**PŘÍLOHA Č. 3**

**TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ**

Technická a organizační opatření - vyjádření Zpracovatele – ke Zpracovatelské smlouvě č. …………..

[x]  Řádné

[ ]  Opravné

# Důvěrnost

## Řízení fyzického přístupu

1.1.1 Osobní data Správce jsou uložena a/nebo zpracovávána:

[ ]  v kancelářích Zpracovatele

[ ]  v datových centrech nebo serverovnách Správce

[ ]  u poskytovatele IT služeb (např. poskytovatele cloudu):\_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  nehodí se

Osobní údaje patřící Správci jsou uloženy a / nebo zpracovány:

[ ]  v kancelářích Zpracovatele

[ ]  v datovém centru Správce nebo v serverech

[ ]  u následujícího poskytovatele IT služeb (např. Poskytovatele cloudu):\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 nebo [ ]  nehodí se

1.1.2 Budovy jsou zabezpečeny pomocí následujících opatření:

 Bezpečnostní systém Video monitoring Jiné nehodí se

1.2.1.1 Kancelářská budova: [ ]  [ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]

1.1.2.2 Datové centrum: [ ]  [ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]

1.1.3 Přístup do prostor je zabezpečen:

 Manuálně zamykací syst. Smart karta systém Jiné\* nehodí se

1.1.3.1 Kanceláře [ ]  [ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]

1.1.3.2 Serverovny [ ]  [ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]

1.1.3.2 Datové centrum [ ]  [ ]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]

\*např. Body jednotného přístupu, biometrická kontrola

1.1.4 Oprávněný přístup je zdokumentován podle jména:

[ ]  ano [ ]  ne [ ]  nehodí se

1.1.5 Pravidla pro přístup do budovy pro třetí strany/hosty/návštěvy:

 Jmenná dokumentace. Vstup, pobyt v doprovodu nehodí se

 Ano Ne

1.1.5.1 Kanceláře [ ]  [ ]  [ ]  [ ]

1.1.5.2 Serverovny [ ]  [ ]  [ ]  [ ]

1.1.5.2 Datové centrum [ ]  [ ]  [ ]  [ ]

1.1.6 Pravidla pro vstup do budovy pro personál úklidu a údržby:

 Jmenná dokumentace. Vstup, pobyt v doprovodu nehodí se

 Ano Ne

1.1.6.1 Kanceláře [ ]  [ ]  [ ]  [ ]

1.1.6.2 Serverovny [ ]  [ ]  [ ]  [ ]

1.1.6.2 Datové centrum [ ]  [ ]  [ ]  [ ]

1.1.7 Existují zdokumentovaná pravidla pro odebrání oprávnění vstupu do budov a přístupových práv k počítačovým systémům při odchodu zaměstnance:

[ ]  ano [ ]  ne

## Řízení přístupu do systému

1.2.1 Síť společnosti je oddělena od veřejné sítě pomocí firewallu:

[ ]  ano [ ]  ne

pokud ano:

1.2.1.1 Typ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.1.2 Postup a časový interval aktualizací: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.2 Pro všechny IP adresy napojené na internet jsou pravidelně prováděny penetrační testy:

[ ]  ano [ ]  ne

1.2.3 Zaměstnanci musí dodržovat následující požadavky ohledně hesla:

1.2.3.1 [ ]  individuální heslo do počítače každého ze zaměstnanců, které musí být udržováno v tajnosti

1.2.3.2 [ ]  případně minimální délka: počet znaků/složitost: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.3.3 [ ]  případně interval změny: prosím uveďte interval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.3.4 [ ]  automatické zamykání obrazovky po určité době: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.4 Na následujících rozhraních do sítí společnosti jsou používány antivirové programy:

[ ]  E-mail [ ]  FTP [ ]  Internet

1.2.5 Antivirový program se používá na všech serverech:

1.2.5.1 [ ]  ano Způsob a frekvence aktualizací:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.5.2 [ ]  ne Uveďte operační systém a důvod: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  nehodí se - důvod: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.6 Antivirový program se používá na všech počítačích na jednotlivých pracovištích:

1.2.6.1 [ ]  ano Způsob a frekvence aktualizací: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.6.2 [ ]  ne Uveďte operační systém a důvod: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  nehodí se - důvod: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.2.7 Aktualizace bezpečnostního softwaru jsou nahrávány do stávajícího softwaru pravidelně a automaticky:

[ ]  ano [ ]  ne

1.2.8 Na počítačích na jednotlivých pracovištích mají práva místní správy následující zaměstnanci

Správci, vývojáři, technici: [ ]  ano [ ]  ne

Uživatelé: [ ]  ano [ ]  ne

1.2.9 Zaměstnanci mají oprávnění přístupu na internet:

1.2.9.1 [ ]  ano [ ]  ne

Pokud ano: je nainstalována omezená konfigurace prohlížeče, kterou zaměstnanci nemohou změnit:

1.2.9.2 [ ]  ano [ ]  ne [ ]  nehodí se

## Řízení přístupu k datům

1.3.1 Jsou zavedeny zdokumentované koncepty založené na rolích:

[ ]  ano [ ]  ne

1.3.2 Organizace udělování oprávnění je založena na jmenné dokumentaci (zejména kdo může udělit jaká práva):

[ ]  ano [ ]  ne

1.3.3 Přístupová práva jsou přidělována na základě potřeby práce s daty, a jsou aktualizována a jmenně zdokumentována:

[ ]  ano [ ]  ne

1.3.4 Počet administrátorů s povolením kopírovat/exportovat databáze Správce úplně nebo ve velkém rozsahu: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.3.5 Počet zaměstnanců (ne správců!) s povolením kopírovat/exportovat databáze Správce úplně nebo ve velkém rozsahu: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Formáty, v nichž může probíhat export (např. csv, xlsx): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.3.6 Následující součásti počítačů pracovní stanice jsou uzamčeny/deaktivovány tak, že nelze externě uložit žádná exportovaná data:

[ ]  USB porty

[ ]  CD/DVD vypalovačky

[ ]  sloty paměťových karet

[ ]  Jiné mobilní nosiče dat, pokud ano, jaké: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  Nejsou deaktivovány žádné nosiče

1.3.7 Je nastavena vzdálená údržba/vzdálený přístup pro:

[ ]  Jiné poskytovatele

[ ]  Zaměstnance

Pokud ano, vyplňte prosím následující údaje:

1.3.7.1 Typ ověřování: (např. heslo, nebo PIN a token): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.3.7.2 Při ověřování heslem:

odchylky od informací pod bodem 1.2.3\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.3.7.3 Použité protokoly nebo mechanismy (např. SSH, VPN, RDP): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.3.7.4 Další bezpečnostní opatření: (např. schvalování jednotlivých relací\_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  není nastaven vzdálený přístup/údržba

1.3.8 Zpracovatel má stanovena pravidla pro mobilní práci (např. z domova) k zajištění důvěrnosti, integrity, dostupnosti a odolnosti zpracování dat (tato informace nenahrazuje souhlas odběratele požadovaný pro mobilní práci v souladu s přílohou „Dodatečné podmínky - zpracování dat [ZB/D]“):

1.3.8.1 [ ]  ano [ ]  ne

Zaměstnanci prošli školením mobilní práce, a existuje jmenná dokumentace tohoto školení

1.3.8.2 [ ]  ano [ ]  ne nebo [ ]  nehodí se

## Řízení separace

1.4.1 Jaká opatření byla přijata pro oddělení dat Správce?

[ ]  Vyhrazený klient určený pro tuto zakázku

[ ]  Oddělení sítě pomocí následujících opatření: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  nehodí se

1.4.2 Pro výše uvedené sítě/segmenty Správce je zavedena koncepce přístupu založená na rolích, což vylučuje, aby zaměstnanci, kteří pro klienta nepracují, měli přístup k datům:

[ ]  ano [ ]  ne [ ]  nehodí se

1.4.3 Zaměstnanci byli písemně zavázání nepoužívat informace z databází Správce v jiných projektech / pro jiné účely:

[ ]  ano [ ]  ne [ ]  nehodí se

# Integrita dat

## Řízení zpřístupnění

2.1.1 Pokud jsou mezi Správcem a Zpracovatelem přenášena data pomocí nosičů dat (např. papírové dokumenty, pevný disk, USB disk, CD):

Jsou data na nosiči šifrována: [ ]  ano [ ]  ne

2.1.1.1 Pokud ano, jakým postupem: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.1.1.2 Postup odpovědi Správci při obdržení nebo podezření na ztrátu: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  Nosiče dat se nepoužívají

2.1.2 Druh šifrování při předávání dat mezi Zpracovatelem a Správcem, pokud jsou data předávána elektronicky:

2.1.2.1 [ ]  SFTP

2.1.2.2 [ ]  S/MIME

2.1.2.3 [ ]  HTTPS (např. webové rozhraní, cloudové úložiště), prosím popište: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.1.2.4 [ ]  SSL-VPN nebo Citrix; prosím popište: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.1.2.5 [ ]  Jiné; prosím popište: \_\_\_\_\_\_\_\_\_\_\_\_\_\_nebo [ ]  Data nejsou předávána elektronicky

2.1.3 Jsou Zpracovatelem uchovávána osobní data Správce?

[ ]  ano, nešifrovaná [ ]  ano, šifrovaná [ ]  ne

 2.1.3.1 Pokud jsou data uchovávána v šifrované podobě, popište prosím postup: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.1.4 Jakým způsobem jsou chráněna data Správce na zálohách (např. bezpečné uložení na zálohovém médiu, šifrování záloh)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ nebo [ ]  Data objednatele nejsou zálohována

2.1.5 Mazání dat Správce:

2.1.5.1 Jak probíhá mazání dat (např. v souladu se standardními postupy)?

Elektronická data v systémech \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]  nehodí se

Elektronické nosiče dat: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]  nehodí se

Papírové dokumenty: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]  nehodí se

2.1.5.2 Kdy jsou data smazána, nebo zničeny nosiče dat?\_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  nehodí se

2.1.5.3 Jakým způsobem je dokumentováno mazání dat nebo likvidace nosičů? \_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  nehodí se

2.1.6 Opatření na ochranu dat Správce (včetně dočasných) na mobilních zařízeních:

Mobilní pracovní stanice / nosiče dat atd. (např. ochranné filtry na obrazovce, šifrování; případně uveďte podrobnosti o šifrování):

2.1.6.1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]  žádná opatření [ ]  nehodí se

Chytré telefony, tablety apod. (např. řízení mobilních zařízení, šifrování případně uveďte podrobnosti o šifrování):

2.1.6.2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ ]  žádná opatření [ ]  nehodí se

## Řízení vstupů

2.2.1 Pro možnost sledování mazání nebo změn v datech Správce byly pro jednotlivé zaměstnance vytvořeny soubory záznamů označené jménem:

[ ]  ano [ ]  ne [ ]  nehodí se

2.2.2 Tyto soubory záznamů jsou vytvořeny na základě omezeného přístupu:

[ ]  ano [ ]  ne [ ]  nehodí se

# Dostupnost a odolnost

## Řízení dostupnosti

3.1.1 Podrobnosti zálohování dat:

3.1.1.1 Frekvence zálohování (časový interval): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

 3.1.1.2 Počet uchovávaných generací záloh\_\_\_\_\_\_\_\_\_\_\_\_\_\_ nebo [ ]  nehodí se

3.1.2 Umístění médií se zálohou:

[ ]  Safe [ ]  Externí úložiště vzdálené ≥5 km (vzdušnou čarou), nebo [ ]  nehodí se

3.1.3 Doba opětovného spuštění po úplném zničení datového centra ve dnech: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ nebo [ ]  nehodí se

3.1.4 Údržba IT systémů je zabezpečena smluvně třetími stranami:

[ ]  ano, pouze v rámci zemí EU ☐ ano, je možný přístup k datům ze třetích zemí [ ]  ne

# Postupy pro pravidelné přezkoumání a hodnocení

## Řízení objednávky

4.1.1 Zaměstnanci Zpracovatele, kteří zpracovávají nebo mají přístup k osobním údajům Správce, se písemně zavázali zachovávat mlčenlivost ve vztahu k zacházení s osobními údaji:

[ ]  ano [ ]  ne

4.1.2 Zaměstnanci byli písemně zavázáni k zachovávání mlčenlivosti v telekomunikačním styku

[ ]  ano [ ]  ne

4.1.3 Zaměstnavatel od svých zaměstnanců vyžaduje následující písemná prohlášení (v souvislosti s ochranou osobních údajů a dat a/nebo v souvislosti s mobilní prací): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

4.1.4 Při využití subdodavatelů, kteří mají přístup k datům Správce:

4.1.4.1 Byly uzavřeny smlouvy se subdodavateli, kteří zpracovávají údaje Správce podle § 4 a 8 a § 28 EU BDSG a případně a případně zabezpečena provozní bezpečnost podle článku 4 směrnice 2002/58/EG ve spojení se směrnicí 009/136/EG:

[ ]  ano [ ]  ne

4.1.4.2 Existují subdodavatelé mimo EU, kteří mají přístup k údajům Správce:

[ ]  ano [ ]  ne

4.1.4.3 Subdodavatelé, kteří mají přístup k údajům Správce, dodržují tato technická a organizačními opatření sjednaná v tomto kontrolním seznamu stejně jako sám Zpracovatel, což je ošetřeno smluvně:

[ ]  ano [ ]  ne nebo [ ]  Nejsou využívání subdodavatelé, kteří mají přístup k datům objednatele

4.1.5 Je zavedeno školení pro zaměstnance s ohledem ochranu osobních údajů, které je jmenně dokumentováno:

[ ]  ano [ ]  ne

4.1.6 V současné době máme následující certifikáty/koncepty ochrany dat pro společnost Zpracovatele, které předkládáme zároveň s tímto kontrolním seznamem (uveďte příslušné názvy a data):\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4.1.7 Pokud je prováděna údržba s vyžitím cloudu (viz 1.1.1, 2.1.2, 4.1.4), je třeba předložit i schéma architektury, znázorňující použité komponenty, místa úložišť a použité protokoly (prosím uveďte název a datum):\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Jiné

4.2.1 Zpracovatel používá následující postupy k pravidelné kontrole a hodnocení účinnosti technických a organizačních opatření, s cílem zajistit bezpečné zpracování dat ve smyslu čl. 32 odst. 1 GDPR:

[ ]  ISMS v souladu s následující normou (např. ISO 27001/2): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  Jiný postup (prosím uveďte): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

nebo [ ]  nehodí se - důvod: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 4.2.2 Pokud plnění podle této smlouvy zahrnuje také poskytování služeb nebo vývoj softwaru (např. Software jako služba): Společnost Zpracovatele má zavedená pravidla (uveďte prosím název a datum):

4.2.2.1 na "ochranu údajů po projektování", s cílem zohlednit právo na soukromí při vývoji a navrhování výrobků, služeb a aplikací (např. opatřeními, jako je pseudonymizace): \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 4.2.2.2 využití osobních údajů při vyvíjení softwaru: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ nebo [ ]  nehodí se

4.2.3 Společnost Zpracovatele má zavedeny směrnice na postup v případě bezpečnostních incidentů:

4.2.3.1 [ ]  ne [ ]  ano (uveďte prosím jaké): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Zajišťují tyto směrnice, že je Správce okamžitě informován?

4.2.3.2 [ ]  ne [ ]  ano (popište prosím postup): \_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Podpis

## Potvrzujeme, že zde uvedené informace odpovídají aktuálnímu stavu námi zavedených technických a organizačních opatření k ochraně Osobních údajů. Odchylky od zde poskytnutých informací budou prokazatelně oznámeny Správci bez zbytečného odkladu.

Za Zpracovatele:

V \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ dne \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Za Zpracovatele:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jméno a příjmení osoby Pracovní zařazení

Název společnosti

## Vyjádření Správce k technickým a organizačním opatřením Zpracovatele:

[ ]  Předložené zajištění technických a organizačních opatření je dostačující. Souhlasíme s uzavřením Smlouvy.

[ ]  Předložené zajištění technických a organizačních opatření je nedostačující. V zajištění technických a organizačních opatření požadujeme učinit úpravy v  a to v rozsahu: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Za Správce:

V \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ dne: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jméno a příjmení osoby Pracovní zařazení

Název společnosti