Best Practice:
Právne a procesné štandardy pri implementácii inteligentných riešení vo verejnej správe a územnej samospráve

1. ÚVOD

Digitálna transformácia verejnej správy a územnej samosprávy je v súčasných podmienkach neoddeliteľne spätá s budovaním dátovo orientovaného, sieťovo prepojeného a technologicky podporovaného prostredia výkonu verejných úloh. Kým v skorších fázach elektronizácie verejnej správy bol dôraz kladený predovšetkým na digitalizáciu administratívnych procesov, elektronickú komunikáciu a evidenčné informačné systémy, aktuálna vývojová etapa sa čoraz výraznejšie opiera o fyzicky distribuované inteligentné zariadenia, senzorické siete, komunikačné vrstvy, cloudové infraštruktúry, automatizované vyhodnocovanie dát a o následnú integráciu týchto prvkov do procesov riadenia verejných služieb. Práve v tomto kontexte nadobúda zásadný význam Internet vecí (ďalej ako „IoT") ako technicko-právny fenomén, ktorý už nemožno vnímať len ako technologickú inováciu, ale ako infraštruktúrny a regulačný základ mnohých moderných riešení verejnej správy.

V podmienkach miest, obcí, samosprávnych krajov, škôl, dopravných systémov, environmentálneho monitoringu, verejného osvetlenia, odpadového hospodárstva, energetického manažmentu či správy verejného priestoru sa IoT stáva základnou vrstvou inteligentného prostredia. Umožňuje nepretržitý zber údajov z fyzického sveta, ich prenos do riadiacich a analytických systémov, generovanie upozornení, predikcií alebo automatizovaných reakcií, a tým aj zásadnú zmenu v spôsobe, akým verejný sektor plní svoje funkcie. Takéto riešenia však zároveň výrazne zasahujú do režimu ochrany osobných údajov, kybernetickej bezpečnosti, správy informačných technológií vo verejnom sektore, verejného obstarávania, správy majetku, zodpovednosti za rozhodovanie a pri niektorých typoch systémov aj do regulačného rámca umelej inteligencie. Právna reflexia IoT vo verejnej správe je preto nevyhnutná z dvoch základných dôvodov.

- Po prvé, IoT riešenia spravidla nevystupujú ako izolované technické komponenty, ale ako súčasť širších rozhodovacích, monitorovacích a prevádzkových procesov, ktoré môžu mať priamy alebo nepriamy dopad na jednotlivca, na dostupnosť verejnej služby, na rozdelenie verejných zdrojov alebo na výkon verejnej moci.

- Po druhé, ich infraštruktúrna povaha spôsobuje, že právne riziká nevznikajú len pri samotnom spracúvaní údajov, ale už pri návrhu senzorickej siete, pri definovaní jej účelu, pri integrácii s ďalšími systémami, pri voľbe komunikačného protokolu, pri spôsobe bezpečnostného riadenia zariadení a pri nastavení zmluvných a obstarávacích podmienok.

1.1. INTELIGENTNÉ RIEŠENIA AKO INFRAŠTRUKTÚRNY A REGULAČNÝ EKOSYSTÉM

Pojem inteligentné riešenia sa v kontexte verejnej správy často používa ako všeobecné označenie pre digitálne, automatizované alebo dátovo podporované systémy, ktoré prispievajú k riadeniu verejných služieb, infraštruktúry alebo správnych procesov. V právne presnom zmysle však treba tento pojem chápať širšie a systémovejšie. Inteligentné riešenie totiž typicky nepredstavuje iba softvér alebo analytickú aplikáciu, ale komplexný funkčný ekosystém, v ktorom sa prepájajú zariadenia na fyzickej vrstve, komunikačné siete, zber a prenos dát, ich ukladanie, vyhodnocovanie, vizualizácia, rozhodovacie pravidlá, integračné väzby, zmluvné vzťahy a procesné dôsledky. V prostredí verejnej správy je tento systémový pohľad obzvlášť dôležitý. Každé inteligentné riešenie totiž vchádza do existujúceho režimu výkonu verejných úloh a stáva sa súčasťou verejnoprávneho rozhodovacieho alebo prevádzkového rámca. Ak napríklad samospráva nasadí senzory dopravy, inteligentné osvetlenie, environmentálne stanice alebo zariadenia na monitorovanie odpadu, nejde len o technickú modernizáciu. Ide o vytvorenie novej dátovej reality, ktorá bude vplývať na manažérske rozhodovanie, na prevádzkové zásahy, na plánovanie investícií a v niektorých prípadoch aj na kontrolné alebo sankčné činnosti. Technológia sa tak stáva súčasťou normatívne relevantného prostredia a musí byť posudzovaná nielen z pohľadu výkonnosti, ale aj z pohľadu práva.

1.2. INTERNET VECÍ (IOT) V PODMIENKACH VEREJNEJ SPRÁVY A ÚZEMNEJ SAMOSPRÁVY

Internet vecí (IoT) predstavuje hlavnú technologickú líniu, na ktorej sú budované súčasné inteligentné riešenia vo verejnom sektore. Na účely tohto dokumentu treba IoT vymedziť ako sieť fyzických zariadení, objektov, senzorov, akčných prvkov, riadiacich jednotiek a komunikačných modulov, ktoré sú schopné zbierať údaje o svojom prostredí, prenášať ich prostredníctvom elektronických komunikačných sietí, prijímať pokyny alebo automatizovane reagovať na zistený stav. V prostredí verejnej správy môže ísť o zariadenia monitorujúce dopravu, obsadenosť parkovacích miest, kvalitu ovzdušia, intenzitu hluku, spotrebu energií, stav verejného osvetlenia, naplnenosť odpadových nádob, pohyb osôb v budovách, prevádzku vozidiel, mikroklimatické podmienky, stav mostných konštrukcií alebo ďalšie parametre relevantné pre výkon verejných služieb.

Právne významné je, že IoT systémy majú spravidla viacvrstvovú architektúru. Na najnižšej úrovni sa nachádza fyzická vrstva zariadení a senzorov, ktorá interaguje s materiálnym prostredím. Nad ňou existuje komunikačná vrstva, prostredníctvom ktorej sa dáta prenášajú cez siete typu LTE, 5G, LoRaWAN, NB-IoT, Wi-Fi, Bluetooth alebo iné protokoly. Nasleduje vrstva dátového zberu, úložiska a integračných služieb, často realizovaná v cloudovom alebo hybridnom prostredí. Nad ňou je aplikačná a analytická vrstva, v ktorej sú dáta agregované, vizualizované a spracúvané s cieľom generovať

odporúčania, alarmy, riadiace impulzy alebo výstupy pre verejné rozhodovanie. Táto viacvrstvovosť spôsobuje, že právna zodpovednosť, bezpečnostné povinnosti a procesné riziká nevznikajú iba v jednej fáze, ale priečne naprieč celým životným cyklom systému.

V právnom prostredí verejnej správy preto nemožno IoT posudzovať len ako súbor zariadení. IoT je potrebné chápať ako dátovú infraštruktúru výkonu verejných úloh, ktorá musí byť zlučiteľná s princípmi zákonnosti, proporcionality, účelového obmedzenia, minimizácie zásahu, informačnej bezpečnosti, transparentnosti a verejnej kontrolovateľnosti. Technologický dodávateľ, ktorý navrhuje IoT systém pre mesto, obec alebo kraj, tak musí predvídať nielen fyzickú a komunikačnú funkcionalitu zariadení, ale aj ich právny režim, prevádzkové dôsledky a budúce integračné účinky. Ak má byť riešenie použiteľné vo verejnej správe, musí byť navrhnuté tak, aby rešpektovalo pravidlá verejného obstarávania, princípy ochrany osobných údajov, požiadavky kybernetickej bezpečnosti, interoperabilitu IT vo verejnom sektore, ako aj potrebu zachovania rozhodovacej a prevádzkovej autonómie verejného subjektu. Právne požiadavky preto nemožno chápať ako externé obmedzenie technológie, ale ako súčasť jej kvality, trhovej spôsobilosti a inštitucionálnej legitimity.

2. PRÁVNY A REGULAČNÝ RÁMEC

2.1. VEREJNÉ OBSTARÁVANIE PRI IOT PROJEKTOCH

Verejné obstarávanie zohráva pri implementácii IoT riešení zásadne formujúcu úlohu, pretože práve v tejto fáze sa určuje, či bude budúca infraštruktúra otvorená, interoperabilná, bezpečná a dlhodobo udržateľná, alebo či sa verejný subjekt dostane do technologickej, zmluvnej a ekonomickej závislosti od jedného dodávateľa. IoT projekty sú z pohľadu verejného obstarávania špecifické tým, že predmet zákazky často netvorí iba jeden softvérový produkt alebo jedno zariadenie, ale celý systém pozostávajúci zo senzorických prvkov, komunikačných modulov, riadiacich jednotiek, dátových úložísk, integračných mostov, analytických vrstiev a servisnej podpory. Ak verejný obstarávateľ alebo dodávateľ túto systémovosť podcení, vzniká vysoké riziko, že podklady budú formulované spôsobom, ktorý nebude súťažne neutrálny alebo nebude dostatočne chrániť budúcu prevádzkovú autonómiu verejného partnera.

Z právneho hľadiska je nevyhnutné, aby boli podklady k IoT projektu pripravené v súlade so zásadami rovnakého zaobchádzania, zákazu diskriminácie, transparentnosti a proporcionality. V praxi to znamená, že technická špecifikácia nesmie byť postavená tak, aby fakticky opisovala jeden konkrétny proprietárny systém, jeden konkrétny protokol, jedného výrobcu senzorov alebo jednu konkrétnu cloudovú architektúru, pokiaľ takýto postup nie je výnimočne objektívne odôvodnený. Pri IoT býva veľmi častou chybou, že sa verejnému obstarávateľovi „predpripraví" opis riešenia na báze konkrétnej platformy vrátane jej komunikačných vlastností, dátového modelu, spôsobu správy zariadení a servisného rozhrania. Takto nastavený predmet zákazky však môže v skutočnosti znamenať vylúčenie konkurencie a vytvorenie situácie, v ktorej bude budúce rozširovanie alebo obmena systému fakticky možná len cez pôvodného dodávateľa.

Pri IoT projektoch treba preto venovať mimoriadnu pozornosť „*vendor lock-in*"[1], ktorý má v tomto segmente ešte hlbší dosah než pri bežných softvérových zákazkách. Ak sú totiž fyzické zariadenia, komunikačné vrstvy, cloudová infraštruktúra, správa firmvéru, dátové modely a vizualizačné rozhrania navrhnuté ako uzavretý proprietárny systém, verejný subjekt môže stratiť schopnosť meniť dodávateľa bez masívnych nákladov, bez výmeny už nainštalovaného hardvéru alebo bez straty historických dát. V prostredí miest, obcí a krajov je takýto stav mimoriadne rizikový, pretože IoT zariadenia majú často dlhý životný cyklus, bývajú rozmiestnené vo verejnom priestore a ich výmena predstavuje nielen finančný, ale aj organizačný a bezpečnostný zásah. Právne a procesne správne nastavenie preto vyžaduje, aby boli už v zadávacej dokumentácii a následne aj v zmluvách presne formulované

[1] Vendor lock-in predstavuje stav, v ktorom sa verejný subjekt stáva technologicky, ekonomicky alebo organizačne závislým od konkrétneho dodávateľa v takom rozsahu, že zmena dodávateľa alebo migrácia riešenia si vyžaduje neprimerané náklady, zásadné technické zásahy alebo stratu prístupu k údajom, funkcionalitám či prevádzkovému know-how. Pri návrhu, obstarávaní a prevádzke IoT riešení je preto nevyhnutné prijímať technické, organizačné a zmluvné opatrenia smerujúce k zachovaniu interoperability, prenositeľnosti dát a možnosti efektívnej zmeny dodávateľa počas celého životného cyklu systému.

požiadavky na interoperabilitu, otvorenosť alebo štandardizáciu dátových formátov, dokumentované API[2], prenositeľnosť konfigurácií, export historických dát, prístup k logom, správu zariadení a podmienky migrácie do iného prostredia. V prípade senzorických sietí je vhodné požadovať aj transparentné vymedzenie komunikačných protokolov, spôsobu aktualizácie zariadení, kompatibility s infraštruktúrou tretích strán a odolnosti voči výpadkom alebo budúcej modularizácii. Dodávateľ, ktorý uvažuje o pôsobení vo verejnom sektore, by mal preto svoje IoT riešenie navrhovať tak, aby bolo možné ho obstarať na základe funkčných a výkonových požiadaviek, nie na základe skrytého opisu jedinej uzavretej platformy.

2.2. OCHRANA OSOBNÝCH ÚDAJOV PRI IOT SYSTÉMOCH

V prostredí verejnej správy sa aj zdanlivo technické alebo environmentálne údaje môžu stať osobnými údajmi, ak sú priraditeľné ku konkrétnej osobe alebo ak v kombinácii s ďalšími prvkami umožňujú osobu identifikovať či individualizovať jej správanie, pohyb alebo postavenie. Právna citlivosť IoT vyplýva zo samotnej povahy senzorického monitoringu. Ak zariadenia v reálnom čase alebo v krátkych intervaloch zbierajú údaje o polohe, pohybe, využívaní infraštruktúry, spotrebe alebo interakcii osôb s verejným priestorom, môže ísť o spracúvanie osobných údajov aj vtedy, keď primárnym cieľom systému nebolo „identifikovať osobu" v tradičnom zmysle slova. Typickým príkladom sú parkovacie systémy, kamerové systémy s čítaním evidenčných čísel, senzory v budovách verejných inštitúcií, systémy sledovania pohybu služobných vozidiel, zariadenia evidujúce vstupy a výstupy, či inteligentné dochádzkové alebo prístupové systémy. V takýchto prípadoch už nejde len o technické dáta, ale o údaje, ktoré sa môžu viazať na konkrétnu fyzickú osobu alebo aspoň na jej individualizovateľné správanie. V prostredí verejnej správy je navyše potrebné vziať do úvahy, že samotná existencia zákonného cieľa ešte automaticky neznamená neobmedzenú možnosť nasadiť akúkoľvek senzorickú alebo monitorovaciu technológiu. Na každé spracúvanie sa vzťahujú zásady zákonnosti, obmedzenia účelu, minimalizácie údajov, obmedzenia uchovávania a integrity spracúvania. Pri IoT to znamená, že verejný orgán a jeho dodávateľ musia vedieť odôvodniť, prečo je potrebné určitý údaj zbierať, ako často sa má merať, aká presnosť je primeraná, ako dlho je potrebné údaj uchovávať, akým spôsobom sa bude zabezpečovať jeho pseudonymizácia alebo anonymizácia a kto bude mať k výstupom prístup.

Obzvlášť citlivá je hranica medzi prevádzkovým monitoringom a monitoringom správania osôb. Mnohé IoT riešenia sa navonok prezentujú ako systémy na správu majetku alebo verejnej infraštruktúry, no ich faktickým dôsledkom môže byť pomerne detailné

[2] Dokumentované API predstavuje technické rozhranie systému, ktorého funkcionalita, dátové štruktúry, komunikačné pravidlá a integračné mechanizmy sú dostupné v dostatočne podrobnej technickej dokumentácii. Požiadavka na dokumentované API umožňuje zabezpečiť interoperabilitu, prenositeľnosť dát, integráciu s ďalšími systémami a znižovať riziko vzniku závislosti verejného subjektu od konkrétneho dodávateľa. Pri obstarávaní IoT riešení by mala byť dostupnosť a dokumentovanosť API jednou zo základných technických požiadaviek na dodávané riešenie.

sledovanie používania verejného priestoru alebo zariadení konkrétnymi osobami. Táto skutočnosť musí byť predmetom predchádzajúcej právnej analýzy. Ak systém umožňuje vyvodiť závery o pohybe, rutine, prítomnosti alebo preferenciách jednotlivcov, už nemožno hovoriť o neutrálnej technickej infraštruktúre. V takom prípade nastupuje plná požiadavka ochrany práv dotknutých osôb vrátane informačných povinností, prísnejšieho testu proporcionality a často aj potreby vypracovať DPIA.[3]

Pri IoT infraštruktúre je nevyhnutné pristupovať veľmi obozretne aj k pseudonymizovaným alebo agregovaným dátam. Skutočnosť, že systém neukladá meno osoby, ešte neznamená, že spracúvanie je automaticky mimo pôsobnosti pravidiel ochrany osobných údajov. Ak možno údaje spätne spojiť s konkrétnym zariadením, vozidlom, miestom, časovou stopou alebo kombináciou ďalších identifikátorov, právny režim ochrany osobných údajov sa môže uplatniť v plnej miere. Dodávateľ IoT riešenia preto musí už v návrhovej fáze vedieť preukázať, akým spôsobom bude minimalizovať riziko spätného priradenia dát, ako bude riešiť prístupové práva a ako bude architektonicky rozlišovať medzi údajmi nevyhnutnými na samotnú prevádzku a údajmi, ktoré by predstavovali neprimeraný zásah do súkromia.

2.3. KYBERNETICKÁ BEZPEČNOSŤ IOT V PROSTREDÍ VEREJNEJ SPRÁVY

Kybernetická bezpečnosť predstavuje pri IoT riešeniach vo verejnom sektore fundamentálnu právnu aj technickú požiadavku. Na rozdiel od tradičných informačných systémov, ktoré sú typicky umiestnené v kontrolovanom prostredí serverovní alebo administratívnych sietí, IoT zariadenia bývajú rozmiestnené vo verejnom priestore, v technických objektoch, na budovách, v dopravnej infraštruktúre, na mobiliári alebo v iných fyzicky exponovaných lokalitách. Táto rozptýlenosť sama osebe zvyšuje riziko fyzického zásahu, neoprávnenej manipulácie, rušenia signálu, kompromitácie zariadení alebo podvrhnutia dát.

Právny a procesný rámec kybernetickej bezpečnosti preto musí pri IoT projektoch počítať s tým, že zraniteľnosť nevzniká iba na úrovni centrálneho systému, ale na každom jednotlivom zariadení a na každom bode prenosovej a integračnej reťaze. Verejný orgán i dodávateľ musia vedieť preukázať, ako sa budú spravovať identity zariadení, aké autentifikačné a autorizačné mechanizmy budú použité, ako bude zabezpečené šifrovanie komunikácie, ako sa budú distribuovať aktualizácie firmvéru, ako bude prebiehať detekcia anomálií, ako sa budú riešiť incidenty a čo sa stane v prípade výpadku konektivity alebo

[3] Posúdenie vplyvu na ochranu osobných údajov (DPIA) predstavuje systematický proces identifikácie, hodnotenia a zmierňovania rizík vyplývajúcich zo spracúvania osobných údajov. Jeho cieľom je zabezpečiť, aby navrhované riešenie rešpektovalo práva a slobody dotknutých osôb a aby boli primerane implementované technické, organizačné a bezpečnostné opatrenia. Pri IoT projektoch sa DPIA vykonáva ešte pred nasadením systému a musí zohľadňovať celý životný cyklus údajov vrátane zberu, prenosu, uchovávania, analýzy a zdieľania údajov.

narušenia integrity dát. V prostredí verejnej správy ide o otázky, ktoré majú priamy dopad na kontinuitu výkonu verejnej služby a v niektorých prípadoch aj na bezpečnosť osôb a majetku.

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a zákon č. 69/2018 Z.z o kybernetickej bezpečnosti vytvárajú základný rámec pre riadenie životného cyklu IT vo verejnom sektore a z jeho princípov vyplývajú pre IoT riešenia významné dôsledky. Verejný orgán musí mať nad informačnými technológiami reálnu správnu, prevádzkovú a kontrolnú kapacitu, čo sa pri IoT týka nielen softvérového dashboardu, ale aj samotných zariadení, komunikácie, aktualizácií a rozhraní. Ak dodávateľ navrhne systém tak, že verejný partner nebude schopný samostatne zistiť stav zariadení, auditovať ich činnosť, exportovať ich dáta alebo zmeniť servisný model, dostáva sa takýto projekt do napätia s požiadavkou riadneho riadenia IT vo verejnej správe. Veľmi citlivou témou je aj prepojenie IoT so službami cloudu a edge computingu. Ak sa dáta zo senzorov vyhodnocujú v externom prostredí, je potrebné presne vymedziť, kde sa tieto dáta spracúvajú, kto k nim pristupuje, ako sa auditujú, aké sú podmienky ich prenosu, ako dlho sa uchovávajú a za akých okolností možno vykonať ich migráciu. Tieto otázky majú nielen bezpečnostný, ale aj právny rozmer, pretože verejný subjekt musí byť schopný zodpovedať za správu dát, ktoré vznikajú pri plnení jeho verejných úloh.

3. ODPORÚČANÝ POSTUP PRE IMPLEMENTÁCIU

FÁZA 1: PRÍPRAVA PROJEKTU A PRÍPRAVA NA ÚČASŤ VO VEREJNOM OBSTARÁVANÍ

Implementácia IoT riešenia vo verejnej správe sa musí začínať dôslednou prípravnou fázou, ktorá spája dve navzájom prepojené oblasti pripravenosti hospodárskeho subjektu na účasť vo verejnom obstarávaní a dôkladné pochopenie technických, právnych a prevádzkových požiadaviek pripravovaného projektu. Úspešná účasť vo verejnom obstarávaní sa totiž nezačína samotným predložením ponuky, ale vytvorením interných predpokladov na to, aby dodávateľ vedel pripraviť kvalitné, realizovateľné a právne udržateľné riešenie reflektujúce potreby verejného obstarávateľa.

Prvým krokom je overenie právnej, organizačnej a podnikateľskej pripravenosti hospodárskeho subjektu. Dodávateľ by mal disponovať potrebnými oprávneniami na výkon činností súvisiacich s predmetom zákazky, mať aktuálne údaje v príslušných registroch a preveriť svoju schopnosť splniť podmienky účasti, ktoré sa vo verejných obstarávaniach bežne vyžadujú. Súčasne je potrebné identifikovať odborné kapacity, technické vybavenie, personálne zdroje, certifikácie a referencie, ktoré budú tvoriť základ budúcej ponuky. V prípade potreby je vhodné už v tejto fáze zvážiť využitie subdodávateľov, vytvorenie konzorcia alebo preukazovanie technickej a odbornej spôsobilosti prostredníctvom iných subjektov.

Paralelne s internou pripravenosťou musí dodávateľ dôkladne analyzovať samotný projekt a jeho účel. Pri IoT riešeniach je nevyhnutné pochopiť nielen technické požiadavky verejného obstarávateľa, ale aj právny a spoločenský kontext, v ktorom bude systém nasadený. Nestačí vychádzať len z technologických možností navrhovaného riešenia. Dodávateľ by mal posúdiť, aký problém má systém riešiť, aké procesy bude podporovať, aké údaje bude spracúvať a aké dôsledky môže mať jeho prevádzka na jednotlivcov, organizáciu alebo verejný záujem.

Osobitná pozornosť musí byť venovaná predbežnému právnemu, dátovému a bezpečnostnému posúdeniu navrhovaného riešenia. Dodávateľ by mal identifikovať predpokladané dátové toky, kategórie spracúvaných údajov, spôsob komunikácie medzi zariadeniami, integračné rozhrania, prevádzkové role a bezpečnostné opatrenia. Ak navrhované riešenie zahŕňa spracúvanie osobných údajov alebo môže predstavovať zvýšené riziko pre práva a slobody fyzických osôb, je potrebné už v prípravnej fáze zohľadniť požiadavky na posúdenie vplyvu na ochranu osobných údajov. Ak je súčasťou riešenia aj systém umelej inteligencie, je potrebné posúdiť aj jeho regulačné a etické aspekty vrátane možných požiadaviek vyplývajúcich z AI Actu.

V tejto etape je zároveň potrebné aplikovať princípy nevyhnutnosti, proporcionality a minimalizácie údajov. IoT technológie často umožňujú zhromažďovať väčší rozsah údajov, než je potrebný na dosiahnutie sledovaného cieľa. Dodávateľ by preto mal už pri návrhu

riešenia posúdiť, aké údaje sú skutočne potrebné, v akej kvalite a frekvencii majú byť spracúvané a aká doba uchovávania údajov je primeraná sledovanému účelu.

Neoddeliteľnou súčasťou prípravnej fázy je aj technická pripravenosť na elektronickú komunikáciu vo verejnom obstarávaní. Dodávateľ musí disponovať potrebnými prístupmi do elektronických systémov, kvalifikovaným elektronickým podpisom a internými procesmi umožňujúcimi efektívnu prípravu a predkladanie ponúk.

V závere prípravnej fázy by mal dodávateľ vyhodnotiť, či disponuje dostatočnými odbornými, technickými, personálnymi a finančnými kapacitami na realizáciu zákazky a či navrhované riešenie zodpovedá požiadavkám verejného obstarávateľa. Výstupom tejto fázy by malo byť rozhodnutie o účasti vo verejnom obstarávaní a vytvorenie pevného organizačného, technického a právneho základu pre prípravu konkurencieschopnej ponuky.

FÁZA 2: PRÍPRAVA PONUKY A NASTAVENIE ZMLUVNÉHO A TECHNICKÉHO MODELU RIEŠENIA

Po rozhodnutí o účasti vo verejnom obstarávaní vstupuje dodávateľ do fázy prípravy ponuky a návrhu zmluvného, technického a prevádzkového modelu riešenia. Pri IoT projektoch nestačí pripraviť iba cenovú ponuku alebo technickú špecifikáciu zariadení. Dodávateľ musí preukázať schopnosť zabezpečiť celý životný cyklus riešenia vrátane jeho nasadenia, prevádzky, bezpečnostnej správy, aktualizácií, servisu, spracúvania údajov a budúceho rozvoja. Verejní obstarávatelia čoraz častejšie posudzujú nielen technické parametre ponúkaného riešenia, ale aj jeho udržateľnosť, interoperabilitu a schopnosť fungovať v súlade s právnymi požiadavkami počas celej doby prevádzky.

Pri príprave ponuky musí dodávateľ dôkladne analyzovať požiadavky verejného obstarávateľa a preveriť, či navrhované riešenie spĺňa všetky funkčné, technické, bezpečnostné a právne kritériá. Súčasťou tejto analýzy by malo byť aj posúdenie rizík spojených s prevádzkou systému, závislosťou od konkrétnych technológií, dostupnosťou náhradných komponentov a schopnosťou zabezpečiť dlhodobú podporu riešenia.

Osobitnú pozornosť je potrebné venovať návrhu zmluvného modelu. IoT projekty spravidla nezahŕňajú iba dodávku zariadení, ale aj poskytovanie súvisiacich služieb, cloudovej infraštruktúry, konektivity, aktualizácií firmvéru, technickej podpory a bezpečnostných služieb. Dodávateľ by mal preto jasne definovať rozsah poskytovaných služieb, spôsob ich poskytovania, parametre úrovne služieb (SLA), reakčné časy pri incidentoch, dostupnosť systému, pravidlá údržby a spôsob riešenia prevádzkových problémov.

Významnou súčasťou tejto fázy je aj návrh modelu správy dát a prístupových práv. Dodávateľ by mal transparentne definovať, aké údaje bude systém spracúvať, kde budú údaje uchovávané, kto bude mať k údajom prístup a akým spôsobom budú zabezpečené ich integrita, dôvernosť a dostupnosť. Ak riešenie zahŕňa spracúvanie osobných údajov, musí byť

už v tejto fáze zrejmé, aké úlohy bude dodávateľ vykonávať a či bude vystupovať ako sprostredkovateľ alebo v inom právnom postavení podľa GDPR.

Dodávateľ by mal zároveň navrhnúť riešenie tak, aby minimalizoval riziko vendor lock-in. Verejní obstarávatelia čoraz častejšie požadujú otvorené štandardy, dokumentované API, možnosť exportu dát, interoperabilitu s inými systémami a jasne definované podmienky migrácie riešenia. Súčasťou návrhu by preto mala byť aj dokumentácia integračných rozhraní, opis dátových formátov, podmienky odovzdania technickej dokumentácie a mechanizmy umožňujúce budúcu zmenu dodávateľa bez neprimeraných nákladov alebo straty údajov.

Neoddeliteľnou súčasťou prípravy ponuky je aj zohľadnenie požiadaviek kybernetickej bezpečnosti. Dodávateľ by mal preukázať, akým spôsobom budú zariadenia chránené pred neoprávneným prístupom, ako bude zabezpečená autentifikácia používateľov, šifrovanie komunikácie, správa aktualizácií, monitorovanie incidentov a riešenie zraniteľností počas celej životnosti systému. Ak je riešenie určené pre prostredie kritickej alebo významnej infraštruktúry, je potrebné počítať aj s dodatočnými regulačnými požiadavkami vyplývajúcimi z právnych predpisov upravujúcich kybernetickú bezpečnosť.

V prípade, že navrhované riešenie obsahuje prvky umelej inteligencie, dodávateľ musí posúdiť aj súlad riešenia s požiadavkami vyplývajúcimi z Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 o umelej inteligencii (AI Act). Súčasťou prípravy ponuky by malo byť identifikovanie úlohy systému umelej inteligencie v rámci riešenia, posúdenie prípadnej klasifikácie systému, identifikácia požiadaviek na transparentnosť, dokumentáciu a dohľad človeka nad systémom.

Výstupom tejto fázy by mala byť komplexná ponuka, ktorá nielen spĺňa formálne požiadavky verejného obstarávania, ale zároveň preukazuje schopnosť dodávateľa zabezpečiť dlhodobú, bezpečnú a právne udržateľnú prevádzku IoT riešenia vo verejnom sektore.

FÁZA 3: PILOTNÉ TESTOVANIE IOT RIEŠENIA A OVERENIE SPOĽAHLIVOSTI SYSTÉMU

Po úspešnom výbere vo verejnom obstarávaní a uzatvorení zmluvného vzťahu vstupuje dodávateľ do fázy pilotného testovania riešenia. Cieľom tejto etapy nie je iba preukázanie technickej funkčnosti jednotlivých komponentov, ale predovšetkým overenie, že navrhované IoT riešenie je schopné spoľahlivo fungovať v konkrétnom prevádzkovom prostredí verejného obstarávateľa. Pilotné testovanie predstavuje kľúčový moment, v ktorom sa teoretické predpoklady návrhu konfrontujú s reálnymi podmienkami nasadenia a v ktorom sa odhaľujú potenciálne technické, prevádzkové, bezpečnostné a právne riziká.

Dodávateľ musí zabezpečiť, aby pilotné testovanie prebiehalo podľa vopred definovanej metodiky a aby boli jasne stanovené kritériá úspešnosti jednotlivých testov. Už pred začatím pilotnej prevádzky by mali byť určené merateľné ukazovatele výkonnosti systému, spôsob ich vyhodnocovania a postup pri identifikácii a odstraňovaní zistených nedostatkov. Súčasťou

pilotného projektu by mala byť aj dokumentácia všetkých vykonaných testov, ich výsledkov a prijatých nápravných opatrení.

Osobitnú pozornosť musí dodávateľ venovať overeniu funkčnosti fyzických zariadení a senzorov. V rámci pilotu je potrebné preveriť presnosť merania, stabilitu výstupov, spoľahlivosť komunikácie medzi zariadeniami, odolnosť voči vonkajším vplyvom, kvalitu prenosu dát a schopnosť systému reagovať na prevádzkové výpadky alebo neštandardné situácie. Dodávateľ by mal zároveň overiť správnosť konfigurácie zariadení, kvalitu ich kalibrácie a dlhodobú stabilitu prevádzky pri rôznych prevádzkových podmienkach.

Ak riešenie zahŕňa analytické alebo rozhodovacie mechanizmy, je potrebné vykonať aj audit kvality údajov a správnosti analytických výstupov. Dodávateľ by mal preukázať, že systém dokáže identifikovať chybné, neúplné alebo nedôveryhodné údaje a že disponuje mechanizmami na zabránenie vzniku nesprávnych alebo zavádzajúcich výstupov. V prípade systémov využívajúcich algoritmy umelej inteligencie alebo pokročilú analytiku je potrebné preveriť aj transparentnosť fungovania modelov, reprodukovateľnosť výsledkov a schopnosť spätne vysvetliť, na základe akých vstupov alebo parametrov bol vytvorený konkrétny výstup.

Dodávateľ by mal v rámci pilotnej prevádzky osobitne testovať aj bezpečnostné aspekty riešenia. Súčasťou overovania by mala byť kontrola autentifikačných mechanizmov, správy používateľských oprávnení, šifrovania komunikácie, integrity prenášaných údajov, logovania udalostí a schopnosti systému odolávať bežným kybernetickým hrozbám. Ak to povaha riešenia vyžaduje, je vhodné vykonať aj bezpečnostné testovanie alebo penetračné testy zamerané na identifikáciu potenciálnych zraniteľností.

V prípade, že systém spracúva osobné údaje alebo môže mať dopad na práva a slobody fyzických osôb, mal by dodávateľ počas pilotného testovania priebežne overovať aj súlad navrhovaného riešenia s požiadavkami ochrany osobných údajov. Praktické skúsenosti získané počas pilotu môžu totiž odhaliť nové dátové toky, prevádzkové scenáre alebo riziká, ktoré nebolo možné identifikovať v prípravnej fáze projektu.

Pilotné testovanie nesmie byť chápané ako neobmedzený experiment. Dodávateľ by mal zabezpečiť, aby rozsah testovania, účel spracúvania údajov, okruh zapojených subjektov a doba trvania pilotu boli jasne vymedzené a zodpovedali podmienkam dohodnutým s verejným obstarávateľom. Výstupom tejto fázy by malo byť preukázanie pripravenosti riešenia na prechod do produkčnej prevádzky a odstránenie všetkých identifikovaných nedostatkov, ktoré by mohli negatívne ovplyvniť jeho bezpečnosť, spoľahlivosť alebo právnu udržateľnosť.

FÁZA 4: PREVÁDZKA, PODPORA A TRANSFER KNOW-HOW PRI IOT EKOSYSTÉME

Po úspešnom ukončení pilotného testovania a nasadení riešenia do produkčnej prevádzky vstupuje dodávateľ do najdlhšej a z hľadiska dlhodobej zodpovednosti najnáročnejšej fázy životného cyklu IoT projektu. V tejto etape už nie je primárnym cieľom vývoj alebo implementácia systému, ale zabezpečenie jeho stabilnej, bezpečnej a dlhodobo udržateľnej prevádzky v prostredí verejného sektora. Práve počas prevádzky sa ukazuje, či je riešenie schopné plniť svoj účel nielen technicky, ale aj organizačne, bezpečnostne a právne.

Dodávateľ musí zabezpečiť nepretržitý monitoring systému a priebežne vyhodnocovať jeho funkčnosť, dostupnosť a výkonnosť. Monitoring by nemal byť obmedzený iba na technickú prevádzku centrálnej platformy, ale mal by zahŕňať aj stav jednotlivých zariadení, kvalitu merania, správnosť komunikácie medzi komponentmi, dostupnosť dátových tokov, kvalitu logovania a schopnosť systému reagovať na prevádzkové udalosti. Priebežné sledovanie prevádzky umožňuje včas identifikovať vznikajúce problémy a predchádzať ich negatívnym dôsledkom na fungovanie systému.

Neoddeliteľnou súčasťou prevádzky je aj zabezpečovanie aktualizácií, opráv chýb a odstraňovania zraniteľností. Dodávateľ by mal disponovať procesmi umožňujúcimi pravidelnú aktualizáciu firmvéru zariadení, softvérových komponentov, komunikačných modulov a bezpečnostných mechanizmov. Osobitnú pozornosť je potrebné venovať zraniteľnostiam, ktoré môžu vzniknúť v dôsledku technologického vývoja alebo objavenia nových kybernetických hrozieb. Súčasťou zodpovednosti dodávateľa by preto malo byť aj priebežné monitorovanie bezpečnostnej situácie a prijímanie primeraných opatrení na ochranu systému.

Počas prevádzky musí dodávateľ priebežne vyhodnocovať aj kvalitu spracúvaných údajov. Pri IoT riešeniach môže v dôsledku opotrebenia zariadení, zmien prostredia alebo neaktuálnej kalibrácie dochádzať k postupnému znižovaniu presnosti merania. Dodávateľ by preto mal zabezpečiť pravidelné kontroly funkčnosti zariadení, opätovnú kalibráciu senzorov, overovanie správnosti dát a identifikáciu anomálií, ktoré by mohli ovplyvniť dôveryhodnosť výstupov systému.

Ak riešenie obsahuje analytické alebo AI komponenty, je potrebné priebežne sledovať aj ich výkonnosť a správanie. Dodávateľ by mal monitorovať, či nedochádza k poklesu presnosti modelov, vzniku systematických odchýlok alebo neočakávaných výsledkov spôsobených zmenami vstupných údajov. V prípade systémov využívajúcich umelú inteligenciu je vhodné pravidelne preverovať aj transparentnosť fungovania modelov, možnosť vysvetlenia výsledkov a súlad s regulačnými požiadavkami počas celého obdobia prevádzky.

Osobitne významnou povinnosťou dodávateľa je zabezpečenie transferu know-how na verejného obstarávateľa. Dodávateľ by nemal vytvárať stav, v ktorom je verejný subjekt dlhodobo odkázaný výlučne na jeho odborné znalosti alebo technické kapacity. Súčasťou

projektu by preto malo byť systematické odovzdávanie dokumentácie, školení, prevádzkových postupov a technických informácií potrebných na pochopenie fungovania riešenia. Verejný obstarávateľ by mal byť schopný porozumieť základnej architektúre systému, princípom jeho fungovania, spôsobu správy zariadení, interpretácii údajov a postupom pri riešení prevádzkových alebo bezpečnostných incidentov.

Dodávateľ by mal zároveň počas celej doby prevádzky podporovať interoperabilitu a predchádzať vzniku neprimeranej závislosti verejného obstarávateľa od konkrétnej technológie alebo dodávateľa. To zahŕňa zachovanie prístupu k dátam, poskytovanie dokumentovaných API, priebežnú aktualizáciu technickej dokumentácie a zabezpečenie podmienok umožňujúcich budúcu migráciu riešenia alebo jeho prevzatie iným subjektom.

Výstupom tejto fázy by nemala byť iba technicky funkčná prevádzka systému, ale aj vytvorenie podmienok pre jeho dlhodobú udržateľnosť, bezpečný rozvoj a efektívne využívanie vo verejnom sektore bez vzniku technologickej alebo organizačnej závislosti od konkrétneho dodávateľa.

4. IDENTIFIKÁCIA KĽÚČOVÝCH RIZÍK

4.1. PRÁVNE RIZIKÁ PRI IOT RIEŠENIACH VO VEREJNOM SEKTORE

Dodávateľ IoT riešení pre verejný sektor musí už v počiatočných fázach projektu identifikovať a riadiť viaceré právne riziká, ktoré môžu ovplyvniť úspešnosť implementácie, prevádzku systému aj jeho súlad s právnymi predpismi. Špecifikom IoT projektov je skutočnosť, že technické možnosti riešenia často presahujú rámec toho, čo je z právneho hľadiska prípustné alebo primerané. Právne riziká preto nevznikajú až počas prevádzky systému, ale často už pri jeho návrhu a architektonickom nastavení.

Prvým významným rizikom je navrhnutie riešenia, ktorého fungovanie predpokladá rozsah zberu údajov alebo monitorovania, ktorý nemusí byť v konkrétnom prostredí verejnej správy právne obhájiteľný. Dodávateľ musí už pri návrhu systému zohľadňovať nielen technické požiadavky verejného obstarávateľa, ale aj právny rámec, v ktorom bude riešenie používané. Riziko vzniká najmä v prípadoch, keď systém umožňuje sledovanie pohybu osôb, monitorovanie správania používateľov verejných služieb alebo vytváranie detailných dátových profilov bez dostatočného právneho základu alebo bez primeraného obmedzenia rozsahu spracúvaných údajov.

Významným právnym rizikom je aj nesprávne posúdenie požiadaviek na ochranu osobných údajov. IoT riešenia často spracúvajú údaje, ktoré umožňujú priamu alebo nepriamu identifikáciu fyzických osôb, a to aj v prípadoch, keď identifikácia nie je primárnym cieľom systému. Dodávateľ by preto mal už v návrhovej fáze posúdiť, či navrhované riešenie vyžaduje vykonanie posúdenia vplyvu na ochranu osobných údajov (DPIA), aké kategórie údajov budú spracúvané, aké budú účely spracúvania a aké technické a organizačné opatrenia budú potrebné na zabezpečenie súladu s požiadavkami GDPR. Podcenenie týchto aspektov môže viesť nielen k právnym problémom na strane verejného obstarávateľa, ale aj k zmluvným, reputačným a obchodným dôsledkom pre dodávateľa.

Ďalším významným rizikom je postupné funkčné rozširovanie systému nad rámec pôvodne definovaného účelu. Dodávateľ musí počítať s tým, že údaje získavané prostredníctvom IoT infraštruktúry môžu byť pre verejného obstarávateľa atraktívne aj na ďalšie využitie. Ak však systém nie je navrhnutý s dostatočnými obmedzeniami alebo kontrolnými mechanizmami, môže vzniknúť riziko, že bude používaný na účely, ktoré neboli pôvodne predpokladané alebo právne posúdené. Takéto rozširovanie funkcionality môže viesť k porušeniu princípov účelového viazania údajov, proporcionality alebo zákonnosti spracúvania.

Osobitne závažným právnym rizikom je vytvorenie riešenia, ktorého výstupy môžu byť využívané pri rozhodovacích, kontrolných alebo sankčných procesoch bez primeranej transparentnosti a možnosti preskúmania. Ak systém využíva automatizované pravidlá, pokročilú analytiku alebo prvky umelej inteligencie na identifikáciu rizikových situácií, podozrivého správania alebo priorít zásahu, dodávateľ musí zabezpečiť, aby boli výstupy

systému dostatočne vysvetliteľné, overiteľné a podliehali primeranému ľudskému dohľadu. V opačnom prípade môže vzniknúť riziko, že výkon verejnej moci bude fakticky ovplyvňovaný technickým mechanizmom bez dostatočnej právnej kontroly.

Ak navrhované riešenie obsahuje komponenty umelej inteligencie, dodávateľ musí zároveň zohľadniť aj regulačné požiadavky vyplývajúce z AI Act. Rizikom môže byť nesprávna klasifikácia systému, absencia požadovanej technickej dokumentácie, nedostatočné riadenie rizík, chýbajúce mechanizmy ľudského dohľadu alebo nedostatočná transparentnosť fungovania modelov. Tieto nedostatky môžu významne ovplyvniť možnosť nasadenia riešenia vo verejnom sektore.

4.2. TECHNICKÉ A EKONOMICKÉ RIZIKÁ IOT INFRAŠTRUKTÚRY

Dodávateľ IoT riešenia musí už v návrhovej fáze zohľadňovať aj technické a ekonomické riziká, ktoré môžu ovplyvniť dlhodobú prevádzku systému a jeho životaschopnosť vo verejnom sektore. Jednou z najčastejších chýb býva sústredenie pozornosti výlučne na funkčnosť riešenia alebo na úspešné absolvovanie pilotného testovania bez dostatočného posúdenia nákladov a prevádzkových požiadaviek počas celého životného cyklu systému.

Významným rizikom je nesprávne odhadnutie životnosti zariadení a nárokov na ich údržbu. Dodávateľ by mal už pri návrhu riešenia zohľadniť prevádzkové podmienky, odolnosť zariadení voči vonkajším vplyvom, dostupnosť náhradných dielov, možnosti servisných zásahov a predpokladané náklady na obnovu alebo výmenu jednotlivých komponentov. Zariadenia, ktoré fungujú spoľahlivo počas pilotnej prevádzky, nemusia automaticky zabezpečiť rovnakú úroveň spoľahlivosti počas niekoľkoročnej prevádzky vo verejnom priestore.

Dôležitým technicko-ekonomickým rizikom je aj podcenenie nákladov na konektivitu, cloudové služby, prevádzkové licencie, bezpečnostné aktualizácie a technickú podporu. Dodávateľ by mal byť schopný transparentne vyhodnotiť celkové náklady životného cyklu riešenia a zohľadniť ich pri návrhu obchodného modelu. V opačnom prípade môže dôjsť k situácii, keď sa riešenie stane ekonomicky neudržateľným alebo keď budú dodatočné náklady významne prevyšovať pôvodné očakávania verejného obstarávateľa.

Osobitným technicko-ekonomickým rizikom je vznik vendor lock-in, teda neprimeranej závislosti verejného obstarávateľa od konkrétneho dodávateľa, výrobcu alebo technologickej platformy. Takáto situácia vzniká najmä v prípadoch, keď je riešenie založené na proprietárnych komunikačných protokoloch, uzavretých dátových modeloch, neštandardizovaných integračných mechanizmoch alebo technológiách, ktoré neumožňujú jednoduchú migráciu údajov a systémov. Dodávateľ by mal preto už pri návrhu riešenia podporovať využívanie otvorených štandardov, interoperabilných rozhraní a mechanizmov umožňujúcich budúcu integráciu alebo migráciu.

Riziko vendor lock-in sa významne zvyšuje v prípadoch, keď riešenie neobsahuje dokumentované API, neumožňuje export údajov v štandardizovaných formátoch alebo neposkytuje dostatočnú technickú dokumentáciu integračných rozhraní. Nedostatočná interoperabilita môže výrazne obmedziť možnosti ďalšieho rozvoja riešenia a negatívne ovplyvniť jeho dlhodobú využiteľnosť vo verejnom sektore.

Významným technickým rizikom je aj podcenenie požiadaviek kybernetickej bezpečnosti. IoT infraštruktúra pozostáva z veľkého množstva zariadení, komunikačných kanálov a integračných prvkov, ktoré môžu predstavovať potenciálne vstupné body pre kybernetické útoky. Dodávateľ musí zabezpečiť primeranú úroveň ochrany zariadení, šifrovanie komunikácie, správu identít a prístupových práv, monitorovanie bezpečnostných udalostí a pravidelné aktualizácie bezpečnostných mechanizmov. Nedostatočne zabezpečené riešenie môže viesť k strate dôvery verejného obstarávateľa, prevádzkovým výpadkom, kompromitácii údajov alebo k vzniku významných finančných škôd.

Dôležitým technickým rizikom je aj neškálovateľnosť riešenia. Dodávateľ musí počítať s tým, že úspešný pilotný projekt môže byť v budúcnosti rozšírený na výrazne väčší počet zariadení, lokalít alebo používateľov. Ak architektúra systému neumožňuje efektívne spracovanie rastúceho objemu dát, integráciu s ďalšími informačnými systémami alebo adaptáciu na nové komunikačné technológie, môže sa riešenie stať technologicky alebo ekonomicky neudržateľným ešte pred dosiahnutím očakávaných prínosov projektu.

Úspešný dodávateľ IoT riešení by preto mal už v návrhovej fáze pristupovať k riadeniu rizík ako k neoddeliteľnej súčasti architektúry systému. Identifikácia právnych, technických, bezpečnostných a ekonomických rizík nesmie byť jednorazovou aktivitou vykonanou pred predložením ponuky, ale kontinuálnym procesom sprevádzajúcim celý životný cyklus projektu od návrhu riešenia až po jeho dlhodobú prevádzku.

5. ZÁVER A ZHRNUTIE KĽÚČOVÝCH ODPORÚČANÍ

Internet vecí predstavuje v súčasnej fáze digitalizácie verejnej správy a územnej samosprávy jednu z najvýznamnejších technologických oblastí, prostredníctvom ktorých sa fyzické procesy verejných služieb premieňajú na dátovo podporované a digitálne koordinované prostredie. Pre technologické a softvérové spoločnosti však IoT nepredstavuje iba príležitosť na dodávku nových technológií, ale aj zvýšenú mieru zodpovednosti za spôsob, akým budú tieto technológie vplývať na fungovanie verejnej správy, spracúvanie údajov, bezpečnosť infraštruktúry a výkon verejných úloh. Úspešné IoT riešenie vo verejnom sektore preto nemožno hodnotiť iba podľa jeho technických parametrov alebo ekonomických prínosov, ale aj podľa jeho právnej udržateľnosti, bezpečnosti, transparentnosti a schopnosti fungovať v prostredí verejnej správy.

Základným metodickým východiskom pre dodávateľa musí byť skutočnosť, že IoT nie je iba technickou sieťou zariadení, ale prostredím, ktoré podlieha viacerým regulačným režimom. Každý senzor, komunikačný modul, dátové úložisko, integračné rozhranie alebo analytická vrstva môžu vstupovať do oblasti ochrany osobných údajov, kybernetickej bezpečnosti, regulácie informačných technológií vo verejnej správe, verejného obstarávania alebo regulácie umelej inteligencie. Dodávateľ preto musí už od začiatku navrhovať riešenie tak, aby právna, bezpečnostná a procesná zhoda bola prirodzenou súčasťou architektúry systému, a nie dodatočne riešenou formalitou po ukončení vývoja.

Pri návrhu riešení určených pre verejný sektor by mali technologické a softvérové spoločnosti vychádzať z princípov otvorenosti, interoperability, auditovateľnosti a prenositeľnosti. IoT riešenie by malo využívať štandardizované alebo otvorené dátové formáty, dokumentované API, transparentné integračné mechanizmy a architektúru umožňujúcu budúce rozširovanie alebo migráciu systému. Dodávateľ by mal zároveň minimalizovať riziko vzniku vendor lock-in a vytvárať podmienky, ktoré umožnia verejnému partnerovi zachovať kontrolu nad dátami, konfiguráciami, dokumentáciou a prevádzkou systému počas celej doby jeho životnosti.

Osobitnú pozornosť je potrebné venovať ochrane osobných údajov a spracúvaniu dát. Dodávateľ musí už v návrhovej fáze dôsledne posudzovať rozsah zbieraných údajov, ich nevyhnutnosť, frekvenciu spracúvania, dobu uchovávania a účel využitia. Pri riešeniach, ktoré pracujú s lokalizačnými údajmi, monitorovaním verejného priestoru, identifikáciou osôb alebo analytickými mechanizmami s dopadom na jednotlivcov, je potrebné počítať s prísnejšími požiadavkami ochrany osobných údajov, vrátane možnej potreby vykonania posúdenia vplyvu na ochranu osobných údajov (DPIA) a implementácie dodatočných bezpečnostných opatrení.

Rovnako dôležitou oblasťou je kybernetická bezpečnosť. IoT riešenia určené pre verejný sektor musia byť navrhované s predpokladom dlhodobej prevádzky v prostredí zvýšeného bezpečnostného rizika. Dodávateľ musí zabezpečiť ochranu zariadení pred neoprávneným

prístupom, šifrovanie komunikácie, bezpečnú správu identít a prístupových oprávnení, riadenie aktualizácií, monitorovanie bezpečnostných udalostí a efektívne riešenie incidentov. Súčasťou návrhu by mali byť aj mechanizmy umožňujúce auditovanie, logovanie a spätné preverovanie činnosti systému.

Ak riešenie obsahuje prvky umelej inteligencie alebo pokročilej analytiky, dodávateľ musí zohľadniť aj požiadavky vyplývajúce z regulácie umelej inteligencie. Systémy využívajúce algoritmické rozhodovanie alebo automatizované vyhodnocovanie údajov musia byť navrhnuté transparentne, s možnosťou vysvetlenia výstupov, primeraným ľudským dohľadom a dokumentáciou umožňujúcou preukázať súlad s požiadavkami AI Actu.

Mimoriadne dôležité je zachovať rozdiel medzi technologickou podporou verejných procesov a výkonom verejnej moci. Dodávateľ musí pri návrhu riešenia počítať s tým, že IoT systém môže podporovať rozhodovanie, monitorovanie alebo správu verejných služieb, nesmie však vytvárať stav, v ktorom by technologický systém fakticky nahrádzal zákonom predpokladané rozhodovanie a zodpovednosť orgánov verejnej moci. Zariadenia, dáta a algoritmy môžu verejnú správu podporovať a zefektívňovať, no nesmú nahradiť zákonnosť, preskúmateľnosť, proporcionalitu a ľudskú zodpovednosť za výkon verejných úloh.

Významnou súčasťou zodpovedného prístupu dodávateľa je aj transfer know-how a zabezpečenie dlhodobej prevádzkovej udržateľnosti riešenia. Dodávateľ by nemal vytvárať prostredie, v ktorom je verejný partner odkázaný výlučne na jeho odborné znalosti alebo technické kapacity. Súčasťou projektu by preto mala byť kvalitná technická dokumentácia, zrozumiteľný opis architektúry systému, dokumentované integračné rozhrania, školenia používateľov a administrátorov, ako aj jasne definované procesy prevádzky, údržby a budúcej migrácie riešenia.

Z pohľadu budúceho vývoja možno očakávať ďalší rast významu IoT riešení v oblastiach dopravy, energetiky, environmentálneho monitoringu, správy verejného priestoru, budov, školstva a sociálnych služieb. Technologické spoločnosti, ktoré budú schopné ponúknuť riešenia spájajúce technickú kvalitu s právnou, bezpečnostnou a etickou udržateľnosťou, budú mať významnú konkurenčnú výhodu. Dlhodobý úspech IoT riešení vo verejnom sektore totiž nebude závisieť iba od počtu nasadených zariadení alebo rozsahu zbieraných dát, ale predovšetkým od schopnosti dodávateľa vytvárať technológie, ktoré sú bezpečné, transparentné, kontrolovateľné a kompatibilné s princípmi demokratickej a zákonnej verejnej správy.

6. MANAŽÉRSKE ZHRNUTIE

Mestá, obce a orgány verejnej správy po celom Slovensku prechádzajú od čiastkovej digitalizácie úradov k budovaniu komplexných dátových ekosystémov. Implementácia technológií Internetu vecí (Internet of Things – IoT), inteligentných senzorických sietí, pokročilej dátovej analytiky a algoritmických systémov (vrátane umelej inteligencie) už nepredstavuje len technologické vylepšenie, ale stáva sa kľúčovou súčasťou fyzickej a digitálnej infraštruktúry miest a štátu.

Smart osvetlenie, environmentálny monitoring, inteligentné riadenie dopravy či automatizované odpadové hospodárstvo prinášajú obrovský potenciál pre zefektívnenie verejných služieb. Tento posun si však vyžaduje zásadnú zmenu vnímania: nasadenie IoT systémov vo verejnom sektore nie je bežným nákupom tovaru ani výlučne technickým projektom. Ide o vytvorenie novej právnej, bezpečnostnej a prevádzkovej reality, ktorá priamo zasahuje do výkonu verejnej moci, nakladania s verejnými zdrojmi a dodržiavania základných práv občanov.

Hlavným cieľom predloženého metodického rámca je poskytnúť samosprávam, orgánom štátnej správy a ich zmluvným dodávateľom jasný, právne záväzný a prakticky aplikovateľný návod. Tento sprievodca eliminuje hlavné riziká spojené s dodávkami moderných technológií – najmä nezákonné spracúvanie dát, kybernetické zraniteľnosti, technologickú závislosť od jediného dodávateľa (*vendor lock-in*) a stratu ľudskej kontroly nad rozhodovaním.

ŠTYRI PILIERE REGULAČNÉHO A PRÁVNEHO RÁMCA

Každý IoT projekt vo verejnom sektore musí od prvej fázy plánovania stáť na štyroch právnych a procesných pilieroch. Ignorovanie ktoréhokoľvek z nich vedie k zmareniu investícií, finančným sankciám alebo právnym sporom.

Pilier 1:
Najväčším ekonomickým a prevádzkovým rizikom pri obstarávaní smart technológií je vytvorenie technologickej závislosti od jediného dodávateľa (*Vendor Lock-in*). Ak samospráva nakúpi uzatvorený, proprietárny systém, stáva sa rukojemníkom jedného výrobcu. Akákoľvek budúca úprava, servis, výmena senzorov alebo rozšírenie systému sa stáva extrémne nákladnou alebo technicky nemožnou. Kľúčové pravidlá pre obstarávanie:

- **Obstarávanie cez funkčné parametre:** Predmet zákazky sa musí v zmysle zákona č. 343/2015 Z. z. o verejnom obstarávaní definovať výhradne cez očakávané funkčné, prevádzkové a výkonnostné výsledky, nie cez odkaz na konkrétne značky či patentované technológie.
- **Otvorené štandardy a otvorené API:** Zmluvné podmienky musia bezpodmienečne vyžadovať podporu medzinárodných otvorených protokolov a poskytnutie plne zdokumentovaného, bezplatného otvoreného rozhrania pre programovanie aplikácií (API).
- **Vlastníctvo dát a Exit stratégia:** Všetky zozbierané a vygenerované dáta sú výhradným vlastníctvom orgánu verejnej moci. Dodávateľ k nim nezískava majetkové ani autorské práva. Zmluva musí od prvého dňa obsahovať záväzný Exit plán ako povinnosť dodávateľa pri ukončení zmluvy odovzdať databázy, prístupové kľúče a poskytnúť plnú súčinnosť pri migrácii na nového dodávateľa.

Pilier 2:
V praxi sa často vyskytuje omyl, že ak IoT systém zbiera len fyzikálne veličiny (napr. intenzitu dopravy či obsadenosť parkoviska), ochrana osobných údajov sa naň nevzťahuje. Ak je však možné akúkoľvek dátovú stopu prepojiť s konkrétnou fyzickou osobou, ide o spracúvanie osobných údajov podľa Nariadenia GDPR. Povinné opatrenia pri práci s dátami:

- **Zásada Data Protection by Design and Default:** Ochrana súkromia musí byť zabudovaná priamo do architektúry systému. Ak je to technicky možné, anonymizácia a agregácia dát sa musí vykonávať priamo na koncovom zariadení (*Edge Computing*) a zo senzora smú odchádzať len anonymné metadáta.
- **Povinné Posúdenie vplyvu na ochranu údajov (DPIA):** Pred spustením systémov s vyšším rizikom (napr. kamerové senzory, monitoring mobility) je orgán verejnej moci povinný vypracovať DPIA podľa čl. 35 GDPR.
- **Právny základ a sprostredkovateľské zmluvy:** Plošný monitoring verejného priestoru nemožno zakladať na súhlase občanov, ale výhradne na plnení úloh vo verejnom záujme alebo pri výkone verejnej moci (čl. 6 ods. 1 písm. e GDPR). S dodávateľom musí byť uzavretá prísna sprostredkovateľská zmluva podľa čl. 28 GDPR, zakazujúca využitie dát na vlastné komerčné účely či trénovanie vlastných AI modelov.

Pilier 3:
Na rozdiel od bežných IT serverov bežne uložených v zamknutých serverovniach sú IoT senzory a komunikačné uzly fyzicky umiestnené vo verejnom priestore (na stĺpoch osvetlenia, cestách, budovách). Sú tak vystavené nielen poveternostným vplyvom, ale aj fyzickému vandalizmu a kybernetickým útokom. Každý senzor predstavuje potenciálnu vstupnú bránu do celej mestskej alebo štátnej IT siete. Štandardy bezpečnosti (Zákon č. 69/2018 Z. z. a Zákon č. 95/2019 Z. z.):

- **Identity zariadení a šifrovanie:** Každé zariadenie musí mať unikátnu kryptografickú identitu. Používanie továrenských/univerzálnych hesiel je prísne zakázané. Celá komunikácia musí byť šifrovaná na koncovej úrovni (*End-to-End Encryption*).
- **Bezpečná správa aktualizácií (OTA):** Dodávateľ musí garantovať bezpečný, kryptograficky overovaný mechanizmus vzdialenej aktualizácie firmvéru počas celého životného cyklu zariadenia.
- **Kontrolná kapacita a incidenty:** Orgán verejnej moci si musí zachovať priamy prístup k bezpečnostným a prevádzkovým logom. Dodávateľ je povinný hlásiť akýkoľvek bezpečnostný incident najneskôr do 12 hodín. Pred ostrým spustením je povinný nezávislý bezpečnostný audit a penetračné testovanie.

Pilier 4:
Nasadzovanie pokročilých algoritmických systémov a prvkov umelej inteligencie podlieha Európskemu aktu o umelej inteligencii (EU AI Act). Vo verejnej správe platia striktné etické a právne limity. Kľúčové princípy:

- **Zákaz nezákonných praktík:** Je prísne zakázané nasadzovať systémy na sociálne obodovávanie občanov (*social scoring*), nekontrolovanú plošnú biometrickú identifikáciu či systémy manipulujúce správanie obyvateľov.

- **Zásada Human-in-the-Loop:** Žiadny autonómny algoritmický systém nesmie sám vydávať právne akty, ukladať pokuty alebo obmedzovať práva občanov. Výstupy AI majú vždy len odporúčací a podporný charakter. Konečné rozhodnutie a plnú právnu zodpovednosť musí vždy niesť oprávnená fyzická osoba (zamestnanec úradu).

ŽIVOTNÝ CYKLUS IMPLEMENTÁCIE IOT PROJEKTU

Realizácia úspešného IoT projektu v podmienkach verejnej správy sa opiera o štruktúrovaný 4-fázový proces:

1. **Fáza 1: Prípravná a architektonická fáza**
    - Identifikácia reálneho mestského/procesného problému (nenakupovať technológiu pre technológiu).
    - Spracovanie analýzy dátových tokov a posúdenia DPIA.
    - Stanovenie rozpočtu TCO (Celkových nákladov na vlastníctvo) a formulácia funkčnej špecifikácie.
2. **Fáza 2: Obstarávacia a zmluvná fáza**
    - Vyhlásenie transparentného verejného obstarávania založeného na otvorených štandardoch.
    - Uzatvorenie zmluvy o diele, zmluvy o spracúvaní osobných údajov a Dohody o úrovni služieb (SLA) s garanciou dostupnosti (min. 99,5 %) a sankciami.
    - Zmluvné ukotvenie 100% vlastníctva dát, otvorených API a Exit plánu.
3. **Fáza 3: Pilotná a akceptačná fáza**
    - Nasadenie v reálnom prostredí na malej vzorke/území po dobu 3 až 6 mesiacov.
    - Overenie presnosti meraní, stabilita konektivity a odolnosť voči výpadkom.
    - Vykonanie nezávislého bezpečnostného auditu a penetračných testov.
4. **Fáza 4: Prevádzková fáza a transfer know-how**
    - Spustenie do plnej prevádzky a odovzdanie kompletnej prevádzkovej dokumentácie.
    - Zaškolenie interných zamestnancov na zaistenie nezávislosti od dodávateľa.
    - Nastavenie plánu pravidelnej re-kalibrácie senzorov na zabránenie tichej degradácii dát (*Data Drift*).

EKONOMICKÁ UDRŽATEĽNOSŤ A SPRÁVA ŽIVOTNÉHO CYKLUS

Najčastejšou manažérskou chybou pri plánovaní smart investícií je posudzovanie projektu len na základe obstarávacej ceny hardvéru. Nákup senzorov a základného softvéru predstavuje spravidla len 30 % celkových nákladov, pričom orgán verejnej moci je povinný vyhodnocovať Celkové náklady na vlastníctvo ako:

- Obstarávaciu cenu hardvéru a vývoj aplikácií.
- Pravidelné poplatky za sieťovú konektivitu (LoRaWAN, NB-IoT, 5G) a cloudové licencie.
- Náklady na výmenu batérií, fyzickú údržbu a pravidelnú re-kalibráciu senzorov.
- Poplatky za bezpečnostný dohľad, priebežné aktualizácie softvéru (*patch management*) a zmluvné SLA.

- Dodávateľ musí zmluvne garantovať dostupnosť náhradných dielov a servisnej podpory po dobu minimálne 7 rokov od odovzdania systému.

CHECKLIST

Projekt a verejné obstarávanie

Oblasť	ZÁVÄZNÉ	ODPORÚČANÉ	AKO RIEŠIŤ
Súťažná neutralita	Špecifikácia nesmie opisovať jeden proprietárny systém bez objektívneho odôvodnenia	Definovať zadanie cez funkčné a výkonové požiadavky	Nepoužívať názvy produktov ani protokolov jedného výrobcu
Vendor lock-in	V zmluve požadovať interoperabilitu, export dát, prístup k logom	Vyžadovať otvorené štandardy a dokumentované API	Zmluvne zakotviť podmienky migrácie a prenositeľnosť konfigurácií
Právne posúdenie	Identifikovať dátové toky a kategórie údajov	Predbežné právne a bezpečnostné posúdenie	Analýza účelu, proporcionality a minimalizácie údajov

Ochrana osobných údajov

Oblasť	ZÁVÄZNÉ	ODPORÚČANÉ	AKO RIEŠIŤ
Právny základ	Každé spracúvanie musí mať zákonný základ a vymedzený účel	Rozlišovať prevádzkový monitoring od monitoringu správania osôb	Právna analýza, či technické dáta nie sú individualizovateľné
Minimalizácia	Zbierať len nevyhnutné údaje; obmedziť frekvenciu, presnosť, dobu uchovávania	Architektonicky oddeliť prevádzkové dáta od údajov zasahujúcich do súkromia	Pseudonymizácia/anonymizácia už na úrovni senzora
DPIA	Vykonať pri vysokom riziku pre práva a slobody osôb	Vypracovať ešte pred nasadením, aktualizovať pri zmene účelu	Zohľadniť celý životný cyklus údajov
Pseudonymizované dáta	Ak je možná spätná identifikácia, GDPR sa uplatní v plnej miere	Dokumentovať, prečo reverzná identifikácia nie je možná	Prístupové práva a opatrenia v architektúre
Informačné povinnosti	Informovať dotknuté osoby v súlade s GDPR	Transparentne označiť senzorické zariadenia vo verejnom priestore	Pripraviť informačné texty a verejné informácie

Kybernetická bezpečnosť

Oblasť	ZÁVÄZNÉ	ODPORÚČANÉ	AKO RIEŠIŤ
Identita a prístup	Správa identít zariadení, autentifikácia, autorizácia	Silné autentifikácie, princíp minimálnej oprávnenosti	Centrálna správa identít, pravidelná revízia oprávnení

Oblasť	ZÁVÄZNÉ	ODPORÚČANÉ	AKO RIEŠIŤ
Šifrovanie	Šifrovanie komunikácie a integrity prenášaných údajov	Šifrovať aj dáta v pokoji (data at rest)	Vybrať protokoly s natívnou end-to-end šifrou (TLS, DTLS)
Aktualizácie	Definovať proces aktualizácií a odstraňovania zraniteľností	Distribuovať aktualizácie overiteľným spôsobom (podpis)	Zmluvne upraviť SLA pre bezpečnostné aktualizácie
Logovanie a audit	Zaznamenávať bezpečnostne relevantné udalosti	Umožniť spätný audit činnosti systému	Centralizovaný log management, definovaná doba uchovávania
Testovanie	Penetračné testy, ak to povaha riešenia vyžaduje	Opakované bezpečnostné testovanie, nielen v pilote	Zahrnúť do zmluvy povinnosť pravidelného testovania

IOT a AI

Oblasť	ZÁVÄZNÉ	ODPORÚČANÉ	AKO RIEŠIŤ
Kontrolná kapacita	Verejný orgán musí mať reálnu kontrolu nad IT vrátane IoT zariadení	Posilniť ju aj nad cloudom a edge vrstvou	Vyhnúť sa riešeniam, kde dodávateľ výlučne kontroluje stav
Audit a export	Verejný subjekt musí byť schopný auditovať a exportovať dáta	Zmluvne garantovať prístup k logom a konfigurácii	Dashboard/SIEM pod kontrolou verejného subjektu
Klasifikácia AI	Identifikovať úlohu AI a posúdiť klasifikáciu podľa AI Act	Začať klasifikáciou už v prípravnej fáze	Záznam o klasifikácii a dokumentácii
Ľudský dohľad	Pri rozhodovacích/kontrolných/sankčných procesoch	AI nesmie fakticky nahradiť zákonné rozhodovanie	Definovať rolu operátora a postup pri spochybnení výstupu

Prevádzka, podpora a transfer know-how

Oblasť	ZÁVÄZNÉ	ODPORÚČANÉ	AKO RIEŠIŤ
Monitoring	Nepretržitý monitoring dostupnosti a výkonnosti	Monitoring aj jednotlivých zariadení, nielen centrálnej platformy	SLA s definovanými reakčnými časmi a eskaláciou
Kalibrácia	Pravidelné kontroly funkčnosti a kalibrácia senzorov	Identifikácia anomálií a trendov znižovania presnosti	Plán údržby s cyklami kalibrácie
Aktualizácie	Pravidelná aktualizácia firmvéru, softvéru, bezpečnostných mechanizmov	Priebežné monitorovanie nových kybernetických hrozieb (CVE)	Proces patch managementu s definovanými oknami

Oblasť	ZÁVÄZNÉ	ODPORÚČANÉ	AKO RIEŠIŤ
Transfer know-how	Odovzdať dokumentáciu, školenia, prevádzkové postupy	Verejný subjekt schopný interpretovať dáta a riešiť incidenty	Plán transferu know-how ako súčasť zmluvy
Interoperabilita	Zachovať prístup k dátam, dokumentované API, aktualizovanú dokumentáciu	Umožniť budúce rozširovanie bez výmeny základnej architektúry	Zmluvné záruky za prenositeľnosť a migráciu

PRÍLOHA Č. 1

CHCEM NIEČO OBSTARAŤ – AKO NA TO?

Jednoduchý prehľad postupu verejného obstarávania

Tento postup vám pomôže zistiť, čo musíte urobiť od identifikácie potreby až po uzavretie zmluvy.

MÔJ CIEĽ
Obstarať tovar, službu alebo stavebné práce v súlade so zákonom, smernicou a princípmi VO.

1 IDENTIFIKUJEM POTREBU

Čo potrebujem obstarať?
Tovar / služba / stavebné práce

Je zákazka v Pláne verejného obstarávania?
- ÁNO → Pokračujem
- NIE → Zdôvodním doplnenie plánu a požiadam o zaradenie

MÁM JASNE DEFINOVANÝ PREDMET ZÁKAZKY?
- ÁNO → pokračujem
- NIE → spresním technické požiadavky (čo, v akom množstve, kvalite, termíne)

2 URČÍM PREDPOKLADANÚ HODNOTU ZÁKAZKY (PHZ)

Odhadnem hodnotu zákazky v € bez DPH

Vzťahuje sa na zákazku niektorá z výnimiek podľa § 1 ZVO?
- ÁNO → Postupujem podľa príslušnej výnimky a zdôvodním ju
- NIE → Pokračujem podľa finančného limitu

3 ZISTÍM, AKÝ POSTUP MUSÍM POUŽIŤ

Podľa predpokladanej hodnoty zákazky (bez DPH)

FINANČNÉ LIMITY SÚ URČENÉ INTERNOU SMERNICOU ORGANIZÁCIE.
Nižšie uvedené limity sú príkladom interného postupu.

DO 3 000 €
PRIAME ZADANIE
- Môžem obstarať priamo u dodávateľa
- Výberiem dodávateľa podľa vlastného uváženia
- Záznam o nákupe (interná evidencia)

3 000 € – 29 999 €
PRIESKUM TRHU
- Oslovím min. 3 dodávateľov
- Písomne alebo elektronicky
- Vyberiem najvhodnejšiu ponuku
- Zápisnica z prieskumu trhu

30 000 € – 49 999 €
PRIESKUM TRHU + ZVEREJNENIE VÝZVY
- Zverejním výzvu na webovom sídle verejného obstarávateľa aspoň 3 pracovné dni
- Oslovím min. 3 dodávateľov (ak to je vzhľadom na predmet zákazky možné)
- Vyberiem najvhodnejšiu ponuku
- Zápisnica + doklad o zverejnení výzvy

OD LIMITU URČENÉHO INTERNOU SMERNICOU
POSTUP PODĽA ZÁKONA O VEREJNOM OBSTARÁVANÍ (realizovaný útvarom VO)
- Formálne verejné obstarávanie podľa zákona a smernice
- Vyhodnotenie ponúk a určenie úspešného uchádzača
- Zmluva / objednávka

NEZABUDNITE
- Zákaz delenia zákaziek
- Zákaz konfliktu záujmov

Dodržiavať princípy: rovnaké zaobchádzanie, nediskriminácia, transparentnosť, proporcionalita, hospodárnosť a efektívnosť.

4 PRÍPRAVA A SCHVÁLENIE

Pripravím požiadavku a zabezpečím schválenie podľa interných pravidiel organizácie.

VYPRACUJEM POŽIADAVKU (predmet, PHZ, zdôvodnenie, kritériá) → ZABEZPEČÍM FINANČNÉ KRYTIE → SCHVÁLIM POŽIADAVKU (oprávnená osoba) → ODOVZDÁM NA REALIZÁCIU (ak realizuje OVO)

5 REALIZÁCIA VEREJNÉHO OBSTARÁVANIA

Postupujem podľa zvoleného postupu.

ZVEREJNENIE / OSLOVENIE DODÁVATEĽOV → PRIJÍMANIE PONÚK → VYHODNOTENIE PONÚK → URČENIE ÚSPEŠNÉHO UCHÁDZAČA → ZÁPISNICA Z VYHODNOTENIA

6 UZAVRETIE ZMLUVY / OBJEDNÁVKY

Uzavriem zmluvu alebo vystavím objednávku.

PODPÍŠEM ZMLUVU alebo vystavím objednávku → ZVEREJNÍM ZMLUVU / OBJEDNÁVKU PODĽA OSOBITNÝCH PREDPISOV (ak sa vyžaduje)

7 PLNENIE A UKONČENIE

Sledujem plnenie a ukončím zákazku.

KONTROLUJEM PLNENIE → PREBERIEM DODÁVKU / SLUŽBU / PRÁCE → ARCHIVUJEM DOKUMENTÁCIU podľa registratúrnych a osobitných predpisov → VYHODNOTÍM A ULOŽÍM REFERENCIE

PRÍKLADY NÁKUPOV, PRI KTORÝCH SA MÔŽE UPLATNIŤ VÝNIMKA PODĽA § 1 ZVO

(nie vždy – posúdenie výnimky musí byť vždy individuálne)

- Reprezentačné účely, darčeky, vecné ceny, kytice
- Pohostenia pri oficiálnych návštevách a podujatiach
- Občerstvenie na porady, konferencie
- Školenia, konferencie, vzdelávanie
- Cestovné lístky, taxi, ubytovanie, prepravné služby
- Poštové služby, notárske služby
- Parkovacie karty, diaľničné poplatky, nájom parkovacích miest
- Správne a súdne poplatky, členské príspevky, poplatky organizáciám

NA ČO SI DAŤ POZOR?

- Nedelite zákazku s cieľom obísť finančný limit.
- Oznámte potenciálny konflikt záujmov ešte pred začiatkom obstarávania.
- Vyhnite sa konfliktu záujmov (oznámte ho a neparticipujte).
- Vždy dokumentujte svoje kroky (zápisnice, ponuky, zverejnenia).
- Dodržiavajte zásady hospodárnosti a efektívnosti.
- Bez písomnej zmluvy/objednávky nevzniká záväzok.

UŽITOČNÉ DOKUMENTY

- Plán verejného obstarávania
- Požiadavka / žiadanka
- Záznam o prieskume trhu
- Zápisnica z vyhodnotenia
- Zmluva / objednávka
- Doklad o zverejnení (ak sa vyžaduje)
- Dokumentácia k zákazke

KTO JE KTO?

JA – GESTOR / OBJEDNÁVATEĽ
Identifikujem potrebu, pripravím podklady pre určenie PHZ, pripravím požiadavku, spolupracujem pri VO, preberám plnenie.

ÚTVAR VO (OVO) / GARANT VO
Poskytuje metodickú podporu, realizuje verejné obstarávanie podľa zákona a smernice.

SCHVAĽOVATEĽ
Schvaľuje požiadavky, zmluvy a iné úkony podľa vnútorných pravidiel organizácie.

PRÁVNY ZÁKLAD

Zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov

Smernica o verejnom obstarávaní

* CRZ = Centrálna registratúra zmlúv vedená Úradom vlády SR – zverejňujú povinné osoby podľa osobitných predpisov.

PRÍLOHA Č. 2

CHCEM SA ZAPOJIŤ DO VEREJNÉHO OBSTARÁVANIA

SPRIEVODCA PRE DODÁVATEĽA – AKO PREBIEHA PROCES

Verejné obstarávanie je transparentný proces, v ktorom majú všetci uchádzači rovnaké podmienky. Tento prehľad vám ukáže, ako sa úspešne zapojiť do súťaže o zákazku.

MÔJ CIEĽ
Získať zákazku férovým a zákonným spôsobom.

1 NÁJDEM VYHLÁSENÚ ZÁKAZKU

Sledujem zverejnené zákazky a vyberiem tú, ktorá zodpovedá mojim možnostiam.

- IS EVO isvo.gov.sk
- Elektronická platforma uvedená vo výzve
- Vestník verejného obstarávania
- TED – európsky portál verejného obstarávania

Vaše zdroje informácií

2 OVERÍM SI PODMIENKY ÚČASTI

Dôkladne si prečítam súťažné podklady a overím, či spĺňam všetky požiadavky.

- Predmet zákazky a jeho rozsah
- Technické požiadavky a špecifikácie
- Kvalifikačné podmienky
- Lehoty a spôsob predkladania ponúk
- Kritériá na vyhodnotenie ponúk
- Zmluvné podmienky
- Požiadavky na plnenie a záruky

2a POTREBUJEM VYSVETLENIE?

Ak niečomu nerozumiem, môžem požiadať o vysvetlenie súťažných podkladov.

- Kladiem otázky včas
- Žiadosť podám cez systém
- Sledujem zverejnené odpovede

3 ROZHODNEM SA, ČI SA ZAPOJÍM

Zhodnotím svoje možnosti a rozhodnem sa, či podám ponuku.

- Spĺňam všetky požiadavky?
- Mám potrebné skúsenosti a kapacity?
- Vieme splniť požadovaný termín a kvalitu?

4 PRIPRAVÍM PONUKU

Vypracujem ponuku v súlade so súťažnými podkladmi a priložím všetky požadované dokumenty.

- Cenová ponuka
- Doklady preukazujúce splnenie podmienok účasti
- Referencie a skúsenosti
- Čestné vyhlásenia
- Technické podklady

Ponuka musí spĺňať požiadavky uvedené v súťažných podkladoch.

5 PODÁM PONUKU ELEKTRONICKY

Ponuku predkladám elektronicky prostredníctvom systému určeného vo výzve alebo súťažných podkladoch.
Najčastejšie ide o IS EVO alebo inú elektronickú platformu.

- Prihlásim sa do systému
- Vyplním požadované formuláre
- Nahrám ponuku a prílohy
- Odošlem najneskôr do uplynutia lehoty

Po uplynutí lehoty nie je možné ponuku zmeniť ani doplniť.

6 KOMUNIKUJEM POČAS HODNOTENIA

Počas obstarávania komunikujem iba prostredníctvom určeného elektronického prostriedku.

- Sledujem otázky a vysvetlenia v systéme
- Na výzvu verejného obstarávateľa poskytnem vysvetlenie alebo doplním dokumenty v rozsahu prípustnom podľa zákona.
- Zachovávam dôvernosť a nekontaktujem verejného obstarávateľa inak ako cez systém.

7 VÝSLEDOK OBSTARÁVANIA

Verejný obstarávateľ vyhodnotí ponuky a oznámi výsledok.

SOM ÚSPEŠNÝ
- Dostanem oznámenie o úspešnosti
- Predložím požadované doklady na preukázanie splnenia podmienok účasti
- Poskytnem súčinnosť pri podpise zmluvy
- Pripravím sa na plnenie zmluvy

alebo

SOM NEÚSPEŠNÝ
- Dostanem oznámenie o výsledku
- Mám možnosť využiť opravné prostriedky (v zákonom ustanovených prípadoch a lehotách)
- Získam spätnú väzbu (ak je poskytnutá)

8 PLNENIE ZMLUVY

Ak som úspešný uchádzač, plním zmluvu riadne, včas a v dohodnutej kvalite.

- Dodám tovar / uskutočním práce / poskytnem služby
- Fakturujem podľa zmluvy
- Dodržiavam zmluvné podmienky a termíny
- Budujem dobré referencie pre ďalšie príležitosti

NA ČO SI DAŤ POZOR?

- Nepodávajte ponuku po lehote.
- Predložte všetky požadované dokumenty v správnom formáte.
- Komunikujte výlučne prostredníctvom systému určeného vo výzve.
- Dodržujte technické špecifikácie a požiadavky.
- Vyhnite sa konfliktu záujmov a nepravdivým údajom.
- Nedodržanie pravidiel môže viesť k vylúčeniu zo súťaže alebo sankciám.

UŽITOČNÉ TIPY

- Začnite s prípravou ponuky v dostatočnom predstihu.
- Dôkladne si prečítajte všetky súťažné podklady.
- Pýtajte sa – využite možnosť žiadať o vysvetlenie.
- Predkladajte kvalitnú a jasnú ponuku.
- Budujte portfólio a dobré meno – pomôže pri ďalších zákazkách.
- Zvážte zápis do Zoznamu hospodárskych subjektov (ZHS) – môže zjednodušiť preukazovanie splnenia podmienok účasti.

AKÉ DOKUMENTY MÔŽU BYŤ POŽADOVANÉ?

- Jednotný európsky dokument (JED)
- Výpis z registra / živnostenský list
- Doklady preukazujúce splnenie podmienok účasti
- Referencie / zoznam zákaziek
- Finančné ukazovatele
- Technické listy, certifikáty
- Iné podľa povahy zákazky

KTO JE KTO?

- **Verejný obstarávateľ** organizácia, ktorá obstaráva tovar, služby alebo práce
- **Komisia na vyhodnotenie ponúk** posudzuje a hodnotí ponuky podľa pravidiel
- **Elektronický prostriedok** (webová platforma) systém určený na komunikáciu a predkladanie ponúk

PRÁVNY ZÁKLAD

Zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

FAIR PLAY, TRANSPARENTNOSŤ A KVALITNÁ PONUKA SÚ CESTOU K ÚSPECHU VO VEREJNOM OBSTARÁVANÍ.

Viac informácií a návody nájdete na: **www.uvo.gov.sk**

ĎAKUJEME, ŽE PRISPIEVATE K EFEKTÍVNEMU A FÉROVÉMU VEREJNÉMU OBSTARÁVANIU.