

**Ministerstvo průmyslu a obchodu
České republiky
Sekce fondů EU – Řídící orgán OP TAK**

**Příloha č. 10
Podporované oblasti
Aplikace – výzva II. – VÝVOJ DIGITÁLNÍHO ŘEŠENÍ**



Seznam podporovaných oblastí výzvy Aplikace II. – VÝVOJ DIGITÁLNÍCH ŘEŠENÍ

1) Umělá inteligence a strojové učení, včetně velkých dat a bezpečnosti

Tato technologická oblast se zaměřuje na interakci mezi vědou o datech, velkými objemy dat a těžením dat, jakož i na metody používané ke zpracování dat pomocí algoritmů a dalších metod učení. Do konkrétních případů použití zahrnují např. rozpoznávání vzorů, algoritmické učení, automatizace, prediktivní analýza, rozpoznávání hlasu, např.:

- **Velká data:** Sběr, ukládání, zpracování / čištění a analýza velkého množství dat shromážděných z rozsáhlých transakcí (například v maloobchodě nebo ve finančním sektoru), dat shromážděných ze senzorů internetu věcí nebo jiných aplikací.
- **Těžení dat:** Zpracování velkých objemů dat za účelem identifikace anomálií, vzorců a korelací dat s cílem předvídat výsledky.
- **Strojové učení:** Algoritmy pro učení vyvinuté a aplikované na data na základě řízeného, neřízeného nebo zesíleného učení; výpočetní statistiky, neuronové sítě a technologie nebo prototypy, které z nich vycházejí a jejich optimalizace.
- **Umělá inteligence:** Využití algoritmů simulujících lidskou inteligenci pro zpracování přirozeného jazyka, analýzu dat, expertní systémy, strojového vidění, kreativity, vykreslování obrazu, her a široké škály dalších technologických aplikací.
- **Bezpečná umělá inteligence:** Nástroje a algoritmy zajišťující bezpečné nasazení umělé inteligence v konkrétních případech použití interagujících s lidmi a veřejným majetkem (kritická infrastruktura a další).

2) Kybernetická bezpečnost

Digitální řešení v kybernetické bezpečnosti zahrnují vývoj digitálních řešení pro ochranu dat, detekci anomálií a prevenci kybernetických útoků. Moderní přístupy zahrnují použití umělé inteligence pro detekci a prevenci kybernetických hrozeb, vývoj pokročilých šifrovacích metod, jako je post kvantová kryptografie, a zajištění bezpečnosti v síťových prostředích 5G/6G. Důraz je kladen na ochranu dat a systémů v prostředí internetu věcí (IoT) a rozšířených sítí např.:

- **Ochrana dat a soukromí:** Zaměření na pokročilé šifrování (včetně post kvantové kryptografie) a anonymizaci dat pro ochranu soukromí. Důraz na bezpečný přenos a ukládání dat, zejména v 5G/6G sítích a cloudových službách.
- **Detekce a prevence hrozeb:** Využití umělé inteligence a strojového učení k detekci kybernetických útoků a anomálií. Zahrnuje také behaviorální analýzu uživatelů a simulaci kybernetických útoků pro testování zabezpečení.
- **Zabezpečení sítí a IoT:** Vývoj bezpečnostních řešení pro internet věcí (IoT) a ochranu kritické infrastruktury. Zaměření na pokročilé firewall technologie a obranu proti DDoS útokům.
- **Forenzika a reakce na incidenty:** Zlepšení digitální forenzní analýzy pro rychlé odhalení útoků a obnovu systémů. Automatizace reakcí na kybernetické incidenty v reálném čase.

3) Pokročilá výroba a robotika

Pokročilé výrobní procesy využívají softwarové nástroje pro různorodé technologie typu 3D a 4D tisk, Průmysl 4.0, digitálních dvojčat, či aplikace IoT při sledování výroby apod., které se často prolínají s dalšími oblastmi jako je robotika, AI, virtuální a rozšířená realita, IoT, Edge Computing např.:

- **Digitální dvojčata:** aplikace digitálních technologií pro zrcadlení a modelování výrobních postupů a produktivity.
- **Internet věcí a senziorika:** využití internetu věcí, fúze dat a senzioriky pro výrobní pracovní postupy i trvanlivost, sledovatelnost, výkonnost, systémy kvality a další.
- **Robotika:** v robotice jsou softwarové systémy klíčové pro řízení a automatizaci robotických procesů, včetně kolaborativních robotů (kobotů) a autonomních systémů.

4) Pokročilé technologie ve zdravotnictví

Pokročilé SW nástroje ve zdravotnictví zahrnují rozvoj precizní medicíny, která využívá genomické informace pro personalizovanou léčbu. Zdravotní bioinformatika a analýza dat se zaměřují na lepší využití lékařských údajů pro predikci zdravotních rizik a optimalizaci léčby např.:

- Věda náročná na data; zdravotní bioinformatika.
- Sledování zdravotního stavu pacientů a biodata; lepší využití lékařských údajů.
- Zlepšení systémů poskytování lékařských a farmaceutických služeb s využitím dat a technologií; precizní medicína.
- Telemedicína: monitorování pacientů na dálku pomocí nositelných zařízení.

5) Udržitelná energie a čisté (nízkoemisní) technologie

Oblast udržitelné energie zahrnuje vývoj digitálních řešení pro:

- Optimalizaci spotřeby energie.
- Monitorování a řízení chytrých sítí (smart grids).
- Pokročilé algoritmy pro predikci a správu obnovitelných zdrojů energie.
- Správu baterií a další technologie pro ukládání energie.

6) Inteligentní dopravní aplikace pro města

V oblasti inteligentní dopravy se vývoj zaměřuje na digitální řešení pro:

- Autonomní vozidla.
- Chytré dopravní systémy (ITS).
- Aplikace pro řízení městské mobility.

7) Komunikační a síťové technologie

Rozvoj softwarových komponent pro sítě 5G a 6G zlepšuje spolehlivost a rychlost datových přenosů. Zaměřuje se na optimalizaci síťové infrastruktury prostřednictvím softwarově definovaných sítí (SDN) a virtualizace funkcí sítí (NFV), včetně řešení pro Edge computing např.:

- **5G / 6G sítě:** Inovativní SW komponenty těchto sítí; řešení vedoucí k nižšímu zpoždění při přenosu a/nebo vyšší spolehlivosti přenosu.
- **Bezpečnost komunikací:** Vývoj nových forem zabezpečení komunikace, včetně šifrovacích klíčů, distribuce kvantových klíčů a dalších; testování a monitorování narušení kybernetické bezpečnosti; inovativní SW komponenty pro zvýšení bezpečnosti sítí; monitorování rádiových emisí a další.
- **Zvyšování efektivity přenosu a snižování energetické náročnosti:** Vývoj efektivnějších metod pro kódování a kompresi signálu, opatření k významnému snižování kapacitních nároků provozovaných aplikací na komunikační síť.

8) Blockchain a distribuované sítě

Vývoj blockchainových technologií zahrnuje chytré smlouvy (smart contracts), decentralizované aplikace (DApps) a správu digitálních identit. Blockchain zajišťuje transparentnost a efektivitu v dodavatelských řetězcích a dalších oblastech, jako je finančníctví např.:

- **Smart contracts:** Automatizované smlouvy na blockchainu bez potřeby třetích stran.
- **Decentralizované aplikace (DApps):** Vytváření distribuovaných aplikací, které fungují na blockchainu.
- **Správa digitálních identit:** Ochrana soukromí a správa identity pomocí blockchainu.

Podporován není vývoj kryptoměn ani řešení pro jejich těžbu.

9) Kvantové výpočty a kvantová komunikace

Kvantové výpočty a simulace, které se zaměřují na vývoj nových algoritmů a aplikací využívajících kvantové počítače, mohou přinést zásadní inovace v oblasti materiálového výzkumu, farmaceutik a dalších technologických odvětví. Kvantová komunikace je přelomová technologie pro bezpečný přenos informací a ochranu dat.

- **Kvantová komunikace:** Zabezpečení dat a komunikací pomocí kvantových metod, kvantová a post kvantová kryptografie.
- **Kvantové simulace:** Simulace složitých systémů pro informační podporu vývoje nových materiálů, léčiv, energetiky, dopravy atd.
- **Kvantové výpočty:** Kvantové počítače s různými designy, materiály pro kvantové počítače, kvantové algoritmy, kvantové a hybridní výpočty.

10) Fintech a digitální finance

Fintech technologie zahrnují vývoj SW nástrojů pro decentralizované finance (DeFi). Klíčové oblasti zahrnují také Regtech pro automatizaci regulací a Insurtech, které mění pojišťovnictví pomocí digitálních řešení např.:

- **Decentralizované finance:** Platformy pro půjčky, investice a transakce bez bankovních prostředníků.
- **Regtech a Insurtech:** Automatizace regulačních procesů a inovace v pojišťovnictví.

Podporován nebude vývoj digitálních řešení spojených s výrobou, zpracováním, přepravou, distribucí, skladováním nebo spalováním fosilních paliv.