) Zpracovatel zpracovává osobní údaje pouze na základě písemně doložených pokynů správce, pokud mu takové zpracování neukládá právo Unie nebo členského státu, které se na správce vztahuje. V tomto případě zpracovatel správce informuje o uvedeném právním požadavku před zpracováním, pokud to právní předpisy nezakazují z důvodů důležitého veřejného zájmu. Po celou dobu zpracování osobních údajů může správce rovněž vydávat další pokyny. Tyto pokyny musí být vždy písemně doloženy.
- b) Zpracovatel neprodleně informuje správce v případě, že dle jeho názoru pokyny správce porušují nařízení (EU) 2016/679 / nařízení (EU) 2018/1725 nebo příslušná ustanovení Unie nebo členského státu o ochraně údajů.

7.2 Omezení účelu

Zpracovatel zpracovává osobní údaje pouze pro konkrétní účel nebo účely zpracování, jak je stanoveno v příloze II, pokud od správce neobdrží další pokyny.

7.3 Doba trvání zpracování osobních údajů

Zpracování zpracovatelem probíhá pouze po dobu stanovenou v příloze II.

7.4 Zabezpečení zpracování

- a) Za účelem zajištění bezpečnosti osobních údajů musí zpracovatel zavést přinejmenším technická a organizační opatření uvedená v příloze III. Součástí těchto opatření musí být ochrana údajů před narušením bezpečnosti, které by vedlo k jejich náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému zpřístupnění nebo přístupu k nim (porušení zabezpečení osobních údajů). Při posuzování vhodné úrovně zabezpečení vezmou strany v úvahu aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování a rizika pro subjekty údajů.
- b) Zpracovatel poskytne svým zaměstnancům přístup ke zpracovávaným osobním údajům pouze v rozsahu nezbytně nutném pro provádění, správu a kontrolu smlouvy. Zpracovatel zajistí, aby se osoby oprávněné zpracovávat obdržené osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

7.5 Citlivé údaje

Pokud zpracování zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu nebo o sexuálním životě či sexuální orientaci dané osoby nebo údaje týkající se odsouzení v trestních věcech a trestných činů (dále jen „citlivé údaje“), uplatní zpracovatel zvláštní omezení nebo další záruky.

7.6. Dokumentace a soulad

- a) Strany musí být schopny prokázat dodržování těchto doložek.
- b) Zpracovatel neprodleně a odpovídajícím způsobem vyřídí dotazy správce, které se týkají zpracovávání podle těchto doložek.
- c) Zpracovatel poskytne správci veškeré informace potřebné k prokázání souladu s povinnostmi stanovenými v těchto doložkách, které vyplývají přímo z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725. Zpracovatel též na žádost správce umožní audity činností zpracování, na něž se tyto doložky vztahují, a k těmto auditům přispěje, a to v přiměřených intervalech nebo pokud existují známky nesouladu. Při rozhodování o přezkumu nebo auditu může správce zohlednit příslušná osvědčení držena zpracovatelem.
- d) Správce se může rozhodnout, zda audit provede sám, nebo jím pověří nezávislého auditora. Audity mohou rovněž zahrnovat kontroly v objektech a prostorách zařízení zpracovatele a případně jsou předem včas ohlášeny.
- e) Strany na požádání zpřístupní informace uvedené v této doložce, včetně výsledků případných auditů, příslušnému dozorovému úřadu, respektive příslušným dozorovým úřadům.

7.7 Využívání dílčích zpracovatelů údajů

- a) **MOŽNOST 1: KONKRÉTNÍ PŘEDCHOZÍ POVOLENÍ:** Bez předchozího konkrétního písemného povolení správce nesmí zpracovatel zadat dílčímu zpracovateli žádnou ze svých činností spojených se zpracováním údajů, které jsou vykonávány jménem správce v souladu s těmito doložkami. Zpracovatel předloží žádost o konkrétní povolení nejméně [UPŘESNĚTE ČASOVÝ ÚSEK] před zapojením dotčeného dílčího zpracovatele, a to společně s informacemi, jež jsou nezbytné k tomu, aby správce mohl o povolení rozhodnout. Seznam dílčích zpracovatelů, kteří správce schválil, je uveden v příloze IV. Smluvní strany přílohu IV průběžně aktualizují.

MOŽNOST 2: OBECNÉ PÍSEMNÉ POVOLENÍ: Zpracovatel má obecné povolení správce k zapojení dílčích zpracovatelů ze schváleného seznamu. Zpracovatel výslovně písemně informuje správce o všech zamýšlených změnách uvedeného seznamu přijetím nebo nahrazením dílčích zpracovatelů nejméně [UPŘESNĚTE ČASOVÝ ÚSEK] předem, čímž poskytne správci dostatek času na to, aby mohl vznést námitku proti takovým změnám před zapojením dotčeného dílčího zpracovatele / dotčených dílčích zpracovatelů. Zpracovatel poskytne správci informace nezbytné k tomu, aby správce mohl uplatnit své právo vznést námitku.

- b) Pokud zpracovatel zapojí dílčího zpracovatele do provádění konkrétních činností zpracování (jménem správce), učiní tak prostřednictvím smlouvy, která ukládá dílčímu zpracovateli v podstatě stejné povinnosti v oblasti ochrany údajů, jaké jsou v souladu s těmito doložkami uloženy zpracovateli údajů. Zpracovatel zajistí, aby dílčí

zpracovatel plnil povinnosti, které se na zpracovatele vztahují podle těchto doložek a nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

- c) Zpracovatel poskytne správci na jeho žádost opis dohody s dílčím zpracovatelem a veškeré následné změny dohody. V rozsahu nutném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, může zpracovatel před poskytnutím opisu text dohody upravit.
- d) Zpracovatel nese vůči správci plnou odpovědnost za to, aby dílčí zpracovatel plnil povinnosti vyplývající z jeho smlouvy se zpracovatelem. Zpracovatel správce uvědomí, pokud dílčí zpracovatel neplní své povinnosti vyplývající z uvedené smlouvy.
- e) Zpracovatel s dílčím zpracovatelem schválí doložku ve prospěch třetí strany, podle níž v případě, že zpracovatel fakticky zmizí, z právního hlediska zanikne, nebo se ocitne v platební neschopnosti, má správce právo ukončit smlouvu s dílčím zpracovatelem a pověřit dílčího zpracovatele, aby osobní údaje vymazal nebo vrátil.

7.8 Mezinárodní předávání údajů

- a) Jakékoli předání údajů zpracovatelem do třetí země nebo mezinárodní organizaci se provádí pouze na základě písemně doložených pokynů správce nebo za účelem splnění konkrétního požadavku podle právních předpisů Unie nebo členského státu, které se na zpracovatele vztahují, a to v souladu s kapitolou V nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.
- b) Správce souhlasí s tím, že pokud zpracovatel v souladu s doložkou 7.7 zapojí dílčího zpracovatele do provádění konkrétních činností zpracování (jménem správce) a uvedené činnosti zahrnují předání osobních údajů ve smyslu kapitoly V nařízení (EU) 2016/679, mohou zpracovatel a dílčí zpracovatel zajistit soulad s ustanoveními kapitoly V nařízení (EU) 2016/679 použitím standardních smluvních doložek přijatých Komisí v souladu s čl. 46 odst. 2 nařízení (EU) 2016/679, pokud jsou splněny standardní podmínky pro použití těchto smluvních doložek.

Doložka 8

Pomoc poskytovaná správci

- a) Zpracovatel neprodleně informuje správce o každé žádosti, kterou obdržel od subjektu údajů. Na tuto žádost neodpovídá sám, pokud k tomu není správcem zmocněn.
- b) Zpracovatel pomáhá správci při plnění jeho povinností reagovat na žádosti subjektů údajů o výkon jejich práv s přihlédnutím k povaze zpracování. Při plnění svých povinností podle ustanovení písmen a) a b) postupuje zpracovatel v souladu s pokyny správce.
- c) Kromě toho, že má zpracovatel povinnost pomáhat správci podle doložky 8 písm. b), zpracovatel správci dále pomáhá při zajišťování plnění následujících povinností, a to s přihlédnutím k povaze zpracování údajů a informacím, které má zpracovatel k dispozici:
 - 1) povinnost provést posouzení dopadu zamýšlených operací zpracování na ochranu osobních údajů (dále jen „posouzení vlivu na ochranu údajů“), pokud

- je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob;
- 2) povinnost konzultovat před zpracováním příslušný dozorový úřad, respektive příslušné dozorové úřady, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika;
 - 3) povinnost zajistit, aby byly osobní údaje přesné a aktuální, a to tím, že zpracovatel správce neprodleně informuje, pokud se dozví, že osobní údaje, které zpracovává, jsou nepřesné nebo zastaralé;
 - 4) povinnosti podle [MOŽNOST 1] článku 32 nařízení (EU) 2016/679 / [MOŽNOST 2] článku 33 a článků 36 až 38 nařízení (EU) 2018/1725.
- d) V příloze III strany stanoví vhodná technická a organizační opatření, jimiž je zpracovatel povinen správci pomáhat při uplatňování této doložky, jakož i oblast působnosti a rozsah požadované pomoci.

Doložka 9

Ohlašování případů porušení zabezpečení osobních údajů

V případě porušení zabezpečení osobních údajů zpracovatel spolupracuje se správcem a pomáhá mu při plnění jeho povinností podle článků 33 a 34 nařízení (EU) 2016/679 nebo případně podle článků 34 a 35 nařízení (EU) 2018/1725, přičemž zohlední povahu zpracování a informace, které má zpracovatel k dispozici.

9.1 Porušení zabezpečení údajů zpracovávaných správcem

V případě porušení zabezpečení osobních údajů zpracovávaných správcem zpracovatel napomáhá správci:

- a) při ohlašování případů porušení zabezpečení osobních údajů příslušnému dozorovému úřadu, respektive příslušným dozorovým úřadům, a to bez zbytečného odkladu poté, co se o něm správce dozvěděl, je-li to relevantní / (pokud je nepravděpodobné, že by porušení zabezpečení osobních údajů vedlo k ohrožení práv a svobod fyzických osob);
- b) při získávání následujících informací, které musí být podle [MOŽNOST 1] čl. 33 odst. 3 nařízení (EU) 2016/679 / [MOŽNOST 2] čl. 34 odst. 3 nařízení (EU) 2018/1725 uvedeny v oznámení správce, a to musí přinejmenším zahrnovat:
 - 1) povahu daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
 - 2) pravděpodobné důsledky porušení zabezpečení osobních údajů;
 - 3) opatření přijatá nebo navržená k přijetí v souvislosti s porušením zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout všechny tyto informace najednou, musí původní oznámení obsahovat informace, které jsou v dané době k dispozici, a další informace jsou poté poskytnuty bez zbytečného odkladu, jakmile jsou dostupné.

- c) při plnění povinnosti v souladu s [MOŽNOST 1] článkem 34 nařízení (EU) 2016/679 / [MOŽNOST 2] článkem 35 nařízení (EU) 2018/1725 oznámit bez zbytečného odkladu subjektu údajů porušení zabezpečení osobních údajů, pokud je pravděpodobné, že dané porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

9.2 Porušení zabezpečení údajů zpracovávaných zpracovatelem

V případě porušení zabezpečení osobních údajů zpracovávaných zpracovatelem o tom zpracovatel informuje správce bez zbytečného odkladu poté, co se o tomto porušení dozvěděl. Takové oznámení obsahuje alespoň:

- a) popis povahy daného případu porušení (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a záznamů údajů);
- b) údaje o kontaktním místě, kde lze získat více informací o daném porušení zabezpečení osobních údajů;
- c) pravděpodobné důsledky a opatření přijatá nebo navržená k přijetí v souvislosti s porušením zabezpečení, a to včetně opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout všechny tyto informace najednou, musí původní oznámení obsahovat informace, které jsou v dané době k dispozici, a další informace jsou poté poskytnuty bez zbytečného odkladu, jakmile jsou dostupné.

Strany stanoví v příloze III všechny další informace, které má zpracovatel poskytnout, když správci poskytuje pomoc při plnění povinností správce podle [MOŽNOST 1] článků 33 a 34 nařízení (EU) 2016/679 / [MOŽNOST 2] článků 34 a 35 nařízení (EU) 2018/1725.

ODDÍL III – ZÁVĚREČNÁ USTANOVENÍ

Doložka 10

Porušení doložek a ukončení smlouvy

- a) Aniž jsou dotčena jakákoli ustanovení nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725, pokud zpracovatel poruší své povinnosti podle těchto doložek, může mu správce nařídit, aby pozastavil zpracovávání osobních údajů, dokud zpracovatel nebude plnit povinnosti podle těchto doložek, nebo dokud nebude smlouva vypovězena. Zpracovatel neprodleně informuje správce v případě, že z jakéhokoli důvodu není schopen plnit ustanovení těchto doložek.
- b) Správce je oprávněn vypovědět smlouvu v rozsahu, v němž se týká zpracování osobních údajů v souladu s těmito doložkami, pokud:
 - 1) správce pozastavil podle písmene a) zpracovávání osobních údajů zpracovatelem a plnění povinností podle těchto doložek není obnoveno v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení;
 - 2) zpracovatel závažně nebo trvale porušuje tyto doložky nebo povinnosti, které pro něj vyplývají z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725;
 - 3) zpracovatel neplní závazné rozhodnutí příslušného soudu nebo příslušného dozorového úřadu, respektive příslušných dozorových úřadů týkající se jeho povinností vyplývajících z těchto doložek nebo z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.
- c) Zpracovatel je oprávněn vypovědět smlouvu v rozsahu, v němž se týká zpracování osobních údajů podle těchto doložek, pokud poté, co informoval správce o tom, že pokyny správce porušují platné právní požadavky podle doložky 7.1 písm. b), správce na splnění těchto pokynů trvá.
- d) Po ukončení smlouvy zpracovatel podle volby správce vymaže veškeré osobní údaje zpracovávané jménem správce a potvrdí správci, že tak učinil, nebo vrátí veškeré osobní údaje správci a vymaže stávající kopie, pokud právo Unie nebo členského státu nepožaduje uchovávání osobních údajů. Dokud nejsou osobní údaje vymazány nebo vráceny, zpracovatel nadále zajišťuje dodržování souladu s těmito doložkami.

PŘÍLOHA I: SEZNAM STRAN

1. Správce/správci:

Název a adresu společnosti SEMA GmbH Computer Software und Hardware-Vertrieb naleznete v cenové nabídce.

Samostatný podpis těchto standardních smluvních doložek odpovědnou osobou se nevyžaduje. Tyto standardní smluvní doložky jsou nedílnou součástí smlouvy o pronájmu softwaru. Podpisem nabídky společnosti SEMA GmbH Computer Software und Hardware-Vertrieb na uzavření smlouvy o předplatném odpovědnou osobou jsou závazně uzavřeny i tyto standardní smluvní doložky.

2. Zpracovatel/zpracovatelé:

Název: SEMA GmbH Computer Software und Hardware-Vertrieb
Adresa: Salzstraße 25, 87499 Wildpoldsried

Jméno, funkce a kontaktní údaje kontaktní osoby:

Claudia Kirchgessner
Head of Backoffice
Podpis: _____

Silvia Emilius
Backoffice
Podpis: _____

Poverenec pro ochranu osobních údajů: Joachim Hanke

PŘÍLOHA II: POPIS ZPRACOVÁNÍ

Zaměstnanci zákazníka, orgány zákazníka, další osoby, jejichž údaje zákazník ukládá do svých systémů, ke kterým má SEMA přístup.

Údaje, které poskytují informace o přístupu k softwaru SEMA a jeho dalším používání výše uvedenými skupinami osob ze strany zákazníka, např. přihlašovací údaje apod.

Nedochází ke zpracování citlivých údajů

Údaje nejsou společností SEMA cíleně zpracovávány. Zpracování probíhá spíše jen v rozsahu, v jakém je přístup k údajům nevyhnutelný, aby bylo možné plnit smlouvu o předplacených službách, zejména služby péče, které jsou podle ní poskytovány.

Realizace smlouvy o předplacených službách.

Po dobu trvání smlouvy o předplacených službách.

Zpracování prostřednictvím dílčích zpracovatelů probíhá pouze ve výše uvedeném rozsahu a po výše uvedenou dobu a pouze v rozsahu, v jakém smlouva o předplacených službách umožňuje zapojení dílčích zpracovatelů.

PŘÍLOHA III – Technická a organizační opatření

1. Pseudonymizace	
Dochází k přímému zpracování osobních údajů za účelem zpracování objednávky. Existuje možná viditelnost nebo přístup k osobním údajům. Pseudonymizace nebo anonymizace se neprovádí.	
2. Šifrování	
Všechny mobilní datové nosiče jsou šifrovány podle nejnovějších poznatků. Nakládání s daty a jejich ukládání upravují interní směrnice IT.	
3. Zajištění zachování důvěrnosti informací	
Kontrola vstupu:	<p>Jedná se o administrativní budovu, kterou využívají pouze společnosti SEMA GmbH a WGsystem GmbH. Vstupní dveře jsou zajištěny bezpečnostním zámekem s elektromotorem. Tyto zámky lze otevřít pouze pomocí čipové karty. Vstupní dveře jsou zvenčí opatřeny pouze pevnou koulí namísto kliky a mimo pracovní dobu se zamykají motorickým zámekem. Záznamy o zaměstnancích jsou mimo pracovní dobu uzamčeny v kartotékách. Serverovna je také zabezpečena bezpečnostním zámekem s elektromotorem, který lze otevřít pouze pomocí čipové karty.</p> <p>Tato místnost je nepřetržitě zamčená.</p> <p>Čipové karty jsou vydávány pouze oprávněným osobám a po vypršení platnosti oprávnění jsou okamžitě odebrány. Oprávnění ke vstupu je zaznamenáno a zdokumentováno příslušnými opatřeními. Pokud dojde ke ztrátě přístupového zařízení nebo pokud bývalá oprávněná osoba dobrovolně nevrátí přístupové zařízení, dojde k individuální blokaci přístupového zařízení.</p> <p>Okna v budově a kancelářských a obchodních prostorách jsou s izolačním trojsklem. Mimo pracovní dobu jsou okna na všech místech zavřena.</p> <p>Cizí osoby se mohou zdržovat v celé budově firmy pouze za přítomnosti zaměstnanců. Pomocný personál je vždy vybírán pečlivě.</p> <p>U sboru dobrovolných hasičů ve Wildpoldsriedu je ve speciálně vyčleněném trezoru čipová karta s přístupovým oprávněním ke všem třem venkovním dveřím.</p>

3. Zajištění zachování důvěrnosti informací	
Kontrola vstupu a přístupu	<p>Pro přístup do systémů zpracování dat je zaveden systém hesel. Jsou nastaveny zásady hesla. Každá oprávněná osoba obdrží individuální uživatelské ID a osobní heslo, které musí být uchováváno v tajnosti a nesmí být předáváno třetím stranám. Je zavedeno opatření pro případ nepřítomnosti. Oprávnění jsou pravidelně kontrolována. Po uplynutí oprávnění je heslo zablokováno. Heslo se skládá nejméně ze 14 znaků (náhodně vybraná velká písmena, malá písmena, speciální znaky a číslice). Po třech neúspěšných pokusech je ID uživatele zablokováno.</p> <p>Podle současného stavu techniky jsou interní sítě uzavřeny proti přístupu zvenčí úplným fyzickým oddělením interních a externích sítí. Je nastavena brána firewall s alespoň denními aktualizacemi softwaru. Cesty připojení zvenčí jsou zabezpečeny pomocí protokolu https a certifikátů.</p> <p>Přístupy uživatelů se zaznamenávají při přihlašování a odhlašování. Jsou zavedeny organizační požadavky, jako jsou organizační schémata, popisy pracovních míst a úkolů. Ty jsou pravidelně aktualizovány a převáděny do definic rolí. Přidělení rolí se pravidelně vyhodnocuje. Používá se koncept oprávnění. V rámci konceptu přístupových oprávnění jsou nastavena odstupňovaná přístupová oprávnění, která povolují vstup, čtení, kopírování, změnu nebo odstranění údajů klienta během zpracování, používání a po uložení pouze v rozsahu potřebném pro příslušný úkol a jinak tomu zabraňují. Koncept autorizace přístupu zahrnuje správu přístupových práv správci systému. Testovací provoz je oddělen od výrobního provozu. Používání internetu a elektronické pošty se kontroluje a organizuje a rovněž je upraveno soukromé používání internetu a elektronické pošty ve firmě. Prostory, kde jsou uloženy nosiče dat, jsou speciálně zabezpečeny. Nosiče dat a chybné výtisky, které již nejsou potřeba, se likvidují v souladu s předpisy o ochraně osobních údajů.</p>
Kontrola oddělení dat	<p>Údaje jsou uloženy pro více než jednoho správce a jsou uloženy v multi client databázi. Účely, pro které mají být příslušné údaje zpracovány a použity, se dokumentují. Přístupová práva jsou jasně definována.</p> <p>Je zaveden koncept shromažďování a zpracování dat. Výrobní sítě jsou od testovací sítě fyzicky odděleny vhodnými opatřeními. Úroveň bezpečnosti testovacích systémů je stejně vysoká jako u výrobních systémů. Je zaručeno, že výrobní data se používají jako testovací data pouze po konzultaci se zákazníkem.</p>
4. Zajištění dostupnosti a připravenosti	
Kontrola dostupnosti	<p>Dodavatel zaručí dostatečnou softwarovou ochranu proti narušení integrity systému pomocí skenerů uložených v paměti proti virům, trojským koním, červům a jinému škodlivému softwaru. Spouštění cizího softwaru, který není určen pro dané pracoviště, je zabráněno smluvními zakazy uživatelů, filtry nevyžádané pošty, monitorováním licencí a minimálně denní aktualizací operačního systému, stávajícího provozního a bezpečnostního softwaru. Dostatečná ochrana hardwaru je zajištěna nepřerušitelným napájením a dodržováním příslušných protipožárních předpisů. Je zavedena koncepce zabezpečení dat. Tato koncepce umožňuje vytvářet záložní kopie podle principu generování ve vhodných intervalech. Datový fond se zálohuje postupně alespoň jednou denně a jednou týdně kompletně zašifrované na externí paměťové médium. Týdenní úplná záloha je uložena v datovém centru společnosti IDKom Networks. K dispozici je příručka/koncepce pro případ nouze.</p>
Kontrola zakázky	<p>Při předávání datových nosičů, které lze číst, je zajištěno, že na nich nejsou žádná zbytková data, například z jiných operací zpracování.</p>

5. Zajištění integrity	
Kontrola přenosu dat	<p>Přenos dat probíhá prostřednictvím optického připojení společnosti Telekom přes synchronní VDSL, účelem přenosu je zpracování objednávek. Účastníci jsou identifikováni a autentizováni. Autentizace probíhá prostřednictvím uživatelského jména a hesla. Mobilní datové nosiče s daty klientů, mobilní koncová zařízení s daty klientů a porty USB mohou používat pouze zaměstnanci, kteří jsou výslovně oprávněni předávat a zabezpečovat data výhradně pro smluvní a bezpečnostní účely. Heslo se skládá nejméně ze 14 znaků (náhodně vybraná velká písmena, malá písmena, speciální znaky a číslice). Generické pojmy nebo vlastní jména se nesmí používat. Probíhá dokumentace příjemců dat. Likvidaci datových nosičů zajišťuje pan Joachim Hanke a společnost Dorr. Až do zničení jsou nosiče dat uloženy v uzamčeném skladu technologického oddělení. S externím poskytovatelem služeb je uzavřena smlouva o zpracování objednávek.</p>
Kontrola zadávání záznamů	<p>Neoprávněným zápisům, změnám a mazání brání systém hesel. Provádění zápisů, změna nebo vymazání osobních údajů se protokuluje v souladu se základními požadavky pro systém řízení dokumentů. Oprávnění k zapisování se vedou v souladu se základními požadavky pro systém řízení dokumentů a udělují se písemně. Oprávnění k provedení zápisů jsou upravena na vytvořená data protokolu. Jako centrální opatření se při kontrole vstupů pravidelně vyhodnocují systémové protokoly. Systémové protokoly jsou vyhodnocovány anonymně a dotyční uživatelé jsou identifikováni pouze v případě, že k tomu existuje konkrétní důvod. Pro data protokolu platí zásady mazání. Všichni zaměstnanci jsou vázáni mlčenlivostí. Následující aplikace mají druhou kontrolu přístupu: Adito, Outlook, SAGE, BBS Reisekosten, HR Works, veškerý bankovní software, Docuguide, WSystem. Naproti tomu následující aplikace nemají druhou kontrolu přístupu: SEMA Holzbausoftware, kompletní Office, kromě Outlook.</p>
6. Obnovení dat	
<p>K dispozici je samostatná komplexní koncepce zálohování a příručka pro případ nouze. Používá se zálohovací software od známých výrobců.</p>	
7. Průběžné posuzování a hodnocení	
<p>Je zavedena směrnice o ochraně osobních údajů. Byl jmenován pověřenec pro ochranu osobních údajů, který je pravidelně školen v oblasti ochrany osobních údajů. Zaměstnanci jsou pravidelně poučováni ve věci ochrany osobních údajů. Je zaveden proces ohlašování narušení bezpečnosti osobních údajů. Technická a organizační opatření každoročně kontroluje pověřenec pro ochranu osobních údajů a vedoucí oddělení IT. V rámci auditu se kontrolují opatření s ohledem na současný stav techniky a nezbytné technické a právní požadavky a v případě potřeby se upravují. Výsledek auditu je odpovídajícím způsobem zdokumentován.</p>	