

| Řádek                                    | Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem  | Podklad, kterým poskytovatel doloží splnění požadavku   | Bezpečnostní úroveň nabízeného cloud computingu |         |        |          | Třída cloud computingu                  |                                    |  |
|--|--|---|---|---------|--------|----------|---|------------------------------------|--|
|  |  |   | Nízká   | Střední | Vysoká | Kritická | cloud computing ve formě infrastruktury | cloud computing ve formě platformy | cloud computing ve formě aplikačního programového vybavení |
| <b>1. Místo zpracování a uložení dat</b> |  |   |   |         |        |          |   |                                    |  |
| 1.1                                      | Poskytovatel uvádí informace o všech územích států, ve kterých jsou nebo mohou být uložena zákaznická data ve stavu neaktivních dat a specifické provozní údaje ve stavu neaktivních dat, a dále uvádí informace o všech územích států mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, ve kterých předpokládá zpracování zákaznických dat a specifických provozních údajů. | <p>Písemný popis, ze kterého bude vyplývat, na území jakých států jsou nebo mohou být uložena zákaznická data ve stavu neaktivních dat a specifické provozní údaje ve stavu neaktivních dat a na území jakých států mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu se předpokládá zpracování zákaznických dat a na území jakých států se předpokládá zpracování specifických provozních údajů.</p> <p>Má se za to, že předpokládanými územími států, na nichž dochází nebo může docházet ke zpracování zákaznických</p> | X   | X       |        |          | X                                       | X                                  | X  |

|  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|
|  |  | <p>dat nebo specifických provozních údajů nejsou:</p> <ul style="list-style-type: none"><li>- území států, z nichž se mohou nepravdělně vzdáleně připojovat pracovníci technické podpory poskytovatele cloud computingu za účelem technické podpory služby cloud computingu, která se v čase mění a nemohou být specifikována předem;</li><li>- území států, do nichž poskytovatel může předávat zákaznická data nebo specifické provozní údaje za účelem poskytování volitelné doplňkové služby se zapojením třetích stran, která není sama o sobě cloud computingem, aktivované podle volby zákazníka,</li></ul> |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|

|     |  |   |   |   |   |   |   |   |   |
|-----|--|---|---|---|---|---|---|---|---|
|     |  | <p>s tím, že poskytovatel jasně označí třetí stranu, jíž může předat zákaznická data nebo specifické provozní údaje, a je-li to možné, blíže specifikuje, jaká zákaznická data nebo jaké specifické provozní údaje zpravidla předává a na jakou předpokládanou dobu zákaznická data nebo specifické provozní údaje předává.</p> |   |   |   |   |   |   |   |
| 1.2 | <p>Poskytovatel uvádí informace o všech územích států, ze kterých dochází k výkonu správy a dohledu nad službou cloud computingu.</p>  | <p>Písemný popis, ze kterého bude vyplývat, z území jakých států dochází k výkonu správy a dohledu nad službou cloud computingu.</p>  | X | X | X | X | X | X | X |
| 1.3 | <p>Zákaznická data ve stavu neaktivních dat jsou ukládána nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu.</p> <p>V případě, že služba cloud computingu daný požadavek nespĺňuje, poskytovatel takovou službu jasně označuje a uvádí, zda taková služba</p> | <p>Odkaz na část smluvních podmínek, kde je vymezen závazek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států</p>  |   |   | X |   | X | X | X |

|  |  |   |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|
|  | <p>cloud computingu ukládá zákaznická data ve stavu neaktivních dat v pseudonymizované podobě nebo nepseudonymizované podobě.</p> <p>Poskytovatel uvádí místo uložení zákaznických dat ve stavu neaktivních dat.</p> <p>Na základě označení služby cloud computingu jako služby cloud computingu, která nesplňuje požadavek na uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, bude tato služba cloud computingu uvedena na internetových stránkách Národního úřadu pro kybernetickou a informační bezpečnost a daný požadavek se na ni neuplatní. Taková služba cloud computingu bude rovněž označena v katalogu cloud computingu jako služba cloud computingu zapsaná na základě uvedené výjimky citací uvedené výjimky.</p> | <p>Evropského sdružení volného obchodu,</p> <p>nebo v případě, že se požadavek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu nevztahuje na danou službu, jasné označení takové služby a zároveň odkaz na část smluvních podmínek, kde je vymezen závazek uložení zákaznických dat ve stavu neaktivních dat v pseudonymizované podobě,</p> <p>nebo v případě, že se požadavek uložení zákaznických dat ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu neuplatní na danou službu a zároveň taková služba ukládá zákaznická data ve stavu neaktivních dat v nepseudonymizované podobě, jasné označení takové služby.</p> |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|

|     |  |  |  |  |   |  |   |   |   |
|-----|--|--|--|--|---|--|---|---|---|
|     |  | <p>Poskytovatel dále doloží odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) nebo auditní zprávu SOC 2® Type 2, s odkazem na tu část, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých budou zákaznická data uložena ve stavu neaktivních dat s označením, zda jsou nebo nejsou v daném datovém centru uložena v pseudonymizované podobě.</p> |  |  |   |  |   |   |   |
| 1.4 | <p>Specifické provozní údaje jsou ve stavu neaktivních dat ukládány nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu.</p> <p>V případě, že služba cloud computingu daný požadavek nespĺňuje, poskytovatel takovou službu jasně označuje a uvádí, zda taková služba</p> | <p>Odkaz na část smluvních podmínek, kde je vymezen závazek uložení specifických provozních údajů ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských</p>  |  |  | X |  | X | X | X |

|  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|
|  | <p>cloud computingu ukládá specifické provozní údaje ve stavu neaktivních dat v pseudonymizované podobě nebo nepseudonymizované podobě.</p> <p>Poskytovatel uvádí místo uložení specifických provozních údajů ve stavu neaktivních dat.</p> <p>Na základě označení služby cloud computingu jako služby cloud computingu, která nesplňuje požadavek na uložení specifických provozních údajů ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu, bude tato služba cloud computingu uvedena na internetových stránkách Národního úřadu pro kybernetickou a informační bezpečnost a daný požadavek se na ni neuplatní. Taková služba cloud computingu bude rovněž označena v katalogu cloud computingu jako služba cloud computingu zapsaná na základě uvedené výjimky citací uvedené výjimky.</p> | <p>států Evropského sdružení volného obchodu,</p> <p>nebo v případě, že se požadavek uložení specifických provozních údajů ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu nevztahuje na danou službu, jasné označení takové služby a zároveň odkaz na část smluvních podmínek, kde je vymezen závazek uložení specifických provozních údajů ve stavu neaktivních dat v pseudonymizované podobě,</p> <p>nebo v případě, že se požadavek uložení specifických provozních údajů ve stavu neaktivních dat nepřetržitě a výlučně na území členských států Evropské unie a členských států Evropského sdružení volného obchodu neuplatní na danou službu a zároveň taková služba ukládá specifické provozní údaje ve stavu neaktivních dat v nepseudonymizované</p> |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|

|     |  |   |  |  |   |  |   |   |   |
|-----|--|---|--|--|---|--|---|---|---|
|     |  | <p>podobě, jasné označení takové služby.</p> <p>Poskytovatel dále doloží odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) nebo auditní zprávu SOC 2® Type 2, s odkazem na tu část, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých budou specifické provozní údaje uloženy ve stavu neaktivních dat s označením, zda jsou nebo nejsou v daném datovém centru uloženy v pseudonymizované podobě.</p> |  |  |   |  |   |   |   |
| 1.5 | <p>Zákaznická data jsou zpracovávána na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. Aniž jsou dotčeny požadavky stanovené na řádku 1.3 přílohy č. 2 k této vyhlášce, v odůvodněných případech, po</p> | <p>1. Poskytovatel uvede u služby cloud computingu,</p> <p>a) která zpracovává zákaznická data pouze na území</p>   |  |  | X |  | X | X | X |

|  |   |   |  |  |  |  |  |  |
|--|---|---|--|--|--|--|--|--|
|  | <p>nezbytně nutnou dobu a v nezbytném rozsahu mohou být zákaznická data zpracovávána i na území jiných států, pokud poskytovatel popíše, jak budou zákaznická data chráněna před narušením bezpečnosti informací.</p> | <p>členských států Evropské unie a členských států Evropského sdružení volného obchodu:</p> <ul style="list-style-type: none"> <li>- jasné označení takové služby cloud computingu a</li> <li>- deklaraci závazku zpracování zákaznických dat na území členských států Evropské unie a členských států Evropského sdružení volného obchodu,</li> </ul> <p>b) která zpracovává zákaznický obsah pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu a která zpracovává nebo může zpracovávat zákaznická data bez zákaznického obsahu mimo území členských</p> |  |  |  |  |  |  |
|--|---|---|--|--|--|--|--|--|



|  |  |   |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|
|  |  | <p>států Evropské unie a členských států Evropského sdružení volného obchodu:</p> <ul style="list-style-type: none"><li>- jasné označení takové služby cloud computingu,</li><li>- údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat bez zákaznického obsahu, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat bez zákaznického obsahu na příslušném předpokládaném území státu, a údaj o tom, zda jsou nebo nejsou zákaznická data bez zákaznického obsahu pseudonymizována v případě tohoto</li></ul> |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|

|  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|
|  |  | <p>zpracování.<br/> U zákaznických dat bez zákaznického obsahu zpracovávaných mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu popis toho, jak budou chráněna ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů,</p> <p>c) která zpracovává nebo může zpracovávat zákaznická data mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu,</p> <p>- jasné označení takové služby cloud computingu,</p> <p>- údaje o předpokládaném</p> |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|

|  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|
|  |  | <p>území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování.</p> <p>U zákaznických dat zpracovávaných mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu popis toho, jak budou chráněna alespoň ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů.</p> |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
|  |  | <p>2. Má se za to, že předpokládanými územími států, na nichž dochází nebo může docházet ke zpracování zákaznických dat, nejsou:</p> <ul style="list-style-type: none"><li>- území států, z nichž se mohou nepravidelně vzdáleně připojovat pracovníci technické podpory poskytovatele za účelem technické podpory služby cloud computingu, která se v čase mění a nemohou být specifikována předem;</li><li>- území států, do nichž poskytovatel může předávat zákaznická data za účelem poskytování volitelné doplňkové služby se zapojením třetích stran, která není sama o sobě službou cloud computingu, aktivované podle</li></ul> |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|

|     |   |  |  |  |   |  |   |   |   |
|-----|---|--|--|--|---|--|---|---|---|
|     |   | <p>volby zákazníka, s tím, že poskytovatel jasně označí třetí stranu, jíž může předat zákaznická data, a je-li to možné, blíže specifikuje, jaká zákaznická data zpravidla předává a na jakou předpokládanou dobu zákaznická data předává.</p>   |  |  |   |  |   |   |   |
| 1.6 | <p>Specifické provozní údaje jsou zpracovávány na území členských států Evropské unie a členských států Evropského sdružení volného obchodu. Aniž jsou dotčeny požadavky stanovené na řádku 1.4 přílohy č. 2 k této vyhlášce, v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu mohou být specifické provozní údaje zpracovávány i na území jiných států, pokud poskytovatel popíše, jak budou specifické provozní údaje chráněny před narušením bezpečnosti informací.</p> | <p>1. Poskytovatel uvede u služby cloud computingu,</p> <p>a) která zpracovává specifické provozní údaje pouze na území členských států Evropské unie a členských států Evropského sdružení volného obchodu:</p> <ul style="list-style-type: none"> <li>- jasné označení takové služby cloud computingu a</li> <li>- deklaraci závazku zpracování specifických provozních údajů</li> </ul> |  |  | X |  | X | X | X |

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
|  |  | <p>na území<br/>členských států<br/>Evropské unie<br/>a členských států<br/>Evropského<br/>sdružení volného<br/>obchodu,</p> <p>b) která zpracovává<br/>nebo může<br/>zpracovávat<br/>specifické<br/>provozní údaje<br/>mimo území<br/>členských států<br/>Evropské unie<br/>a členských států<br/>Evropského<br/>sdružení volného<br/>obchodu:</p> <ul style="list-style-type: none"><li>- jasné označení<br/>takové služby<br/>cloud computingu,</li><li>- údaje<br/>o předpokládaném<br/>území státu, na<br/>němž dochází nebo<br/>může docházet ke<br/>zpracování<br/>specifických<br/>provozních údajů,<br/>a údaje<br/>o předpokládané<br/>době trvání,<br/>předpokládaném<br/>rozsahu</li></ul> |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|

|  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|
|  |  | <p>a předpokládaném účelu zpracování specifických provozních údajů na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou specifické provozní údaje pseudonymizovány v případě tohoto zpracování.</p> <p>U specifických provozních údajů zpracovávaných mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu popis toho, jak budou chráněny alespoň ve smyslu kapitoly V. obecného nařízení o ochraně osobních údajů.</p> |  |  |  |  |  |  |
|  |  | <p>2. Má se za to, že předpokládanými územími států, na nichž dochází nebo může docházet ke zpracování specifických</p>  |  |  |  |  |  |  |

|  |  |   |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|
|  |  | <p>provozních údajů,<br/>nejsou:</p> <ul style="list-style-type: none"><li>- území států,<br/>z nichž se mohou<br/>nepravidelně<br/>vzdáleně<br/>připojovat<br/>pracovníci<br/>technické podpory<br/>poskytovatele<br/>cloud computingu<br/>za účelem<br/>technické podpory<br/>služby cloud<br/>computingu, která<br/>se v čase mění<br/>a nemohou být<br/>specifikována<br/>předem;</li><li>- území států, do<br/>nichž poskytovatel<br/>může předávat<br/>specifické<br/>provozní údaje za<br/>účelem<br/>poskytování<br/>volitelné<br/>doplňkové služby<br/>se zapojením<br/>třetích stran, která<br/>není sama o sobě<br/>cloud<br/>computingem,<br/>aktivované podle<br/>volby zákazníka,<br/>s tím, že</li></ul> |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|



|     |  |  |  |  |   |  |   |   |   |
|-----|--|--|--|--|---|--|---|---|---|
|     |  | <p>poskytovatel jasně označí třetí stranu, jíž může předat specifické provozní údaje, a je-li to možné, blíže specifikuje, jaké specifické provozní údaje zpravidla předává a na jakou předpokládanou dobu specifické provozní údaje předává.</p>  |  |  |   |  |   |   |   |
| 1.7 | <p>Poskytovatel vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, který je vyjádřen v samostatném dokumentu, který obsahuje údaj o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat.</p> <p>Poskytovatel informuje zákazníka o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování.</p> | <p>Dokument oddělený od podmínek poskytování služby či smlouvy, nebo odkaz na zřetelně uvedený text smluvní dokumentace, jimiž je vyžadován souhlas zákazníka pro případy zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu, které obsahují údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat,</p> <p>nebo odkaz na konkrétní část podmínek poskytování</p> |  |  | X |  | X | X | X |

|     |   |  |  |  |  |   |   |   |   |
|-----|---|--|--|--|--|---|---|---|---|
|     | <p>Alternativně k vyžadování souhlasu a informování zákazníka poskytovatel v základním nastavení služby cloud computingu vyžaduje souhlas zákazníka pro případy zpracování zákaznických dat v každém jednotlivém případě zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu.</p>  | <p>služby nebo část návrhu smluvní dokumentace nebo produktovou specifikaci, ze které bude patrné, že poskytovatel v základním nastavení služby vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat mimo území členských států Evropské unie a členských států Evropského sdružení volného obchodu.</p>  |  |  |  |   |   |   |   |
| 1.8 | <p>Zákaznická data a specifické provozní údaje jsou zpracovávány na území České republiky. Aniž je dotčen požadavek uvedený na řádce 6.6 přílohy č. 2 k této vyhlášce, mimo území České republiky mohou být zákaznická data a specifické provozní údaje zpracovávány pouze v odůvodněných případech, po nezbytně nutnou dobu a v nezbytném rozsahu, pokud poskytovatel popíše, jak budou zákaznická data chráněna před narušením bezpečnosti informací,</p> <p>a pouze s výslovným písemným svolením zákazníka, který je vyjádřen na samostatném dokumentu, který obsahuje údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat, a údaje o předpokládané době trvání, předpokládaném rozsahu</p> | <p>Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy, ve které je závazek zpracovávat zákaznická data a specifické provozní údaje pouze na území České republiky, a dále odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) nebo auditní zprávy SOC 2® Type 2, ze které bude</p> |  |  |  | X | X | X | X |

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
|  | <p>a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování,</p> <p>nebo pouze pokud poskytovatel vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat a specifických provozních údajů mimo území České republiky.</p> | <p>patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých budou zákaznická data a specifické provozní údaje zpracovávány.</p> <p>U služby cloud computingu, která zpracovává nebo může zpracovávat zákaznická data a specifické provozní údaje mimo území České republiky, poskytovatel takovou službu jasně označí a uvede údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat a specifických provozních údajů, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat a specifických provozních údajů na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou zákaznická data a specifické provozní údaje pseudonymizovány v případě tohoto zpracování.</p> |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|

|  |  |   |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|
|  |  | <p>U služby cloud computingu, která zpracovává nebo může zpracovávat zákaznická data a specifické provozní údaje mimo území České republiky, poskytovatel doloží dokument oddělený od podmínek poskytování služby či smlouvy, nebo odkaz na zřetelně uvedený text smluvní dokumentace, jimiž je vyžadován souhlas zákazníka pro případy zpracování zákaznických dat mimo území České republiky, které obsahují údaje o předpokládaném území státu, na němž dochází nebo může docházet ke zpracování zákaznických dat, a údaje o předpokládané době trvání, předpokládaném rozsahu a předpokládaném účelu zpracování zákaznických dat na příslušném předpokládaném území státu a údaj o tom, zda jsou nebo nejsou zákaznická data pseudonymizována v případě tohoto zpracování,</p> <p>nebo odkaz na konkrétní část podmínek poskytování služby nebo část návrhu</p> |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|

|  |  |  |   |   |  |  |   |   |   |
|--|--|--|---|---|--|--|---|---|---|
|  |  | smluvní dokumentace nebo produktovou specifikaci, ze které bude patrné, že poskytovatel vyžaduje souhlas zákazníka v každém jednotlivém případě zpracování zákaznických dat mimo území České republiky.  |   |   |  |  |   |   |   |
| <b>2. Žádosti o zpřístupnění a předání dat</b> |  |  |   |   |  |  |   |   |   |
| 2.1  | Poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje, pokud to právní řád, jemuž poskytovatel podléhá, poskytovateli nezakazuje. | Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje,<br><br>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro | X | X |  |  | X | X | X |

|     |  |   |  |  |   |   |   |   |   |
|-----|--|---|--|--|---|---|---|---|---|
|     |  | <p>provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje.</p> |  |  |   |   |   |   |   |
| 2.2 | <p>Poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje. Pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat zákazníka, vyvine veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zákazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, případně pozastavit účinky zákazu, dokud soud nerozhodne ve věci samé. Pokud nedosáhne zrušení povinnosti zákazu informování</p> | <p>Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze kterého bude patrné, že poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka</p>                          |  |  | X | X | X | X | X |

|  |  |   |  |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|--|
|  | <p>zákazníka, pak poskytovatel zákazníka informuje poté, co vyprší platnost právního zákazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem.</p> | <p>bezodkladně informuje, nebo pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat zákazníka, vyvine veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zákazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, případně pozastavit účinky zákazu, dokud soud nerozhodne ve věci samé, a pokud nedosáhne zrušení povinnosti zákazu informování zákazníka, pak poskytovatel zákazníka informuje poté, co vyprší platnost právního zákazu, např. po vypršení období mlčenlivosti nařízeného zákonem nebo soudem,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF),</p> |  |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|--|

|  |  |   |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|
|  |  | <p>nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel v případě, že obdrží právně závaznou žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, nevyhoví této žádosti a odkáže tohoto žadatele na zákazníka nebo o takové žádosti zákazníka bezodkladně informuje, nebo pokud právní řád, jemuž poskytovatel podléhá, poskytovateli zakazuje informovat zákazníka, vyvine veškeré možné zákonné úsilí, aby dosáhl zrušení tohoto zákazu a využije všech dostupných opravných prostředků s cílem zpochybnit takový zákaz, případně pozastavit účinky zákazu, dokud soud nerozhodne ve věci samé, a pokud nedosáhne zrušení povinnosti zákazu informování zákazníka, pak poskytovatel zákazníka informuje poté, co vyprší platnost právního zákazu, např. po zrušení povinnosti mlčenlivosti stanovené zákonem nebo nařízené soudem</p> |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|



|     |  |  |   |   |  |  |   |   |   |
|-----|--|--|---|---|--|--|---|---|---|
| 2.3 | <p>Poskytovatel v případě, že obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, přezkoumá zákonnost takové žádosti, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti. Poskytovatel se zavazuje, že předá zákaznická data a specifické provozní údaje cizozemskému orgánu pouze, pokud z právního posouzení vyšlo, že žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti.</p> <p>O podkladech sloužících k posouzení poskytovatel provede záznam, který uchová alespoň 5 let pro účely kontroly nebo ho prokazatelně předá zákazníkovi.</p> | <p>Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze kterého bude patrné, že poskytovatel přezkoumá zákonnost cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a poskytovatel předá zákaznická data a specifické provozní údaje cizozemskému orgánu pouze, pokud z právního posouzení vyšlo, že žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních</p> | X | X |  |  | X | X | X |
|-----|--|--|---|---|--|--|---|---|---|

|  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|
|  |  | <p>údajů je přiměřený účelu žádosti,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel přezkoumá zákonnost cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a poskytovatel předá zákaznická data a specifické provozní údaje cizozemskému orgánu pouze, pokud z právního</p> |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|

|     |  |  |  |  |   |  |   |   |   |
|-----|--|--|--|--|---|--|---|---|---|
|     |  | posouzení vyšlo, že žádost cizozemského orgánu má proveditelný, aplikovatelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti.  |  |  |   |  |   |   |   |
| 2.4 | Poskytovatel v případě, že obdrží žádost cizozemského orgánu o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, přezkoumá zákonnost takové žádosti, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a vyvine veškeré možné zákonné úsilí, aby zabránil zpřístupnění nebo předání zákaznických dat a specifických provozních údajů na základě žádosti cizozemského orgánu bez souhlasu zákazníka, zejména zohlední právní závazky a povinnosti vyplývající z právních předpisů Evropské unie a České republiky a bude usilovat o zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů. | Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze kterého bude patrné, že poskytovatel přezkoumá zákonnost cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a vyvine veškeré možné zákonné úsilí, aby zabránil zpřístupnění nebo předání zákaznických dat |  |  | X |  | X | X | X |

|  |  |   |  |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|--|
|  | <p>O podkladech sloužících k posouzení poskytovatel provede záznam, který uchová alespoň 10 let pro účely kontroly nebo ho prokazatelně předá zákazníkovi.</p> | <p>a specifických provozních údajů na základě žádosti cizozemského orgánu bez souhlasu zákazníka, zejména zohlední právní závazky a povinnosti vyplývající z právních předpisů Evropské unie a České republiky a bude usilovat o zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel přezkoumá zákonnost cizozemských orgánů o zpřístupnění, zejména provede právní posouzení, ze kterého bude vyplývat, zda žádost cizozemského orgánu má</p> |  |  |  |  |  |  |  |  |
|--|--|---|--|--|--|--|--|--|--|--|

|     |  |  |   |   |   |   |   |   |   |
|-----|--|--|---|---|---|---|---|---|---|
|     |  | <p>proveditelný a platný právní základ, je právně závazná a rozsah poskytovaných nebo zpřístupňovaných zákaznických dat a specifických provozních údajů je přiměřený účelu žádosti, a vyvine veškeré možné zákonné úsilí, aby zabránil zpřístupnění nebo předání zákaznických dat a specifických provozních údajů na základě žádosti cizozemského orgánu bez souhlasu zákazníka, zejména zohlední právní závazky a povinnosti vyplývající z právních předpisů Evropské unie a České republiky a bude usilovat o zrušení povinnosti zpřístupnění nebo předání zákaznických dat a specifických provozních údajů.</p> |   |   |   |   |   |   |   |
| 2.5 | <p>Poskytovatel jasně a srozumitelně uvádí jeho povinnosti vyplývající z právních předpisů států odlišných od členských států Evropské unie, v nichž poskytovatel předpokládá zpracování zákaznických dat dle rádků 1.1, 1.5 a 1.6 přílohy č. 2 k této vyhlášce týkající se zpřístupnění a předávání zákaznických dat a specifických provozních údajů.</p> | <p>Písemný popis povinností vyplývajících z právních předpisů států odlišných od členských států Evropské unie, v nichž poskytovatel předpokládá zpracování zákaznických dat dle rádků 1.1, 1.5 a 1.6 přílohy č. 2 k této vyhlášce týkající se zpřístupnění a předávání zákaznických dat a specifických provozních</p>   | X | X | X | X | X | X | X |

|     |  |  |  |  |  |   |   |   |   |
|-----|--|--|--|--|--|---|---|---|---|
|     |  | údajů. Písemný popis musí být v takové kvalitě, aby z něj bylo možné zákazníkem posoudit vhodnost právního řádu s ohledem na zpracovávání zákaznických dat a specifických provozních údajů.  |  |  |  |   |   |   |   |
| 2.6 | Poskytovatel v případě, že obdrží žádost cizozemských orgánů o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, tuto žádost odmítne a data nevydává a nezpřístupňuje. | Čestné prohlášení nebo odkaz na část návrhu smlouvy, konkrétní část podmínek poskytování služby cloud computingu nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel v případě, že obdrží žádost cizozemských orgánů o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, tuto žádost odmítne a data nevydá a nezpřístupní,<br><br>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního |  |  |  | X | X | X | X |

|  |  |   |   |   |   |   |   |   |   |
|--|--|---|---|---|---|---|---|---|---|
|  |  | akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel v případě, že obdrží žádost cizozemských orgánů o zpřístupnění nebo předání zákaznických dat a specifických provozních údajů, tuto žádost odmítne a data nevydá a nepřístupní. |   |   |   |   |   |   |   |
| <b>3. Oprávnění k provedení kontroly</b> |  |   |   |   |   |   |   |   |   |
| 3.1                                      | Poskytovatel jednou ročně, nebo na základě opakujících se kybernetických bezpečnostních incidentů, nebo v případě rozporu vůči deklarovaným parametrům, umožňuje Ministerstvu vnitra nebo Národnímu úřadu pro kybernetickou a informační bezpečnost zdarma ve vztahu k dané službě cloud computingu provedení kontroly splnění požadavků podle § 6i odst. 2 a 3 zákona o informačních systémech veřejné správy a podle kontrolního řádu na všech místech a zařízeních, souvisejících s poskytováním služby cloud computingu, a zároveň poskytuje veškerou součinnost, kterou si tyto orgány vyžádají, vyjma zpřístupnění či předání zákaznických dat bez souhlasu dotčeného zákazníka. | Žádný podklad se nevyžaduje.<br><br>Splnění tohoto požadavku ověří Ministerstvo vnitra nebo Národní úřad pro kybernetickou a informační bezpečnost z vlastní činnosti.  | X | X | X | X | X | X | X |

#### 4. Úrovně dostupnosti služby

|     |  |  |   |           |           |           |   |   |   |
|-----|--|--|---|-----------|-----------|-----------|---|---|---|
| 4.1 | Poskytovatel je schopen zajišťovat dostupnost služby cloud computingu s nepřetržitou provozní dobou alespoň v uvedených úrovních vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno ve výměnném uzlu internetu (IXP) deklarovaném poskytovatelem. | <p>Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy, ve které bude poskytovatel garantovat zajištění dostupnosti alespoň v uvedených úrovních,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel je schopen zajišťovat dostupnost služby cloud computingu s nepřetržitou provozní dobou alespoň v uvedených úrovních vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno ve výměnném uzlu internetu</p> | - | 99,45 (%) | 99,90 (%) | 99,99 (%) | X | X | X |
|-----|--|--|---|-----------|-----------|-----------|---|---|---|



|     |   |   |           |   |   |   |   |   |   |
|-----|---|---|-----------|---|---|---|---|---|---|
|     |   | (IXP) deklarovaném poskytovatelem.  |           |   |   |   |   |   |   |
| 4.2 | Poskytovatel je schopen zajišťovat dostupnost služby cloud computingu s provozní dobou alespoň 10 hodin v pracovní dny v uvedené úrovni vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno ve výměnném uzlu internetu (IXP) deklarovaném poskytovatelem. | <p>Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy, ve které bude poskytovatel garantovat zajištění dostupnosti alespoň v uvedených úrovních,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel je schopen zajišťovat dostupnost služby cloud computingu s provozní dobou alespoň 10 hodin v pracovní dny v uvedené úrovni vyhodnocované na měsíční bázi včetně časů nutných pro servisní zásahy, měřeno ve výměnném uzlu</p> | 96,16 (%) | - | - | - | X | X | X |

|   |   |  |   |   |   |   |   |   |   |
|---|---|--|---|---|---|---|---|---|---|
|   |   | internetu (IXP) deklarovaném poskytovatelem.   |   |   |   |   |   |   |   |
| <b>5. Připojení do výměnného uzlu internetu (IXP)</b>   |   |  |   |   |   |   |   |   |   |
| 5.1   | Poskytovatel má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.  | Výpis z veřejně dostupné databáze subjektů připojených do výměnného uzlu internetu,<br><br>nebo platná smlouva s poskytovatelem služby výměnného uzlu internetu,<br><br>nebo čestné prohlášení poskytovatele, že má zajištěno připojení do výměnného uzlu internetu (IXP) v České republice.   |   |   | X | X | X | X | X |
| <b>6. Zajištění poskytování služby cloud computingu</b> |   |  |   |   |   |   |   |   |   |
| 6.1   | Poskytovatel má vyhotoven plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu pro zajištění dostupnosti uvedené v řádcích 4.1 a 4.2 přílohy č. 2 k této vyhlášce. | Strategie zajištění kontinuity provozu a strategie na obnovu po havárii,<br><br>nebo auditní zpráva vyhotovená subjektem nezávislým na poskytovateli, která potvrzuje existenci plánu zajištění kontinuity provozu nabízené služby cloud computingu a plánu na obnovu poskytování nabízené služby cloud computingu po havárii a dokládá ověření jeho aplikace, zejména auditní | X | X |   |   | X | X | X |

|     |  |  |  |  |   |   |   |   |   |
|-----|--|--|--|--|---|---|---|---|---|
|     |  | <p>zpráva vydaná pro účel certifikace ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301 nebo ISO 22301, SOC 2® Type2 nebo atestace podle CSA STAR Level 2 nebo platný certifikát ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301 nebo ISO 22301 vydaný subjektem nezávislým na poskytovateli.</p> <p>V rozsahu dané certifikace nebo auditní zprávy musí být zahrnuta nabízená služba cloud computingu.</p> <p>V případě, že rozsah auditní zprávy nebo certifikace nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, doloží poskytovatel čestné prohlášení, které služby cloud computingu do rozsahu auditní zprávy nebo certifikace spadají.</p> |  |  |   |   |   |   |   |
| 6.2 | <p>Poskytovatel má vyhotoven plán zajištění kontinuity provozu a plán na obnovu po havárii týkající se poskytované služby cloud computingu pro zajištění dostupnosti uvedené v řádcích 4.1 a 4.2 přílohy č. 2 k této vyhlášce.</p> | <p>Strategie zajištění kontinuity provozu a strategie na obnovu po havárii,</p> <p>nebo auditní zpráva vyhotovená subjektem nezávislým na poskytovateli, která potvrzuje existenci plánu</p>   |  |  | X | X | X | X | X |

|     |   |  |  |  |   |   |  |   |   |
|-----|---|--|--|--|---|---|--|---|---|
|     |   | <p>zajištění kontinuity provozu nabízené služby cloud computingu a plánu na obnovu poskytování nabízené služby cloud computingu po havárii a dokládá ověření jeho aplikace, zejména auditní zpráva vydaná pro účel certifikace ČSN ISO/IEC 20000, ISO/IEC 20000, ČSN EN ISO 22301 nebo ISO 22301, SOC 2® Type 2 nebo atestace podle CSA STAR Level 2.</p> <p>V rozsahu dané auditní zprávy musí být zahrnuta nabízená služba cloud computingu. V případě, že rozsah auditní zprávy nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, doloží poskytovatel čestné prohlášení, které služby cloud computingu do rozsahu auditní zprávy spadají.</p> |  |  |   |   |  |   |   |
| 6.3 | <p>Poskytovatel umožňuje synchronní replikaci (zálohování) dat alespoň do jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby cloud computingu poskytované z primárního datového centra.</p> | <p>Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci nebo auditní zpráva vydaná pro certifikaci ČSN EN</p>  |  |  | X | X |  | X | X |

|     |   |  |   |   |   |   |   |   |   |
|-----|---|--|---|---|---|---|---|---|---|
|     |   | ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné umožnění synchronní replikace (zálohování) dat do záložního datového centra.   |   |   |   |   |   |   |   |
| 6.4 | Poskytovatel zajišťuje, že primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo je přijato adekvátní bezpečnostní opatření, nebo se primární a alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra, nacházejí ve vzájemné vzdálenosti nejméně 50 km a u obou datových center je navržena a aplikována fyzická ochrana proti | Odkaz na konkrétní část podmínek poskytování služby nebo část návrhu smlouvy nebo produktovou specifikaci nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo z auditní zprávy SOC 2® Type 2, s odkazem na tu | X | X | X | X | X | X | X |

|  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|
|  | <p>přírodním katastrofám, úmyslnému útoku nebo haváriím.</p> | <p>část, ze které bude patrné zajištění alespoň jednoho záložního datového centra, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra,</p> <p>a</p> <p>pro doložení dostatečné vzdálenosti nebo přijetí adekvátního bezpečnostního opatření zpráva nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, které obsahuje náležitosti uvedené v příloze č. 5 k této vyhlášce,</p> <p>nebo pro doložení vzájemné vzdálenosti nejméně 50 km a návrhu a aplikace fyzické ochrany proti přírodním katastrofám, úmyslnému útoku nebo haváriím odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního</p> |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|

|     |  |   |  |  |   |   |   |   |  |
|-----|--|---|--|--|---|---|---|---|--|
|     |  | akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ze kterých je služba cloud computingu poskytována a ze které bude patrné, že fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím je navržena a aplikována.   |  |  |   |   |   |   |  |
| 6.5 | Poskytovatel zajišťuje, že primární i záložní datové centrum, ve kterých jsou uložena zákaznická data ve stavu neaktivních dat, se nacházejí buďto všechna v České republice, nebo alespoň na území dvou různých členských států Evropské unie a Evropského sdružení volného obchodu. Tento požadavek se neuplatní na služby cloud computingu uplatňující výjimku z požadavků na řádce 1.4 přílohy č. 2 k této vyhlášce. | Odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých jsou uložena zákaznická data ve stavu neaktivních dat. |  |  | X | X | X | X |  |

|     |  |  |   |   |   |   |   |   |   |
|-----|--|--|---|---|---|---|---|---|---|
| 6.6 | Poskytovatel zajišťuje, že primární i všechna záložní datová centra, ze kterých je poskytována služba cloud computingu, se nacházejí v České republice, vyjma případů výslovného písemného svolení zákazníka s ukládáním zákazníkem zašifrovaných zákaznických dat ve stavu neaktivních dat na území jiného členského státu Evropské unie a členského státu Evropského sdružení volného obchodu. | Odkaz na tu část platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávy SOC 2® Type 2, ze které bude patrný úplný výčet datových center a jejich lokace po úroveň katastrálního území/obce, ve kterých bude zákaznický obsah dlouhodobě uložen ve stavu neaktivních dat. |   |   |   | X | X | X | X |
| 6.7 | Poskytovatel je schopen poskytovat nástroje nebo služby pro zvýšení odolnosti vůči útokům typu DoS/DDoS.   | Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo na popis volitelné služby cloud computingu, ze které bude patrný nástroj nebo služba využívaná pro zvýšení odolnosti vůči útokům typu DoS/DDoS,<br><br>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro  | X | X | X | X | X | X | X |



|                            |  |   |  |  |   |   |   |   |   |
|----------------------------|--|---|--|--|---|---|---|---|---|
|                            |  | provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel je schopen poskytovat nástroje nebo služby pro zvýšení odolnosti vůči útokům typu DoS/DDoS, a ze které bude patrný nástroj nebo služba využívané pro zvýšení odolnosti vůči útokům typu DoS/DDoS. |  |  |   |   |   |   |   |
| 6.8                        | Poskytovatel umožňuje obsluhu služby cloud computingu pomocí management portálu nebo jiné formy administrátorské konzole vzdáleně přístupné zákazníkovi v nepřetržitém režimu. | Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo technickou dokumentaci, ze které bude patrné, že poskytovatel umožňuje obsluhu služby cloud computingu pomocí management portálu nebo jiné formy administrátorské konzole vzdáleně přístupné zákazníkovi v nepřetržitém režimu.  |  |  | X | X | X | X | X |
| <b>7. Nakládání s daty</b> |  |   |  |  |   |   |   |   |   |
| 7.1                        | Poskytovatel umožňuje import či export dat v objemu větším než 2 TB  | Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy, nebo   |  |  | X | X | X | X | X |

|     |  |   |   |   |   |   |   |   |   |
|-----|--|---|---|---|---|---|---|---|---|
|     | prostřednictvím zaslání šifrovaných paměťových médií.  | produktovou specifikaci, ze které bude patrné, že poskytovatel umožňuje import či export dat v objemu větším než 2 TB prostřednictvím zaslání šifrovaných paměťových médií.   |   |   |   |   |   |   |   |
| 7.2 | Poskytovatel chrání zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu. | <p>Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné, že poskytovatel chrání zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel chrání</p> | X | X | X | X | X | X | X |

|     |   |  |  |   |   |   |   |   |   |
|-----|---|--|--|---|---|---|---|---|---|
|     |   | zákaznický obsah šifrováním při přenosu a v úložištích ve službě cloud computingu.   |  |   |   |   |   |   |   |
| 7.3 | Poskytovatel umožňuje ochranu zákaznického obsahu šifrováním při přenosu a v úložištích ve službě cloud computingu pomocí některého z algoritmů uvedených v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách. | Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrný způsob šifrování při přenosu a v úložištích ve službě cloud computingu.   |  | X | X | X | X | X | X |
| 7.4 | Poskytovatel umožňuje zákazníkovi využití vlastního šifrovacího klíče (BYOK).   | Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné, že poskytovatel umožňuje zákazníkovi využití vlastních šifrovacích klíčů, a to buď jejich vygenerováním v certifikovaném hardware security modulu (dále jen "HSM modulu") umístěném u poskytovatele pod vzdálenou správou zákazníka, nebo importem těchto klíčů z jiných prostředků pod správou zákazníka. |  |   | X |   | X | X | X |
| 7.5 | Poskytovatel umožňuje uložení šifrovacích klíčů v certifikovaném  | Odkaz na konkrétní část podmínek poskytování   |  |   |   | X | X | X | X |

|     |   |   |  |  |  |   |   |   |   |
|-----|---|---|--|--|--|---|---|---|---|
|     | <p>HSM modulu úrovně ochrany FIPS 140-2 level 2 a vyšší, FIPS 140-3 level 2 a vyšší nebo certifikaci podle Common Criteria minimálně na EAL4 a vyšší, který je pod vzdálenou správou zákazníka nebo instalaci HSM modulu zákazníka do infrastruktury poskytovatele.</p> | <p>služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné, že poskytovatel umožňuje uložení klíčů v certifikovaném HSM modulu úrovně ochrany FIPS 140-2 level 2 a vyšší, FIPS 140-3 level 2 a vyšší nebo certifikaci podle Common Criteria minimálně na EAL4 a vyšší, který je pod správou zákazníka, nebo instalaci certifikovaného HSM modulu zákazníka do infrastruktury poskytovatele.</p> |  |  |  |   |   |   |   |
| 7.6 | <p>Poskytovatel umožňuje bezpečnou likvidaci kryptografických klíčů uložených v certifikovaném HSM modulu řízenou zákazníkem.</p>   | <p>Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrné umožnění bezpečné likvidace kryptografických klíčů uložených v certifikovaném HSM modulu řízené zákazníkem a závazek umožnit/zajistit při ukončení služby cloud computingu likvidaci vrchního přístupového klíče.</p>   |  |  |  | X | X | X | X |

|     |   |   |   |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|
| 7.7 | Poskytovatel umožňuje při ukončení služby cloud computingu bezpečnou likvidaci kryptografických klíčů, které šifrují zákaznický obsah v úložištích v souladu s vyhláškou o kybernetické bezpečnosti.  | Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu, ze které bude patrný popis bezpečné likvidace dat v souladu s vyhláškou o kybernetické bezpečnosti.   |   |   | X |   | X | X | X |
| 7.8 | Poskytovatel vyhotovuje záznam o přístupu jeho interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo bez přechozího svolení zákazníka v daném případě. Tento záznam musí obsahovat alespoň důvod, čas, trvání, typ a rozsah přístupu a dostatek dalších údajů potřebných k tomu, aby mohl zákazník vyhodnotit rizikovost tohoto přístupu. | Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu,<br><br>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel vyhotovuje záznam o přístupu jeho | X | X | X | X | X | X | X |

|     |   |   |   |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|
|     |   | interních a externích pracovníků k nezašifrovaným zákaznickým datům, ke kterému došlo bez přechozího svolení zákazníka v daném případě, a že tento záznam obsahuje důvod, čas, trvání, typ a rozsah přístupu.   |   |   |   |   |   |   |   |
| 7.9 | <p>Poskytovatel umožňuje zákazníkovi přístup k záznamu vytvořenému dle řádku 7.8 přílohy č. 2 k této vyhlášce, a za tím účelem ho poskytovatel uchová alespoň po dobu 7 dní.</p> <p>Poskytovatel nemusí umožňovat přístup k záznamu v případě, že interní a externí pracovníci přistupují k nezašifrovanému zákaznickému obsahu na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat a vyrozumění zákazníka o této žádosti není možné v souladu s body 2.1, 2.2 přílohy č. 2 této vyhlášky.</p> | <p>Odkaz na konkrétní část podmínek poskytování služby cloud computingu nebo část návrhu smlouvy nebo produktovou specifikaci služby cloud computingu,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel umožňuje zákazníkovi přístup k záznamu vytvořenému dle</p> | X | X | X | X | X | X | X |

|   |   |   |   |   |  |  |   |   |   |
|---|---|---|---|---|--|--|---|---|---|
|   |   | řádku 7.8 přílohy č. 2 k této vyhlášce, a že takový záznam uchová alespoň po dobu 7 dní.  |   |   |  |  |   |   |   |
| <b>8. Certifikace služby cloud computingu</b> |   |   |   |   |  |  |   |   |   |
| 8.1   | Poskytovatel provozuje službu cloud computingu v rozsahu systému řízení bezpečnosti informací, který je v souladu s požadavky vyhlášky o kybernetické bezpečnosti nebo s požadavky ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001.   | Čestné prohlášení, že systém řízení bezpečnosti informací, v jehož rozsahu je služba cloud computingu provozována, je v souladu s požadavky vyhlášky o kybernetické bezpečnosti nebo s požadavky ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 a prohlášení o aplikovatelnosti jednotlivých opatření.   | X |   |  |  | X | X | X |
| 8.2   | Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu. | Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, |   | X |  |  | X | X | X |

|     |   |   |  |  |   |   |   |   |   |
|-----|---|---|--|--|---|---|---|---|---|
|     |   | nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven.  |  |  |   |   |   |   |   |
| 8.3 | Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu. | Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu,<br><br>nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do |  |  | X | X | X | X | X |



|     |  |   |  |   |  |  |   |   |   |
|-----|--|---|--|---|--|--|---|---|---|
|     |  | katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro něž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.   |  |   |  |  |   |   |   |
| 8.4 | Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017. | Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017,<br><br>nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do |  | X |  |  | X | X | X |

|     |  |  |  |  |   |   |   |   |   |
|-----|--|--|--|--|---|---|---|---|---|
|     |  | katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti informací, pro něž byl daný certifikát vystaven.  |  |  |   |   |   |   |   |
| 8.5 | Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN EN ISO/IEC 27017 nebo EN ISO/IEC 27017. | Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017, nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu |  |  | X | X | X | X | X |

|     |   |  |  |  |   |   |   |   |   |
|-----|---|--|--|--|---|---|---|---|---|
|     |   | <p>systemu řízení bezpečnosti informací, pro nějž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.</p>  |  |  |   |   |   |   |   |
| 8.6 | <p>Poskytovatel je držitelem platné certifikace ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), do jejíhož rozsahu certifikace náleží posuzovaná služba cloud computingu provozovaná v souladu s postupy normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018.</p> | <p>Platný certifikát ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF) s označením poskytovatele, kdy rozsah certifikace jmenovitě zahrnuje službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu a provozovanou v souladu s postupy normy ČSN ISO/IEC 27018 nebo ISO/IEC 27018,</p> <p>nebo v případě, že rozsah certifikace uvedený na certifikátu nezahrnuje jmenovitě službu cloud computingu, kterou žádá poskytovatel zapsat do katalogu cloud computingu, čestné prohlášení, které služby spadají do rozsahu systému řízení bezpečnosti</p> |  |  | X | X | X | X | X |

|  |  |   |   |  |   |   |   |   |   |
|--|--|---|---|--|---|---|---|---|---|
|  |  | informací, pro něž byl daný certifikát vystaven, a dále příslušné prohlášení o aplikovatelnosti.  |   |  |   |   |   |   |   |
| 8.7  | Poskytovatel je držitelem auditní zprávy SOC 2® Type 2 nebo auditní zprávy o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue C5 vydaný BSI, a to ve formě Type 2, která není starší než 24 měsíců, do jejíhož rozsahu náleží posuzovaná služba cloud computingu, vydaná nezávislým auditorem. | Auditní zpráva SOC 2® Type 2 v doménách bezpečnosti, dostupnosti, procesní integrity, důvěrnosti a soukromí nebo auditní zpráva o vyhodnocení shody s aktuálními požadavky Cloud Computing Compliance Criteria Catalogue (C5) vydaný BSI, a to ve formě Type 2.   |   |  | X | X | X | X | X |
| <b>9. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty</b> |  |   |   |  |   |   |   |   |   |
| 9.1  | Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.   | Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí, nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro | X |  |   |   | X | X | X |

|     |  |  |  |   |   |   |   |   |   |
|-----|--|--|--|---|---|---|---|---|---|
|     |  | <p>provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.</p>   |  |   |   |   |   |   |   |
| 9.2 | <p>Poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí. Poskytovatel umožní zpřístupnění vzdáleně všech událostí týkajících se konkrétního zákazníka zákazníkovi. Nové události zpřístupní zákazníkovi bez zbytečného odkladu po vzniku události, nejpozději však do 24 hodin.</p> | <p>Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo jiný popis služby cloud computingu, ze kterých bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí a umožní zpřístupnění vzdáleně všech událostí týkajících se konkrétního zákazníka zákazníkovi a nové události zpřístupní zákazníkovi bez zbytečného odkladu, nejpozději však do 24 hodin po vzniku události,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN</p> |  | X | X | X | X | X | X |

|     |   |   |   |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|---|
|     |   | ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zpráva SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že poskytovatel má zaveden nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí, umožní zpřístupnění vzdáleně všech událostí týkajících se konkrétního zákazníka zákazníkovi a nové události zpřístupní zákazníkovi bez zbytečného odkladu po vzniku události, nejpozději však do 24 hodin. |   |   |   |   |   |   |   |
| 9.3 | Poskytovatel informuje zákazníka v případě narušení bezpečnosti informací zákaznických dat a specifických provozních údajů bez zbytečného odkladu, ale nejpozději do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat dozvěděl. Jakmile je řešení incidentu uzavřeno, informuje | Odkaz na konkrétní část podmínek poskytování služby cloud computingu, část návrhu smlouvy nebo jiný popis služby cloud computingu, ze které bude patrné, že poskytovatel informuje zákazníka v případě narušení bezpečnosti informací   | X | X | X | X | X | X | X |

|  |  |  |   |   |   |   |   |   |   |
|--|--|--|---|---|---|---|---|---|---|
|  | poskytovatel zákazníka o přijatých opatřeních.   | zákaznických dat a specifických provozních údajů bez zbytečného odkladu, ale nejpozději do 72 hodin od okamžiku, kdy se o narušení bezpečnosti zákaznických dat dozvěděl.  |   |   |   |   |   |   |   |
| <b>10. Testování služby cloud computingu</b> |  |  |   |   |   |   |   |   |   |
| 10.1   | Poskytovatel provádí pravidelně skeny zranitelností. Služba cloud computingu zapisovaná do katalogu cloud computingu musí být zahrnuta do rozsahu skenu zranitelností. | <p>Tři záznamy o provedení skenů zranitelností provedených maximálně 3 měsíce před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu,</p> <p>nebo auditní zpráva vydaná pro certifikaci ČSN EN ISO/IEC 27001, EN ISO/IEC 27001 nebo ISO/IEC 27001 od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů Mezinárodního akreditačního fóra (IAF), nebo auditní zprávu SOC 2® Type 2, s odkazem na tu část, ze které bude patrné, že skeny zranitelností jsou prováděny pravidelně v takovém intervalu, ze kterého bude vyplývat, že byly provedeny alespoň 3</p> | X | X | X | X | X | X | X |

|      |  |   |  |  |   |   |   |   |   |
|------|--|---|--|--|---|---|---|---|---|
|      |  | skeny zranitelnosti maximálně 3 měsíce před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu.   |  |  |   |   |   |   |   |
| 10.2 | Poskytovatel zajišťuje provádění penetračních testů subjektem, který je nezávislý na poskytovateli. Služba cloud computingu zapisovaná do katalogu cloud computingu musí být zahrnuta do rozsahu penetračního testu. | Zpráva z provedení penetračního testu provedeného podle standardu NIST 800-115 nebo v souladu s metodikou OSSTMM. Penetrační test provede subjekt, který je nezávislý na poskytovateli. Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu.                           |  |  | X | X | X | X |   |
| 10.3 | Poskytovatel zajišťuje provádění penetračních testů subjektem, který je nezávislý na poskytovateli. Služba cloud computingu zapisovaná do katalogu cloud computingu musí být zahrnuta do rozsahu penetračního testu. | Zpráva z provedení penetračního testu, při kterém budou ověřena rizika alespoň podle standardu OWASP Top 10 Web Application Security Risks. Penetrační test provede subjekt, který je nezávislý na poskytovateli. Zpráva z provedení penetračního testu nesmí být starší než 24 měsíců před podáním žádosti o zápis služby cloud computingu do katalogu cloud computingu. |  |  | X | X |   |   | X |