Příloha č. 5

Smlouva o zpracování osobních údajů

(dále jen „**SZOÚ**")

Název/jméno a příjmení: **Jihočeské letiště České Budějovice a.s.**

se sídlem/místo podnikání: U Zimního stadionu 1952/2, 370 01, České Budějovice - České Budějovice

IČO: 26093545

DIČ: CZ26093545

zastoupený Robert Kaía, člen představenstva
(jméno, příjmení, funkce)
- dále jen „**Správce**" -

a

Continental Barum s.r.o.
Objízdná 1628
765 02 Otrokovice
IČO: 45788235, DIČ: CZ699000347
zapsaná v obchodním rejstříku vedeném u Krajského soudu v Brně, oddíl C, vložka 15057
Zastoupená: Ing. Martinem Budayem, jednatelem a Ing. Janem Černoškem, jednatelem
- dále jen „**Zpracovatel**" -

- dále společně „**Smluvní strany**" -

Tato SZOÚ stanoví právní závazky Smluvních stran s ohledem na ochranu osobních údajů vyplývajících ze zpracování osobních údajů v souvislosti se smlouvou

5339691 (název smlouvy)

ze dne ..... (dále jen „**Hlavní smlouva**").

SZOÚ se vztahuje na všechny činnosti spojené s Hlavní smlouvou, během níž mají Zpracovatel, zaměstnanci Zpracovatele a/nebo třetí osoby smluvně zajištěné Zpracovatelem přístup k osobním údajům, které mají být dle Hlavní smlouvy zpracovávané pro Správce (dále jen „**Osobní údaje**").

1. PŘEDMĚT A ÚČEL SZOÚ

1.1 Účelem této SZOÚ je vymezení práv a povinností Smluvních stran tak, aby zpracování Osobních údajů probíhalo v souladu s Nařízením Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů; dále jen „**EU GDPR**") a souvisejícími právními předpisy; a zároveň aby byla zajištěna dostatečná a účinná ochrana zpracovávaných Osobních údajů.

1.2 Zpracovatel při činnosti pro Správce podle Hlavní smlouvy bude zpracovávat Osobní údaje týkající se identifikovaných nebo identifikovatelných fyzických osob (dále jen „**Subjekt údajů**"). V takovém případě čl. 28 odst. 3 EU GDPR vyžaduje, aby spolu Smluvní strany uzavřely písemnou smlouvu o zpracování osobních údajů.

1.3 Správce tímto pověřuje Zpracovatele zpracováním Osobních údajů za podmínek sjednaných v této Smlouvě. Zpracovatel pověření Správce přijímá.

Continental

2. PŘEDMĚT A DOBA TRVÁNÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Zpracovatel zpracovává Osobní údaje výhradně pro Správce a v souladu s jeho pokyny. Zpracovatel je zodpovědný za dodržování ustanovení o ochraně osobních údajů podle platné legislativy.

2.1 Předmět zpracování Osobních údajů:
Předmět zpracovávání Osobních údajů, povaha a účel zpracování, jakož i typ Osobních údajů a kategorie Dotčených osob vyplývají:

- z potřeby plnění Hlavní smlouvy; a / nebo
- z potřeby plnění činností zpracování Osobních údajů uvedených v Příloze 1 (Podrobnosti o zpracovávání Osobních údajů); a / nebo
- z potřeby plnění doplňujícího písemného pokynu Správce, viz čl. 9 této ZSOÚ (dále jen „**Pokyny Správce**").

2.2 Doba trvání zpracování Osobních údajů:
Zpracovatel bude Osobní údaje zpracovávat po dobu trvání Hlavní smlouvy a této SZOÚ, nebo po kratší dobu v souladu s Pokyny Správce.

3. TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

3.1 Technická a organizační opatření přijatá Zpracovatelem jsou popsaná v Příloze 2 k této SZOÚ. Technická a organizační opatření jsou předmětem technologického postupu a dalšího vývoje. Zpracovatel je proto oprávněn provádět přiměřená alternativní opatření. Nesmí být ohrožena úroveň bezpečnosti prováděných opatření.

4. PRÁVA SUBJEKTU ÚDAJŮ – OPRAVY, OMEZENÍ ZPRACOVÁNÍ A VYMAZÁNÍ OSOBNÍCH ÚDAJŮ

4.1 Zpracovatel je povinen kontaktovat a poradit se se Správcem v případech, kdy se jedná o respektování práv Subjektů údajů a splnění z nich vyplývajících právních povinností Správce, zejména pokud jde o oznámení adresovaná Subjektu údajů, poskytování informací Subjektu údajů a opravu, vymazání a/nebo omezení zpracování Osobních údajů.

4.2 Zpracovatel může opravit, smazat Osobní údaje nebo omezit zpracování Osobních údajů pouze v souladu s Pokyny Správce. Pokud Subjekt údajů kontaktuje přímo Zpracovatele s žádostí o opravení nebo vymazání Osobních údajů nebo s jinou žádostí o výkon práva podle EU GDPR, pak je Zpracovatel povinen tuto žádost předat Správci.

4.3 Pokud je Správce právně zavázán poskytovat Subjektům údajů informace týkající se zpracování Osobních údajů, pak Zpracovatel poskytne Správci podporu při poskytování těchto informací, a to za podmínky, že Správce Zpracovatele písemně vyzve, přičemž veškeré náklady způsobené Zpracovateli za tyto podpůrné služby nese Správce.

5. KONTROLY A DALŠÍ POVINNOSTI ZPRACOVATELE

Zpracovatel je rovněž odpovědný za dodržování následujících povinností:

5.1 Ochrana důvěrnosti Osobních údajů: všechny osoby, které mají přístup k Osobním údajům z pověření Zpracovatele, zejména v rámci svého pracovněprávního či jiného smluvního vztahu, musí být zavázány k mlčenlivosti o Osobních údajích.

5.2 Provádění a dodržování všech nezbytných technických a organizačních opatření (viz čl. 3 této SZOÚ a článek 32 EU GDPR).

5.3 Schopnost ověřit přijatá technická a organizační opatření na žádost Správce. Zpracovatel může také předložit stávající osvědčení, zprávy nebo certifikace od nezávislých subjektů (jako jsou auditoři, inspektoři, pověřenci pro ochranu údajů, oddělení IT bezpečnosti, auditoři ochrany údajů a auditoři kvality) nebo vhodnou certifikaci z auditu IT bezpečnosti nebo ochrany údajů (např. v souladu se standardem Spolkového úřadu pro informační bezpečnost „BSI Basic Protection").

5.4 Kontroly prostřednictvím pravidelných přezkumů vykonávaných Zpracovatelem a týkající se provádění nebo plnění úkolů při zpracování Osobních údajů dle této SZOÚ, zejména dodržování a případné změny předpisů a opatření pro zpracování Osobních údajů. Oznámení Správci o nedostatcích a/nebo nesrovnalostech zjištěných během přezkumu.

5.5 Jmenování pověřence pro ochranu údajů, pokud je platnou legislativou vyžadováno. Správci budou poskytnuty kontaktní údaje za účelem přímého kontaktu.

5.6 Na vyžádání poskytnout úplnou písemní dokumentaci týkající se zpracování Osobních údajů, na jejichž základě může Správce kdykoli prokázat zákonnost zpracování Osobních údajů.

5.7 Poskytnutí informací a údajů potřebných pro evidenci činností zpracování Správcem; tyto informace musí být poskytnuty pouze na žádost Správce a pouze ve vztahu ke zpracování Osobních údajů.

5.8 Ke zpracování a používání Osobních údajů dochází výhradně v rámci území České republiky, jiného členského státu Evropské unie nebo v jiné zemi, která je stranou Dohody o Evropském hospodářském prostoru. V případě zpracování Osobních údajů ve třetí zemi nebo mezinárodní organizaci je Zprostředkovatel povinen zajistit odpovídající úroveň ochrany Osobních údajů v souladu s čl. 45-47 EU GDPR.

6. VYUŽITÍ SUBDODAVATELŮ

6.1 Pokud jsou Zpracovatelem zapojeni další zpracovatelé (dále jen „**Subdodavatelé**") do zpracování Osobních údajů poskytnutých Správcem, musí být splněny následující požadavky:

- Zpracovatel musí pečlivě vybrat Subdodavatele a před uzavřením smlouvy zajistit, že Subdodavatel bude schopen dodržovat dohody uzavřené mezi Správcem a Zpracovatelem.
- Přibrání Subdodavatelů je povoleno pouze na základě písemného souhlasu Správce.
- Zpracovatel je povinen uzavřít takové smlouvy se Subdodavatelem (Subdodavateli), aby bylo zajištěno dodržování ustanovení o ochraně údajů platných pro smluvní vztah mezi Správcem a Zpracovatelem.

6.2 Pokud Správce již souhlasil s využitím Subdodavatelů, pak jsou uvedeni v seznamu v Příloze 2 k této SZOÚ. Jakékoli pozdější zapojení Subdodavatelů musí být založeno na prokazatelném souhlasu Správce.

6.3 Služby poskytované Zpracovateli jako doplňkové služby na podporu Zpracovatele při zpracování Osobních údajů smluvně dojednaných se nepovažují za subdodavatelské vztahy ve smyslu tohoto ustanovení. Takové služby zahrnují například telekomunikační služby, údržbu a uživatelské služby, úklidové služby, auditorské služby nebo likvidaci paměťových médií. Zpracovatel je povinen uzavřít vhodné a zákonné dohody a přijmout kontrolní opatření k zajištění ochrany a bezpečnosti Osobních údajů Správce, a to i pokud jde o doplňkové služby zakoupené od třetích stran.

7. KONTROLNÍ PRÁVA SPRÁVCE

7.1 Zpracovatel souhlasí s tím, že Správce má právo kdykoli po předem doručeném písemném oznámení v nezbytném rozsahu v rámci běžné pracovní doby zkontrolovat dodržování předpisů o ochraně osobních údajů a ustanovení této SZOÚ Zpracovatelem, zejména prostřednictvím získání informací a kontroly uložených Osobních údajů a programů zpracování údajů.

7.2 Zpracovatel je povinen na požádání poskytnout Správci informace potřebné k plnění jeho povinností souvisejících se zpracováním Osobních údajů a poskytnout příslušné certifikace.

7.3 Náklady a / nebo výdaje spojené s realizací kontrol. práv Správce, zejména náklady na personál Zpracovatele, náklady poskytovatelů služeb výkonu kontroly, cest. náklady atd. snáší Zpracovatel. V případě, že náklady a / nebo výdaje Zpracovatele spojené s výkonem kontrolních práv Správce překročí výšku přiměřenou pro realizaci povinnosti Zpracovatele poskytnout informace podle čl. 28 odst. 3 písm. (h) EU GDPR, má Zpracovatel nárok na přiměřenou náhradu těchto nákladů a / nebo výdajů.

8. OZNÁMENÍ O PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

8.1 Zpracovatel je povinen oznámit Správci každý případ porušení zabezpečení Osobních údajů nebo porušení pověření založeného touto ZSOÚ, za který je zodpovědný Zpracovatel, jeho zaměstnanci nebo Subdodavatelé.

8.2 Povinnost podle bodu 8.1 výše se vztahuje i na případ vážného narušení provozního postupu, podezření na porušení ustanovení právních předpisů o ochraně osobních údajů nebo jiných nesrovnalostí při zacházení s Osobními údaji.

8.3 Pokud bude Správce povinen oznámit případy porušení ochrany Osobních údajů dozorovému úřadu, je Zpracovatel povinen poskytnout podporu Správci.

9. PRÁVO SPRÁVCE VYDÁVAT POKYNY

9.1 Osobní údaje budou zpracovány výlučně v souladu s touto ZSOÚ a Pokyny Správce. Změny v předmětu zpracování Osobních údajů a postupy musí být společně dohodnuty a zdokumentovány. Zpracovatel může vydávat informace třetím stranám nebo Subjektům údajů jen s předchozím písemným souhlasem Správce.

9.2 Slovní pokyny musí být neprodleně potvrzeny Správcem v psané podobě (např. e-mailem). Zpracovatel nebude používat Osobní údaje pro žádný jiný účel. Nebudou provedeny žádné kopie a duplikáty bez oznámení Správci. Tyto případy se nevztahují na záložní kopie, pokud jsou nezbytné k zajištění řádného zpracování Osobních údajů, a údaje potřebné pro splnění zákonných povinností archivace.

9.3 Zpracovatel bude Správce neprodleně informovat, pokud se domnívá, že Pokyny Správce nejsou v souladu s předpisy na ochranu osobních údajů. Zpracovatel je oprávněn pozastavit provádění dotyčného Pokynu Správce, dokud není potvrzen nebo změněn odpovědnou osobou jmenovanou Správcem.

10. VRÁCENÍ, VYMAZÁNÍ ÚDAJŮ/ODEVZDÁNÍ PAMĚŤOVÉHO MÉDIA

10.1 Na žádost Správce nebo při ukončení zpracování Osobních údajů dle této SZOÚ, avšak nejpozději na konci smluvního vztahu se Správcem, je Zpracovatel povinen vrátit Správci, nebo třetí osobě určené Správcem, všechny dokumenty, které má k dispozici, paměťová média, která mu byla poskytnuta, veškeré zpracované a použité výsledky a veškeré archivované údaje spojené se smluvním vztahem nebo vytvořené v důsledku zpracování Osobních údajů. Tato povinnost zahrnuje také kopie a/nebo reprodukce paměťových médií a/nebo archivovaných Osobních údajů. Zpracovatel nemá nárok na jejich zadržení. Takové odevzdání musí být bezplatné a nepodléhá žádným námitkám; veškeré náklady nebo jakékoli jiné výdaje spojené s vrácením nese Zpracovatel.

10.2 Po vrácení údajů podle ustanovení bodu 10.1 této SZOÚ nebo pokud se Správce vzdá takového vrácení, budou veškerá data, která jsou stále na paměťových médiích, Zpracovatelem zlikvidována nebo vymazána v souladu s platnými právními předpisy o ochraně osobních údajů; před konečným smazáním Osobních údajů je třeba získat souhlas Správce. Zpracovatel musí na požádání poskytnout Správci doklad o dokončení výmazu prostřednictvím příslušné dokumentace a/nebo příslušných prohlášení. Správce nemá právo požadovat, aby uchovávané Osobní údaje byly vymazány Zpracovatelem, pokud je Zpracovatel povinen tyto údaje na základě obecně závazného právního předpisu archivovat; u takových Osobních údajů bude Zpracovatel omezen z hlediska jejich zpracování. Zpracování takových Osobních údajů bude omezeno a nesmí dojít k jejich vymazání, pokud je tak právně přípustné (například na základě prováděcích zákonů týkajících se ochrany osobních údajů v jednotlivých místech/zemích), a zejména pokud vymazání není možné z důvodu konkrétního typu archivace (např. zákonné důvody), nebo pokud by to bylo spojeno s neúměrným množstvím práce.

10.3 Dokumentace sloužící k prokázání správného zpracování Osobních údajů v souladu s touto SZOÚ a zákonnými ustanoveními musí být archivována Zpracovatelem po skončení SZOÚ v souladu s platnými pravidly archivace. Ke zrušení této povinnosti může dojít předložením dokumentace na konci platnosti této SZOÚ.

10.4 Na testovací a zbytkový materiál platí odpovídajícím způsobem ustanovení bodů 10.1 a 10.2 této SZOÚ.

11. POVINNOSTI ZPRACOVATELE

11.1 Zpracovatel odpovídá za dodržování všech ustanovení platných právních předpisů o ochraně osobních údajů, zejména za zákonnost předání Osobních údajů Správci.

11.2 Zpracovatel poskytne Správci promptní a kompletní informaci, pokud při přezkumu výsledků zpracování zjistí nedostatky nebo nesoulad s platnou legislativou ochrany osobních údajů.

11.3 Zpracovatel vede záznamy o činnostech zpracování.

12. ODPOVĚDNOST

12.1 Povinnosti ochrany Osobních údajů uvedené v této SZOÚ jsou pro Zpracovatele významnými smluvními závazky (základními povinnostmi) Hlavní smlouvy uzavřené se Správcem. V tomto ohledu je tato SZOÚ považována za doplněk k Hlavní smlouvě.

13. VZTAH K HLAVNÍ SMLOUVĚ, OSTATNÍ ZÁVAZKY A DALŠÍ USTANOVENÍ

13.1 Ustanovení této SZOÚ, včetně jejích příloh, mají přednost před Hlavní smlouvou a slouží jako její doplněk, není-li v této SZOÚ stanoveno jinak.

13.2 V případě, že budou údaje Správce uložené Zpracovatelem ohroženy zablokováním nebo zabavením, insolvenčním řízením nebo řízením o narovnání dluhu nebo jinými událostmi nebo opatřeními zahájenými třetími stranami, Zpracovatel je povinen takovou událost bezodkladně oznámit Správci. Zpracovatel v takovém případě neprodleně informuje všechny věřitele, zástupce a další zúčastněné subjekty, že Správce má výhradní právo k vlastnictví údajů, paměťovým médiím, dokumentům apod.

13.3 Změny a/nebo dodatky k této SZOÚ jsou platné pouze v písemné podobě. To platí i pro zproštění požadavku na písemnou formu.

13.4 Pokud jde o rozhodné právo a místo jurisdikce, použijí se příslušná ustanovení Hlavní smlouvy.

13.5 V případě, že kterékoli ustanovení této SZOÚ není nebo přestane být platné, nebo pokud by tato SZOÚ nebyla úplná, neovlivňuje to platnost ostatních ustanovení. Neplatné nebo neúplné ustanovení se podle potřeby nahradí nebo doplní příslušným ustanovením, které odráží – do zákonně přípustného rozsahu – v maximální možné míře to, co měly Smluvní strany původně v úmyslu, nebo by podle smyslu a účelu této SZOÚ měly v úmyslu, jestliže by předmětnou okolnost byly zohlednily.

13.6 Seznam příloh:
Příloha 1 – Podrobnosti o zpracovávání Osobních údajů
Příloha 2 – Technická a organizační opatření na ochranu Osobních údajů zavedené u Zpracovatele

Za Správce:

18.9.2020
.....
Místo, datum

.....

.....

.....
Správce (uveďte název společnosti)
[titul, jméno, příjmení, funkce]

Za Zpracovatele:

- 6 -01- 2020
.....
Místo, datum

.....

.....

.....
Continental Barum s.r.o.
Ing. Jan Černošek, jednatel

Continental
Continental Barum s.r.o.
Objízdná 1628, 765 02 Otrokovice
M 30

Příloha 1

PODROBNOSTI O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. **Předmět, povaha a účel zpracovaní Osobních údajů**
   Za účelem plnění Hlavní smlouvy, níže uvedených činností a / nebo pokynů Správce, Správce pověřuje Zpracovatele výkonem zejména těchto činností zpracovávání Osobních údajů: Rozsah, druh a účel shromažďování, zpracování a/nebo používání osobních údajů podrobně vyplývá z Rámcové kupní smlouvy. To zahrnuje zejména postupy zpracování údajů pro obchodní aktivity a navazující marketingové programy na podporu prodeje, tj. spotřebitelských soutěží, PR aktivit, průzkumy spokojenosti zákazníků optimalizace mediálního nákupu, rozesílky POS materiálů a vysílání contiTV (písemně i elektronicky).

2. **Kategorie Subjektů údajů**
   - Zákazníci

3. **Typy (kategorie) Osobních údajů**
   Identifikační / soukromé kontaktní údaje:
   - Jméno, příjmení, příp. titul
   - Fotografie, obrazová podobizna
   - Údaje o soukromé adrese
   - Datum narození
   - Údaje z identifikačních průkazů (například občanský průkaz, pas, průkaz pojištění, řidičský průkaz)

   Údaje v souvislosti se smluvním vztahem:
   - Údaje o zúčtování a platbách
   - Historie nákupů / zakázek
   - Bankovní údaje / údaje o kreditních kartách
   - Finanční stav / kredibilita

   Profesní údaje:
   - Informace o osobě
   - Pozice a odpovědnosti
   - Kvalifikace a vzdělání

   Údaje o užívání služeb a IT:
   - Identifikátory zařízení
   - Údaje o používání a připojení
   - Obrazové podobizny / video záznamy
   - Audio / hlasové údaje
   - Telekomunikační údaje / obsah zpráv
   - Identifikační údaje
   - Přístupové údaje
   - Autorizace
   - Meta data

Příloha 2

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ NA OCHRANU OSOBNÍCH ÚDAJŮ ZAVEDENÉ U ZPRACOVATELE

(dle čl. 32 EU GDPR)

Minimální požadavky na technická a organizační opatření při zacházení s informacemi zavedené u Zpracovatele jsou stanoveny v interním předpisu korporace Continental s názvem „P60.02 - The Corporate Policy Continental Information Security Guideline" (dále jen „**CISG**"), v překladu Příručka o informační bezpečnosti ve společnosti Continental. V závislosti na klasifikaci příslušných informací se implementují i další opatření nad rámec těchto minimálních požadavků.

Požadavky stanovené v CISG jsou implementovány ve společnostech koncernu Continental na základě Rámce pro korporátní IT bezpečnost (ang. Corporate Standard Information Security Framework) a příslušného Systému řízení informační bezpečnosti (ang. Information Security Management System, dále jen „**ISMS**").

Relevantní interní předpisy v oblasti IT bezpečnosti platné ve společnostech koncernu Continental (pozn.: názvy předpisů jsou uvedeny níže v anglickém originálu pro jejich jasnější identifikaci, jazykové verze těchto předpisů se mohou měnit, závazná je anglická verze):
- Corporate Policy Continental Information Security Guideline (CISG)
- Corporate Standard Information Security
- Annex 1 - Information Security Management System (ISMS)
- Annex 2 - Roles & Responsibility in Information Security – RACI Chart

1. Kontrola fyzického přístupu

Zabezpečení vstupu/přístupu ke zpracovatelským systémům před neoprávněnými osobami (např. prostřednictvím fyzické ochrany objektu: plot, vrátnice, bezpečnostní služba, závora, turniket, dveře se zámkem, dveře se čtečkou karet, kamerový dohled, organizační zabezpečení majetku, pravidla pro oprávněný přístup, registrace přístupů).

1.1 Následující tech. a organiz. opatření byla provedena Zpracovatelem pro zpracování Osobních údajů popsaných v SZOÚ, v souladu s:

- Corporate Standard Classification of Security Zones
- Annex 1 - Layout and Security Requirements
- Annex 2 - Audio/Visual Recording in Locations
- Corporate Standard Continental ID Cards
- Poplašný systém
- Systém automatického řízení přístupu
- Světelné bariéry/senzory pohybu
- Systém ručního zamykání včetně nastavení klíče (klíčová kniha, vydání klíče)
- Přihlašování návštěvníků
- Pečlivý výběr bezpečnostních pracovníků
- Čipové karty/transpondérové zamykací systémy
- Sledování vstupních dveří videem
- Bezpečnostní zámky
- Osobní prohlídky na vrátnici/recepci
- Pečlivý výběr úklidového personálu
- Povinnost nosit identifikační karty zaměstnanců/hostů
- Různé: deklarováno směrnicemi Zpracovatele S03OS, S06OS, S07OS, S08OS a Prohlášení pro cizí firmy dostupné na vyžádání.

2. Řízení přístupu k údajům/řízení uživatelů

Zajištění proti přístupu neoprávněných osob k automatizovaným systémům zpracování Osobních údajů, zejména pokud je po přístupu do systému možné zkopírovat Osobní údaje (např. potřeba opětovného zadání hesla po spuštění spořiče obrazovky).

2.1 Následující tech. a organiz. opatření byla provedena Zpracovatelem pro zpracování Osobních údajů popsaných v SZOÚ, v souladu s:

- Corporate Manual Password Regulation (M60.02.01)
- Corporate Standard Procedure for Identification and Authorization of Users of IT
- Corporate Standard Client Security Regulation
- Corporate Standard Mobile Environment Governance
- Ověřování pomocí uživatelského jména/hesla (hesla přiřazená na základě platných předpisů o heslech)
- Použití systémů detekce narušení
- Použití antivirového softwaru
- Použití firewall softwaru
- Vytvoření uživatelských profilů
- Přiřazení uživatelských profilů k IT systémům
- Využití technologie VPN
- Použití centrálního administrativního softwaru pro smartphony (např. pro externí vymazání dat)

3. Dohled nad použitím údajů/ukládáním údajů na paměťových médiích/řízením paměti

Předcházení neoprávněnému čtení, kopírování, změně nebo vymazání paměťových nosičů (kontrola paměťových médií), prevence neoprávněného zadávání Osobních údajů a neoprávněný přístup k nim, změna a mazání uložených Osobních údajů (kontrola paměti). Zajistit, aby osoby oprávněné používat automatizovaný systém pro zpracování údajů měly přístup pouze k Osobním údajům, které jsou vhodné pro jejich typ oprávnění (např. prostřednictvím autorizace, hesel, předpisů pro případné opuštění společnosti a přesunutí zaměstnanců do jiných oddělení), (kontrola použití dat).

3.1 Následující tech. a organiz. opatření byla provedena Zpracovatelem pro zpracování Osobních údajů popsaných v SZOÚ, v souladu s:

- Corporate Manual Password Regulation (M60.02.01)
- Corporate Standard Procedure for Identification and Authorization of Users of IT Systems
- Corporate Standard Classification and Control of Information
- Corporate Manual Security Guidelines for Databases - 3.4.6 Data Integrity
- Úlohy a oprávnění založená na principu „potřeby vědět" (neshromažďovat nepotřebné OÚ)
- Počet administrátorů byl zmenšen pouze na „potřebné"
- Zaznamenávání přístupu k aplikacím, zejména záznamům, změnám a vymazání dat
- Fyzické vymazání paměťových médií před opětovným použitím
- Použití skartovacích přístrojů nebo poskytovatelů takových služeb
- Řízení práv určenými správci systému
- Pokyny pro nastavení hesel, vč. jejich délky a změn

4. Řízení předání/řízení přepravy

Zajistit ochranu důvěrnosti a integrity Osobních údajů při předání Osobních údajů a při přepravě datových médií (např. řádným šifrováním datových přenosů, uzavřenými obálkami používanými v poštovních zásilkách, šifrovaným ukládáním na paměťových nosičích).

4.1 Následující tech. a organiz. opatření byla provedena Zpracovatelem pro zpracování Osobních údajů popsaných v SZOÚ, v souladu s:

- Corporate Standard Classification
- Control of Information
- Zřízení vyhrazených linek nebo VPN tunelů
- Šifrovaný přenos dat na internetu (například HTTPS, SFTP apod.)
- Kódování e-mailu
- V případě fyzické přepravy: pečlivý výběr přepravního personálu a vozidel
- V případě fyzické přepravy: zabezpečené kontejnery/balení

5. Kontrola vstupu/řízení přenosu

Zajistit, aby bylo možné následně prověřit a stanovit, které Osobní údaje byly zadány v automatizovaných systémech zpracování údajů, nebo změněny, a v jaké době a kým, například prostřednictvím protokolování (kontroly vstupu). V závislosti na systému dostatečně zajistit, aby bylo možné zkontrolovat a určit, komu a kam byly Osobní údaje předány nebo poskytnuty prostřednictvím zařízení pro přenos dat, nebo komu a kam by mohly být předány (kontrola přenosu).

5.1 Následující tech. a organiz opatření byla provedena Zpracovatelem pro zpracování Osobních údajů popsaných v SZOÚ, v souladu s:

- Continental Information Security Guideline (CISG) – 3.5.10.1 Audit Logging
- Corporate Standard Procedure for Identification and Authorization of Users of IT Systems
- Corporate Standard Classification and Control of Information
- Corporate Manual Security Guidelines for Databases - 3.4.6 Data Integrity
- Protokolování záznamu, změn a vymazání dat
- Sledovatelnost záznamu, změn a vymazání dat pomocí specifických uživatelských jmen (nikoli skupin uživatelů)
- Přidělování práv k záznamu, změny a vymazání údajů na základě příslušného oprávnění
- Vytvoření přehledu, která data mohou být zadána, změněna a smazána s jakými aplikacemi
- Uchování formulářů, z nichž jsou data přebírána v automatizovaném zpracování (dle P70.1 Record Retention)

6. Řízení dostupnosti/obnovení/spolehlivosti/integrita Osobních údajů

Zajistit, aby systémy mohly být obnoveny v případě poruchy (obnovitelnost). Zajistit, aby fungovaly všechny funkce systému a veškeré výpadky byly ohlášeny (spolehlivost). Zajistit, aby uložené Osobní údaje nemohly být poškozeny systémovými poruchami (integrita údajů). Zajistit ochranu Osobních údajů před náhodným zničením nebo ztrátou (dostupnost), např. zavedením vhodných programů pro zálohování a obnovu dat po výpadku systému.

6.1 Následující tech. a organiz. opatření byla provedena Zpracovatelem pro zpracování Osobních údajů popsaných v SZOÚ:

- Corporate Manual Backup
- Recovery Security Regulation (M60.02.08)
- Nepřerušitelný zdroj napájení (UPS)
- Přístroje pro monitorování teploty a vlhkosti v serverových místnostech
- Požární a kouřové detektory
- Alarmy pro neoprávněný přístup do serverových místností
- Testy obnovitelnosti dat
- Ukládání datových záloh na samostatném a bezpečném místě
- V záplavových zónách: serverové místnosti nad povodňovou hladinou vody
- Klimatizační jednotky v serverových místnostech
- Zásuvky s přepěťovou ochranou v serverových místnostech
- Hasicí přístroje v serverových místnostech
- Vytvoření koncepce zálohování a obnovení dat
- Vytvoření nouzového plánu

7. Kontrola rozdělení/oddělitelnost

Zajistit, aby Osobní údaje shromážděné pro různé účely mohly být zpracovány samostatně (například logickým oddělením údajů o zákaznících, specializovanými kontrolami přístupu (autorizační koncept), oddělením testovacích a výrobních údajů).

7.1 Následující tech. a organiz. opatření byla provedena Zpracovatelem pro zpracování Osobních údajů popsaných v SZOÚ, v souladu s:

- Continental Information Security Guideline (CISG) – 3.5.1.4 Separation of development, test and operational facilities
- Fyzicky oddělené ukládání v samostatných systémech nebo paměťových médiích
- Vytváření databázových práv
- Logické oddělení zákazníků (v softwaru)
- Oddělení výrobních a zkušebních systémů

8. Subdodavatelé

Zajistit přiměřenou úroveň technických a organizačních bezpečnostních opatření i na straně subjektů, které jsou Zpracovatelem zapojeny do zpracování Osobních údajů nebo mají přístup k Osobním údajům (výběr vhodného dodavatele). Pokud jsou zajišťováni Subdodavatelé (např. pro webhosting, poskytování výpočetního střediska, provozní software používaný ke zpracování Osobních údajů apod.) při zpracování Osobních údajů popsaných Zpracovatelem, pak realizace technických a organizačních opatření příslušného Subdodavatele musí být upravena vhodnými smlouvami o zpracování osobních údajů. Subdodavatel musí poskytovat dostatečné záruky, že zajistí minimálně taková technická a organizační opatření, jaká jsou dohodnuta mezi Správcem a Zpracovatelem.

8.1 Aktuální seznam Subdodavatelů je uveden zde:
https://www.continental-pneumatiky.cz/osobni/pravidla-ochrany-udaju/agentury-cz