



Smlouva o poskytování služeb dynamického školení kybernetické bezpečnosti a simulace phishingových útoků

číslo 2025/15061

Česká pošta, s.p.

se sídlem: Politických vězňů 909/4, 225 99 Praha 1
IČO: 47114983
DIČ: CZ47114983
zastoupen: Ing. Martinem Götzem, ředitelem úseku ICT
zapsán v obchodním rejstříku u: Městského soudu v Praze, oddíl A, vložka 7565
bankovní spojení: 

dále jen „**Objednatel**“

a

DATACONS s.r.o.

se sídlem: Na Lysinách 92/8, 147 00 Praha 4 - Hodkovičky
IČO: 29018765
DIČ: CZ29018765
zastoupena: Ing. Čestmírem Pailem, jednatelem
zapsána v obchodním rejstříku u: Městského soudu v Praze, oddíl C, vložka 160327
bankovní spojení: 

dále jako „**Dodavatel**“

dále jednotlivě jako „**Smluvní strana**“ a společně jako „**Smluvní strany**“ uzavírají v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“), tuto Smlouvu o poskytování služeb (dále jen „**Smlouva**“).

Preamble

Objednatel provedl dle interních předpisů výběrové řízení k veřejné zakázce „Dynamické školení kybernetické bezpečnosti a simulace phishingových útoků“ (dále jen „**Výběrové řízení**“) na uzavření této Smlouvy. Tato Smlouva je uzavírána s Dodavatelem na základě výsledku Výběrového řízení. Objednatel tímto ve smyslu ust. § 1740 odst. 3 Občanského zákoníku předem vylučuje přijetí nabídky na uzavření této Smlouvy s dodatkem nebo odchylkou.

1 Účel a předmět Smlouvy

1.1 Účelem této Smlouvy je úprava práv a povinností při poskytování služeb mezi Dodavatelem a Objednatelem. Služby mají být Objednatelem použity pro zajištění dynamického školení kybernetické bezpečnosti a simulace phishingových útoků a pro rozvoj bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí zaměstnanců Objednatele.

1.2 Předmětem této Smlouvy je:

- a) služba, či služby poskytované Dodavatelem způsobem a v souladu se specifikací uvedenou v Příloze č. 1 této Smlouvy (dále jen „**Plnění**“).
- b) další doplňkové služby související s Plněním, které si Objednatel vyhrazuje právo doobjednat, a které mohou obsahovat zejména integraci služeb nabízených Dodavatelem do systému Objednatele (dále jen „**Doplňkové služby**“), a to na základě objednávky uvedené v odst. 1.3 této Smlouvy (dále jen „**Objednávka**“). Tyto Doplňkové služby budou účtovány na základě tzv. Men's day (dále jen „**MD**“), přičemž jejich maximální rozsah za celou dobu trvání Smlouvy činí 20 MD. Doplňkové služby budou poskytovány v termínu/čase uvedeném v Objednávce. K převzetí Doplňkové služby dojde podpisem akceptačního protokolu Objednatelem po úspěšné provedené akceptaci. Doplňková služba je však dokončena až odstraněním všech vad zjištěných při akceptaci a uvedených v akceptačním protokolu s výrokem „akceptováno“ včetně uvedení počtu MD. Dodavatel je v rámci akceptačního řízení povinen odstranit zjištěné vady Doplňkové služby nejpozději do pěti (5) pracovních dnů následujících od jejího písemného nahlášení Objednatelem, pokud se Smluvní strany nedohodnou jinak. V případě že Dodavatel ukončí akceptační řízení s výrokem „neakceptováno“ v akceptačním protokolu, je Dodavatel nadále povinen pracovat na řádném odstranění zjištěných vad, přičemž je povinen po jejich odstranění bez zbytečného odkladu vyzvat Objednatele k opakování akceptace. Dojde-li v průběhu akceptace k zjištění neodstranitelné vady, bude to ze strany Objednatele považováno za podstatné porušení této Smlouvy.

Dodavatel odpovídá za provedení Plnění a Doplňkových služeb v souladu s relevantními právními předpisy, technickými normami, a to výlučně osobami, které v době provedení Plnění a Doplňkových služeb disponují příslušnými oprávněními, jsou-li taková právními předpisy vyžadována.

1.3 Dodavatel se zavazuje poskytnout Objednateli Doplňkové služby na základě Objednávky doručené Objednatelem Dodavateli. Objednávka musí obsahovat minimálně tyto náležitosti:

- a) identifikační údaje Objednatele a Dodavatele;
- b) číslo a datum vystavení Objednávky;
- c) číslo Smlouvy;
- d) popis Doplňkové služby;
- e) počet MD;
- f) dobu a místo poskytnutí Doplňkové služby; a
- g) podpis oprávněné osoby Dodavatele.

Dodavatel je povinen písemně potvrdit Objednávku ve lhůtě dvou (2) pracovních dnů od jejího doručení Objednatelem.

Potvrzení Objednávky musí obsahovat minimálně tyto náležitosti:

- a) identifikační údaje Objednatele a Dodavatele;
- b) číslo Objednávky, která je potvrzována; a
- c) podpis oprávněné osoby Dodavatele.



V případě, že Objednávka nebude splňovat uvedené minimální náležitosti, má Dodavatel povinnost na tuto skutečnost neprodleně upozornit Objednatele. Objednatel je poté povinen vystavit novou Objednávku a Dodavatel je povinen ji ve lhůtě dvou (2) pracovních dnů od jejího doručení písemně potvrdit.

Potvrzení Objednávky, které obsahuje dodatky, výhrady, omezení nebo jiné změny se považuje za odmítnutí Objednávky.

- 1.4 Dodavatel se zavazuje poskytnout Objednateli Plnění za podmínek uvedených v této Smlouvě ve sjednaném rozsahu, jakosti a čase.
- 1.5 Objednatel se zavazuje zaplatit za Plnění poskytnuté v souladu s touto Smlouvou Cenu dle odst. 2 této Smlouvy.
- 1.6 Po uzavření Smlouvy sdělí Objednatel Dodavateli tzv. číslo evidenční objednávky (OBJ) pro Plnění dle odst. 1.2 písm. a) této Smlouvy. Toto číslo má pouze evidenční charakter pro Objednatele a nemá žádný vliv na plnění Smlouvy. Oproti tomu k poskytování Doplnkových služeb dle odst. 1.2 písm. b) Smlouvy vyzve Objednatel Dodavatele prostřednictvím objednávky uskutečněné dle odst. 1.3 této Smlouvy. Objednatel však není povinen takovou Objednávku za dobu trvání této Smlouvy učinit.
- 1.7 Objednatel je oprávněn nejdříve po uplynutí jednoho (1) roku ode dne účinnosti této Smlouvy Smlouvu vypovědět, a to i bez udání důvodu. Výpovědní doba činí 1 měsíc od doručení výpovědi Dodavateli.

2 Cena

- 2.1 Cena za 1 rok poskytování Plnění specifikované v Příloze č. 1 Smlouvy činí 899 999,- Kč bez DPH (dále jen „**Cena**“). Cena za 1 MD za Doplnkové služby činí 11 900,- Kč bez DPH.
- 2.2 Cena za Plnění a zároveň cena za 1 MD v sobě zahrnuje veškeré náklady Dodavatele spojené s plněním Smlouvy a poskytnutím Plnění a Doplnkových služeb Objednateli. Cena je cenou konečnou, nejvýše přípustnou a nemůže být zvýšena bez předchozího písemného souhlasu Objednatele.

3 Platební podmínky

- 3.1 Dodavatel vystaví ke dni nabytí účinnosti této Smlouvy na Cenu za první rok trvání této Smlouvy daňový doklad. Za den uskutečnění zdanitelného plnění se považuje den vystavení daňového dokladu, tj. den nabytí účinnosti Smlouvy.
- 3.2 Dodavatel vystaví daňový doklad na Cenu za druhý rok trvání této Smlouvy po uplynutí předchozího období. Za den uskutečnění zdanitelného plnění se považuje den vystavení daňového dokladu, tj. první den období, za které je Cena fakturována.
- 3.3 Splatnost daňových dokladů týkajících se Plnění stejně jako Doplnkových služeb je:
 - a) 30 kalendářních dnů ode dne jeho vystavení Dodavatelem, je-li cena nižší než 300 000,- Kč bez DPH;
 - b) 60 kalendářních dnů ode dne jeho vystavení Dodavatelem, je-li cena vyšší nebo rovna 300 000,- Kč bez DPH.
- 3.4 Objednatel neposkytuje Dodavateli jakékoliv zálohy na Cenu.
- 3.5 Dodavatel zašle daňové doklady spolu s veškerými požadovanými dokumenty Objednateli postupem dle odst. 2.6 Všeobecných obchodních podmínek Objednatele (dále jen „**VOP**“).



Nedílnou součástí daňového dokladu týkajícího se Doplnkových služeb je akceptační protokol s výrokem „akceptováno“.

4 Pojištění

- 4.1 Dodavatel je povinen po celou dobu trvání Smlouvy a Dílčí smlouvy mít sjednáno pojištění odpovědnosti za újmy způsobené v souvislosti se Smlouvou a Dílčí smlouvou Dodavatelem nebo osobou, za niž Dodavatel odpovídá, s pojistnou částkou nejméně ve výši 4 000 000,- Kč.

5 Sankce

- 5.1 V případě nedostupnosti Plnění po dobu delší než 168 hodin je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 10 000 Kč za každých 72 hodin po překročení výše uvedené doby 168 hodin.

6 Zpracování osobních údajů

- 6.1 Dodavatel a Objednatel postupují při zpracování osobních údajů dle čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**GDPR**“).
- 6.2 Dodavatel je v poskytování Plnění (pro účely tohoto článku se rozumí Plněním rovněž Doplnkové plnění) dle této Smlouvy zpracovatelem osobních údajů. Objednatel je ve vztahu k těmto osobním údajům správcem. Plnění zahrnuje činnosti, při kterých dochází ke zpracování osobních údajů Dodavatelem pro Objednatele. Objednatel tímto výslovně pověřuje Dodavatele zpracováním osobních údajů, které mu v rámci Plnění předá, a to ve Smlouvě stanoveném rozsahu, za účelem stanoveným ve Smlouvě a na dobu ve Smlouvě stanovenou. Osobní údaje jsou důvěrnými informacemi ve smyslu VOP, které jsou Přílohou č. 2 této Smlouvy.
- 6.3 Dodavatel bude za účelem poskytování Služeb zpracovávat osobní údaje subjektů údajů – zaměstnanců Objednatele (dále též jen „**Subjekt údajů**“ nebo „**Subjekty údajů**“), a to zejména v rozsahu:
1. jméno a příjmení;
 2. e-mail
 3. zařazení do organizační struktury Objednatele (např. oddělení, pracovní pozice)
 4. osobní číslo, pod kterým je Subjekt údajů veden u Objednatele
 5. typ uživatele pro účely výběru školení (běžný uživatel typu 10, běžný uživatel typu 20, administrátor, management ...)
- 6.4 Dodavatel bude osobní údaje zpracovávat zejména shromažďováním, ukládáním a použitím, a to automatizovaným i neautomatizovaným způsobem, v elektronické i listinné podobě. Smluvní strany si budou předávat osobní údaje bezpečným a kontrolovaným způsobem stanoveným touto Smlouvou.
- 6.5 Nebude-li ze strany Objednatele určeno jinak, bude informační povinnost dle GDPR ve vztahu k Subjektům údajů plněna Objednatelem.
- 6.6 Dodavatel zpracovává osobní údaje pouze na základě písemných pokynů Objednatele, včetně případného předání osobních údajů třetím subjektům, pokud mu toto zpracování již neukládají obecně závazné právní předpisy, které se na Dodavatele vztahují; v takovém případě Dodavatel



Objednatel o takovém právním požadavku informuje ještě před samotným zpracováním, ledaže by obecně závazné právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu. Dodavatel Objednatel neprodleně informuje v případě, že podle jeho názoru určitý pokyn porušuje GDPR nebo jiné obecně závazné předpisy týkající se ochrany údajů. Dodavatel zohledňuje povahu zpracování osobních údajů a jeho případné dopady do soukromí Subjektů údajů, čemuž přizpůsobuje zabezpečení zpracování.

- 6.7 Osobní údaje si budou Smluvní strany - v případě potřeby jejich předání - předávat v zabezpečené podobě. V případě zasílání osobních údajů prostřednictvím e-mailu musí být osobní údaje chráněny heslem, které si kontaktní osoby Smluvních stran vymění jiným kanálem (telefonicky, na ústním jednání apod.), popřípadě se Smluvní strany dohodnou na jiném způsobu zabezpečené komunikace.
- 6.8 Jakákoliv třetí osoba (vyjma zaměstnanců Dodavatele), která jedná z pověření Dodavatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na základě pokynu Objednatel, ledaže jí zpracování osobních údajů ukládají obecně závazné právní předpisy. Dodavatel přijme opatření pro zajištění tohoto požadavku a zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nevztahuje-li se na ně zákonná povinnost mlčenlivosti.
- 6.9 Dodavatel odpovídá za své zaměstnance, kteří v rámci plnění stanovených oprávnění a povinností přicházejí do styku s osobními údaji a jsou povinni v souladu s obecně závaznými právními předpisy zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací. Dodavatel je povinen dohlížet na plnění uvedených povinností ze strany svých zaměstnanců.
- 6.10 Pokud to dovolují obecně závazné právní předpisy, je Dodavatel oprávněn pověřit zpracováním dalšího zpracovatele, pouze však jen s předchozím písemným souhlasem Objednatel; udělený souhlas je Objednatel oprávněn kdykoli odvolat. Pokud Dodavatel zapojí dalšího zpracovatele, aby jménem Objednatel provedl určité činnosti zpracování osobních údajů, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu stejné povinnosti na ochranu osobních údajů, jaké jsou dohodnuty mezi Objednatel a Dodavatel; jedná se zejména o poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování osobních údajů splňovalo požadavky obecně závazných právních předpisů a pravidla a podmínky nakládání s osobními údaji, které se Smluvní strany zavázaly dodržovat. Splnění povinností stanovených v tomto odstavci je Dodavatel povinen Objednateli na jeho výzvu kdykoliv prokázat.
- 6.11 S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování osobních údajů i k různě pravděpodobným a různě závažným rizikům pro práva a svobody Subjektů údajů (fyzických osob) zavede Dodavatel vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, zejména přijme veškerá opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení, ztrátě, zneužití či jinému neoprávněnému zpracování. Dodavatel je povinen zavést alespoň následující bezpečnostní opatření:
 - a) přístup k osobním údajům zachyceným v jakékoli podobě mají pouze oprávněné osoby;
 - b) osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů mají přístup pouze k osobním údajům odpovídajícím jejich oprávnění (zvláštní uživatelská oprávnění);
 - c) dostatečná informovanost oprávněných osob o pravidlech ochrany osobních údajů;

- d) při předávání dokumentů obsahujících osobní údaje musí být tyto dokumenty dostatečně zabezpečeny proti jejich zcizení;
- e) pořizování záznamů pro ověření kdy, kým a z jakého důvodu byly osobní údaje zaznamenány či jinak zpracovány;
- f) stanovení a dodržování postupů na ochranu osobních údajů;
- g) schopnost včas odhalit příp. porušení ochrany osobních údajů;
- h) zajištění dostupnosti a integrity informací;
- i) uzavírání smluv o zpracování osobních údajů s třetími osobami;
- j) pravidelný monitoring a kontrola procesů zpracování osobních údajů;
- k) ochrana před škodlivým programovým vybavením;
- l) existence systému hlášení a vyšetřování mimořádných událostí prolomení bezpečnosti.

Dodavatel je povinen uvedená opatření zajistit vhodným způsobem při realizaci zpracování osobních údajů dle této Smlouvy.

- 6.12 Smluvní strany se zavazují vzájemně si neprodleně ohlašovat všechny jim známé skutečnosti, které by mohly nepříznivě ovlivnit řádné a včasné plnění závazků vyplývajících z tohoto článku Smlouvy a poskytovat si součinnost nezbytnou pro plnění tohoto článku Smlouvy a pro legitimní a legální zpracování osobních údajů.
- 6.13 Dojde-li z jakéhokoli důvodu (např. z důvodu legislativních změn, rozhodnutí státního orgánu atp.) k nutnosti změny dohodnutých pravidel při plnění tohoto článku Smlouvy, zavazují se Smluvní strany neprodleně se o této skutečnosti informovat. Smluvní strany jsou povinny v takovém případě zahájit jednání o změně této Smlouvy a uzavřít dodatek, který předmětné změny bude zohledňovat.
- 6.14 Dodavatel se zavazuje Objednateli poskytnout součinnost při zajišťování souladu s povinnostmi k zabezpečení osobních údajů, ohlašování případů porušení zabezpečení, jak je uvedeno níže, zpracování posouzení vlivu na ochranu osobních údajů, plnění informační povinnosti, výkonu práv Subjektů údajů a případně též konzultacím s dozorovým úřadem či vyřizování žádostí o výkon práva Subjektů údajů, a to vše při zohlednění povahy zpracování a informací, jež má Dodavatel k dispozici.
- 6.15 Dodavatel je povinen informovat Objednatele o každém případě ztráty či úniku osobních údajů, neoprávněné manipulace s osobními údaji nebo jiného porušení zabezpečení osobních údajů (dále jen „**Porušení zabezpečení osobních údajů**“), a to bez zbytečného odkladu, nejpozději do dvaceti čtyř (24) hodin od vzniku Porušení zabezpečení osobních údajů nebo i pouhé hrozby, jestliže Dodavatel mohl o tomto Porušení zabezpečení osobních údajů či i o hrozbě vzniku Porušení zabezpečení osobních údajů vědět při vynaložení veškeré odborné péče. Nemohl-li Dodavatel zjistit případ skutečného či hrozícího Porušení zabezpečení osobních údajů před uplynutím lhůty dle předchozí věty tohoto odstavce, informuje Dodavatel Objednatele nejpozději do dvaceti čtyř (24) hodin od okamžiku, kdy se o vzniku Porušení zabezpečení osobních údajů nebo jeho hrozbě Dodavatel dozví. Dodavatel je i po poskytnutí informace Objednateli povinen být maximálně nápomocen při řešení Porušení zabezpečení osobních údajů, resp. při přijímání opatření ke zmírnění možných nepříznivých dopadů a zabránění vzniku obdobných situací v budoucnu. Informace dle tohoto odstavce Smlouvy musí přinejmenším obsahovat:
- a) odkaz na tuto Smlouvu;



- b) popis povahy daného případu Porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených Subjektů údajů a kategorií a přibližného počtu dotčených záznamů osobních údajů;
- c) popis pravděpodobných důsledků Porušení zabezpečení osobních údajů a
- d) popis opatření, která Dodavatel přijal nebo navrhuje přijmout s cílem vyřešit dané Porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Není-li možné poskytnout informace podle písm. a) – d) současně, mohou být poskytnuty Dodavatelem postupně bez dalšího zbytečného odkladu. Veškeré informace dle tohoto odstavce Smlouvy bude Dodavatel Objednateli zasílat e-mailem na adresu [REDACTED]

- 6.16 Dodavatel se zavazuje bez zbytečného odkladu informovat Objednatele o tom, že ve vztahu k němu bylo ze strany dozorového úřadu zahájeno šetření či řízení související se zpracováním osobních údajů dle této Smlouvy, o průběhu takového šetření či řízení a o výsledku takového šetření či řízení. Dodavatel na výzvu Objednatele též Objednateli zpřístupní veškeré dokumenty, které budou součástí spisu vedeného k předmětnému šetření či řízení.
- 6.17 Dodavatel poskytne Objednateli veškeré informace potřebné k doložení toho, že byly splněny jeho povinnosti, a umožní audity včetně inspekci, prováděné Objednatelem nebo jiným auditorem, kterého Objednatel pověřil, a k těmto auditům, je-li to nezbytné pro řádný výkon auditu, přispěje. Audit je Objednatel oprávněn provádět u Dodavatele, resp. na jakémkoli jiném místě, kde dochází ke zpracování osobních údajů. Audit je Objednatel povinen oznámit Dodavateli minimálně s předstihem pěti (5) pracovních dnů. V průběhu auditu má Objednatel přístup k interním předpisům a systémům vztahujícím se ke zpracování osobních údajů podle této Smlouvy. Objednatel se zavazuje, že ve vztahu k informacím, se kterými se v průběhu auditu či inspekce seznámí, zachová mlčenlivost. Náklady na provedení auditu či inspekce si nese každá Smluvní strana samostatně.
- 6.18 Dodavatel bude osobní údaje zpracovávat pouze po dobu nezbytně nutnou, minimálně po dobu plnění této Smlouvy. Nejpozději do patnácti (15) kalendářních dní po ukončení účinnosti Smlouvy je Dodavatel povinen ukončit veškeré zpracovávání osobních údajů Subjektů údajů. Dodavatel v souladu s rozhodnutím Objednatele všechny osobní údaje buď vymaže či jinak technicky odstraní, nebo je vrátí Objednateli a vymaže existující kopie, pokud obecně závazně právní předpisy nepožadují uložení (archivaci) daných osobních údajů po dobu delší nebo jejich uložení není nezbytné k ochraně práv a oprávněných zájmů Dodavatele.
- 6.19 Dodavatel se zavazuje, že nebude osobní údaje zpracovávané na základě této Smlouvy využívat k jiným účelům než k účelům stanoveným touto Smlouvou.
- 6.20 Dodavatel se zavazuje, že nebude sdružovat osobní údaje zpracovávané na základě této Smlouvy s jakýmkoli dalšími osobními údaji, získanými nebo zpracovávanými pro jiný účel.
- 6.21 Po ukončení této Smlouvy nezanikají povinnosti Dodavatele k zabezpečení a ochraně osobních údajů, povinnost mlčenlivosti ani povinnosti vztahující se k ukončení činnosti Dodavatele, jakož i nároky Objednatele z důvodu porušení takových povinností.
- 6.22 V případě, že v důsledku porušení některé povinnosti Dodavatele dle tohoto článku Smlouvy či v důsledku jednání dalšího zpracovatele vznikne Objednateli povinnost na základě rozhodnutí či výzvy orgánu veřejné moci zaplatit peněžitou částku jako pokutu, sankci, penále, náhradu či jinou platbu obdobného charakteru (dále jen „Sankce“), zavazuje se Dodavatel uhradit Sankci namísto Objednatele, a to nejpozději do pěti (5) pracovních dnů od doručení výzvy k zaplacení. Pokud Objednatel Sankci uhradí sám, zavazuje se Dodavatel uhradit Sankci Objednateli do pěti (5) pracovních dnů od doručení výzvy k zaplacení.



- 6.23 Smluvní strany jako správci zpracovávají osobní údaje kontaktních zástupců Smluvních stran a dalších osob podílejících se na plnění této Smlouvy, a to výhradně pro účely související s plněním této Smlouvy, v nezbytně nutném rozsahu a po dobu trvání Smlouvy. Smluvní strany mohou dále osobní údaje zpracovávat pro účely vyplývající z obecně závazných právních předpisů či za účelem ochrany svých právních nároků, a to po dobu z těchto právních předpisů vyplývajících, resp. po dobu nezbytně nutnou. Informační povinnost ve vztahu k těmto osobám plní každá ze Smluvních stran samostatně.
- 6.24 Pro vyloučení pochybností se stanoví, že dojde-li ze strany Dodavatele k porušení jakékoliv povinnosti uvedené v tomto článku Smlouvy, je Dodavatel povinen zaplatit Objednateli smluvní pokutu stanovenou v odst. 11.1 písm. d) VOP.
- 6.25 Bude-li třeba, upraví Smluvní strany zpracování osobních údajů v příslušné Dílčí smlouvě.

7 Závěrečná ustanovení

- 7.1 Tato Smlouva nabývá platnosti dnem jejího podpisu Smluvními stranami a účinnosti dnem uveřejnění v registru smluv podle zákona o registru smluv, nejdříve však prvního dne, následujícího měsíce po nabytí účinnosti Smlouvy. Smlouva je podepsána připojením kvalifikovaného elektronického podpisu nebo zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, včetně kvalifikovaného časového razítka. Plnění předmětu této Smlouvy před nabytím její účinnosti se považuje za plnění podle této Smlouvy a práva a povinnosti z něj vzniklé se řídí touto Smlouvou.
- 7.2 Smlouva se uzavírá na dobu určitou v trvání 36 měsíců od data účinnosti Smlouvy. Pro případ, že tato Smlouva není uzavírána za přítomnosti obou Smluvních stran, platí, že Smlouva nebude uzavřena, pokud ji Dodavatel podepíše s jakoukoliv změnou či odchylkou, byť nepodstatnou, nebo dodatkem. To platí i v případě připojení obchodních podmínek Dodavatele, které budou odporovat svým obsahem jakýmkoliv způsobem textu této Smlouvy, případně VOP Objednatele.
- 7.3 Smluvní strany výslovně potvrzují, že si vzájemně sdělily veškeré okolnosti důležité pro uzavření Smlouvy. Smluvní strany prohlašují, že se dohodly o veškerých náležitostech Smlouvy.
- 7.4 Smluvní strany potvrzují, že si při uzavírání Smlouvy vzájemně sdělily všechny skutkové a právní okolnosti, o nichž ví nebo vědět musí, tak, aby se každá ze Smluvních stran mohla přesvědčit o možnosti uzavřít platnou Smlouvu a aby byl každé ze Smluvních stran zřejmý zájem druhé Smluvní strany Smlouvu uzavřít.
- 7.5 Tato Smlouva je vyhotovena v elektronické podobě, přičemž každá Smluvní strana obdrží její elektronický originál opatřený platnými elektronickými podpisy. Kontaktní údaje Smluvních stran pro doručování jsou následující:

Kontaktní osoba Objednatele

Ve věcech technických:

[Redacted contact information]

Ve věcech smluvních:

[Redacted contact information]

Kontaktní osoba Dodavatele

Ve věcech technických:

[Redacted contact information]



Ve věcech smluvních:



7.6 Nedílnou součástí této Smlouvy jsou následující přílohy:

Příloha č. 1 – Specifikace Plnění

Příloha č. 2 – VOP

7.7 Smluvní strany potvrzují, že se s textem VOP seznámily před podpisem této Smlouvy a je jim znám jejich význam v souladu a ve spojitosti se Smlouvou. Dále Smluvní strany potvrzují, že veškerým ustanovením Smlouvy a VOP plně a bez jakýchkoli obtíží porozuměly a nepovažují je za nevýhodná. VOP představují závaznou a nedílnou součást Smlouvy.

NA DŮKAZ TOHO, že Smluvní strany s obsahem Smlouvy souhlasí, rozumí ji a zavazují se k jejímu plnění, připojují své podpisy a prohlašují, že tato Smlouva byla uzavřena podle jejich svobodné a vážné vůle prosté tísně, zejména tísně finanční.

V Praze

V Praze

Ing. Martin Götz

ředitel úseku ICT

Česká pošta, s.p.

Ing. Čestmír Pail

jednatel

DATACONS s.r.o.



Příloha č. 1 – Specifikace Plnění

1. Definice pojmů

1.1.1 Uživatel

Pro účely této Smlouvy se „uživatel“ rozumí fyzická osoba, která je s Objednatelem v pracovněprávním vztahu na základě pracovní smlouvy uzavřené dle zákoníku práce, případně osoba vykonávající práci pro Objednatele na základě dohody o pracovní činnosti nebo dohody o provedení práce (dále jen „uživatel“). Do této kategorie spadají jak kmenoví zaměstnanci, tak i brigádníci, kteří vykonávají činnost pro Objednatele na základě platného smluvního vztahu.

1.1.2 Brand

Pro účely této Smlouvy se „brandem“ rozumí souhrn vizuálních a grafických prvků, které reprezentují identitu Objednatele, zejména pak logotyp, barevnost, typografie, grafické styly a další prvky vizuální komunikace (dále je „brand“). Brand je aplikován na všechny výstupy, prezentace a další části předmětu plnění, které mají být vizuálně sladěny s identitou Objednatele. Dodavatel je povinen při tvorbě těchto výstupů respektovat vizuální styl Objednatele a zajistit jejich soulad s jeho brandem.

1.1.3 Platforma

Pro účely této Smlouvy se „Platformou“ rozumí externí služba provozovaná v prostředí Dodavatele, která slouží k realizaci školení zaměstnanců Objednatele v oblasti kybernetické bezpečnosti. Platforma dále zahrnuje nástroje pro simulaci phishingových kampaní, jejich distribuci, sledování reakcí uživatelů a vyhodnocování výsledků těchto kampaní (dále jen „Platforma“).

2. Specifikace Plnění

Platforma musí pokrývat klíčové oblasti znalostí v oblasti kybernetické bezpečnosti, včetně, ale nikoli výlučně, ochrany před phishingem, bezpečného nakládání s daty, správy hesel, bezpečného chování na internetu a dalších relevantních témat. Zároveň musí být technicky uzpůsobena pro použití v prostředí s omezenou šířkou pásma a podporovat bezproblémové využití při práci na dálku, včetně optimalizace pro různá zařízení a typy připojení.

Platforma musí být navržena tak, aby minimalizovala potřebu technických zásahů ze strany Objednatele, a to buď prostřednictvím vestavěných funkcí, nebo formou dodatečných profesionálních služeb poskytovaných Dodavatelem.

Platforma musí v rámci rozvoje umožňovat integraci s běžně používanými systémy IDM.

Přístup do Platformy musí být možný z různých zařízení (např. notebooky, mobilní telefony, tablety) prostřednictvím webového rozhraní, bez nutnosti instalace specifického softwaru nebo aplikace.

Objednatel musí mít možnost upravovat a přizpůsobovat obsah školení dle vlastních potřeb, včetně úprav textů, scénářů a vizuálních prvků.

Zapojení uživatelů do Platformy nesmí vyžadovat žádné dodatečné technické konfigurace nebo složité implementační postupy.

Platforma musí obsahovat nástroje pro sledování a vyhodnocování výkonnostních metrik, které umožní měřit efektivitu samotné Platformy a pokrok uživatelů. Metriky musí být dostupné na úrovni jednotlivých uživatelů, organizačních jednotek (např. oddělení) i celé organizace. Minimálně musí být možné sledovat míru absolvování školení, úspěšnost v testech, čas strávený vzděláváním a změny v chování uživatelů v čase. Výsledky musí být dostupné formou přehledných reportů a exportovatelných dat.

Platforma musí využívat odborně uznávanou a systematickou taxonomii kybernetických útoků, zejména v oblasti sociálního inženýrství, pro návrh, plánování, doporučování a řízení simulovaných útoků. Tato

taxonomie musí sloužit jako rámec pro zajištění toho, že simulace pokrývají všechny klíčové oblasti výukového obsahu, a že uživatelé budou vystaveni různorodým scénářům odpovídajícím reálným hrozbám.

Taxonomie musí umožnit kategorizaci útoků podle typu (např. phishing, spear phishing, pretexting, baiting, tailgating), cílové skupiny, způsobu doručení a úrovně sofistikovanosti. Platforma musí zajistit, že výukový obsah bude strukturován tak, aby pokrýval všechny důležité aspekty kybernetické bezpečnosti a umožnil systematické vzdělávání uživatelů.

Jako příklad akceptovatelné taxonomie lze uvést rámec MITRE ATT&CK, který poskytuje podrobný přehled taktik, technik a postupů používaných útočníky, a který může být využit pro tvorbu realistických a cílených scénářů simulací.

Všechny obsahové moduly navržené Dodavatelem musí být dostupné v jazykové verzi CZ. Moduly, pro které nebude k dispozici odpovídající jazyková verze, budou z nabídky automaticky vyloučeny.

Překlady musí být provedeny kvalifikovanými překladateli, kteří splňují alespoň jednu z následujících podmínek:

- mají příslušné vysokoškolské vzdělání v oboru překladatelství nebo lingvistiky, nebo
- splňují požadavky normy ČSN EN ISO 17100 (Služby překladu – Požadavky na překladatelské služby).

Objednatel se zavazuje pravidelně předávat Dodavateli aktuální seznam uživatelů určených k zařazení do školení prostřednictvím Platformy. Tento seznam bude obsahovat relevantní údaje nezbytné pro vytvoření a správu uživatelských účtů, zejména:

- jméno a příjmení,
- e-mailovou adresu,
- osobní číslo zaměstnance (pokud je přiděleno),
- zařazení do organizační struktury Objednatele (např. oddělení, pracovní pozice).
- typ uživatele pro účely výběru školení (běžný uživatel typu 10, běžný uživatel typu 20, administrátor, management ...)

Předané údaje budou využity pro:

- vytvoření a správu uživatelských účtů v rámci Platformy,
- identifikaci nových uživatelů (přirůstky),
- detekci ukončení pracovního poměru nebo změn v organizační struktuře (úbytky).

Dodavatel je povinen s těmito údaji nakládat v souladu s platnými právními předpisy o ochraně osobních údajů a zajistit jejich bezpečné zpracování.

3. Požadavek na reporty

Platforma musí generovat **pravidelné a ad hoc reporty** pro následující účely:

- **Interní a externí audit** – doložení realizace školení, včetně dat o účasti, úspěšnosti a termínech absolvování.
- **Sledování pokroku uživatelů** – přehledy o individuálním i skupinovém postupu, míře dokončení školení, výsledcích testů a změnách v chování uživatelů.
- **Informování managementu a výboru pro řízení kybernetické bezpečnosti** – souhrnné statistiky o úrovni kybernetického povědomí napříč organizací, trendy a doporučení pro další kroky.

Reporty musí být:

- **Přehledné a vizuálně srozumitelné** (např. grafy, tabulky),
- **Exportovatelné** do běžných formátů (např. PDF, XLSX, CSV),
- **Filtrovací a třídící** podle organizační struktury, časového období, typu školení nebo výsledků.

4. Školení v oblasti kybernetické bezpečnosti

Předmětem plnění je též zajištění školení v oblasti kybernetické bezpečnosti pro uživatele, a to formou distančního školení (online interaktivní forma) s možností převodu školení do podpůrného materiálu pro prezenční školení. Školení bude přizpůsobeno jednotlivým cílovým skupinám uživatelů a zaměřeno na zvýšení povědomí o rizicích a hrozbách v oblasti kybernetické bezpečnosti, prevenci, správnému chování a postupech při incidentu.

Cíle školení

- Zajistit jednorázové školení v rozsahu min. 90 minut pro nové uživatele.
- Zajistit pro stávající uživatele celoroční rozdělení školení do více kratších tematických bloků (tzv. microlearning), z nichž žádný nepřesáhne 30 minut, ale jejichž celkový roční rozsah bude odpovídat níže uvedenému školení pro zaměstnance, případně administrátory.
- Zajistit monitoring absolvování školení, automatická připomenutí neabsolvovaných lekcí a přehledné výstupy pro správu uživatelů (např. reporty pro vedoucí pracovníky nebo administrátora).

Dodavatel zajistí školení minimálně v následujícím rozsahu:

Obsah školení pro běžné uživatele:

- Základní pojmy a principy kybernetické bezpečnosti
- Relevantní kybernetické hrozby a techniky používaných útočníků (např. phishing, spear phishing, ransomware, malware, zneužití legitimních nástrojů, techniky sociálního inženýrství, včetně podvodného volání a SMS – tzv. vishing a smishing), v souladu s rámcem MITRE ATT&CK
- Pravidla bezpečné práce s e-mailem a internetem
- Zásady tvorby a správy hesel, vícefaktorové ověřování (MFA)
- Bezpečná práce s mobilními zařízeními a vzdálený přístup
- Ochrana osobních údajů a citlivých informací
- Povinnosti uživatelů při podezření na bezpečnostní incident

Obsah školení pro IT pracovníky (administrátoři, správci):

- Principy bezpečné správy IT systémů a sítí
- Zabezpečení přístupových práv a identity management
- Zálohování a obnova dat, segmentace sítí
- Detekce a reakce na bezpečnostní incidenty
- Základy forenzní analýzy a logování
- Aktuální hrozby v oblasti malware a zneužití zranitelností
- Zásady bezpečné konfigurace zařízení

Obsah školení pro vrcholový management:

- Kybernetická bezpečnost jako součást řízení organizace
- Právní rámec (ZoKB, GDPR, NIS2 - nZoKB, DORA)
- Role vedení v oblasti bezpečnosti informací



- Řízení rizik a odpovědnost za bezpečnostní incidenty
- Rozhodování v krizových situacích (incident management)

Další požadavky:

- Dodavatel připraví interaktivní školení přizpůsobené jednotlivým skupinám a ICT prostředí Objednatele
- Součástí školení bude krátký test ověřující pochopení klíčových témat
- Dodavatel předloží osnovu školení ke schválení před realizací
- Školení bude realizováno v českém jazyce, v celkovém rozsahu minimálně 90 minut pro běžné uživatele, 120 minut pro IT pracovníky a 60 minut pro vrcholový management
- Školení bude možné opakovat v dalších termínech nebo formou e-learningu
- Dodavatel bude pravidelně poskytovat report pro nastavení získané kvalifikace u uživatelů

5. Harmonogram implementace

Implementace Platformy bude probíhat v následujících fázích:

D – Účinnost Smlouvy

D+7 kalendářních dnů – Dodavatel předá osnovu školení ke schválení Objednateli

D+21 kalendářních dnů – Zahájení přístupu uživatelů do Platformy

D+30 kalendářních dnů – První simulovaná phishingová kampaň

D+60 kalendářních dnů – První hodnocení účinnosti školení (report)

D+90 kalendářních dnů – Závěrečné vyhodnocení a návrh na úpravy obsahu podle výsledků hodnocení

6. Service Level Agreement (SLA)

Dostupnost služby: Platforma musí být dostupná minimálně tři týdny v měsíci.

Reakční doby podpory:

- Kritické incidenty: reakce do 4 hodin.
- Vážné incidenty: reakce do 1 pracovního dne.
- Méně závažné incidenty: reakce do 3 pracovních dnů.

Úrovně závažnosti incidentů:

- Kritické incidenty: úplná nedostupnost Platformy.
- Vážné incidenty: významné omezení funkčnosti Platformy.
- Méně závažné incidenty: drobné omezení funkčnosti Platformy.

7. Provoz a školení

- Nasazení a konfigurace Platformy v prostředí Dodavatele.
- Import uživatelů na základě předaných dat.
- Spuštění simulací phishingových útoků a e-learningových školení.
- Zavedení pokročilých metrik pro měření kybernetického povědomí.
- Personalizace školení na základě chování uživatele a výsledků simulací.



- Využití AI pro doporučování obsahu a predikci rizikového chování.
- Školení zástupců či správců Objednatele pro účely správy a využívání Platformy.

8. Požadavky na bezpečnost a ochranu dat

Platforma musí splňovat následující bezpečnostní požadavky:

- Řízení přístupu k datům uživatelů
- Šifrování dat při přenosu i uložení (např. TLS 1.2+, AES-256).
- Umístění dat v EU (v souladu s GDPR).
- Role-based access control (RBAC).
- Auditní logy a jejich uchování.



Příloha č. 2 - Obchodní podmínky pro poskytování služeb

(Tato strana je úmyslně ponechána prázdná. VOP následují na další straně.)

