DIGITALTECH EDIH - EUROPEAN DIGITAL INNOVATION HUBS

ÁLTALÁNOS FELHASZNÁLÁSI FELTÉTELEK (ÁFF)

Impresszum:

Ez a felhasználási feltételeket rögzítő útmutató a vállalkozásoknak, és egyéb érdekelteknek határozza meg az elérhető szolgáltatások, tanácsadások igénybevételéhez szükséges paramétereket. Jogilag kötelező érvényű, és mint ilyen, egyben meghatározza az Európai Bizottság és a magyar állam, mint Támogatók által támasztott elszámolási kötelezettséget.

A kkv-nak, PSO-nak történő minősítéssel kapcsolatos feltételek meghatározásához útmutató, segédlet érhető el. mely tartalmazza a vonatkozó részleteket és magyarázatokat, ill. elérhetőek nyilatkozatminták is, amelyet az egyes érintettek töltenek ki a státuszuk megállapítása érdekében akkor, amikor a projekt támogatási rendszeréhez folyamodnak az együttműködés keretében.

Jelen Általános Felhasználási Feltételek (a továbbiakban: ÁFF) célja, hogy meghatározza a DEDIH Konzorciumnak (a továbbiakban: Konzorcium), valamint annak tagjai (Szolgáltató) által közösen, illetve egyenként nyújtott tevékenységi portfólió (képzések, szolgáltatások) összetételét, azok igénybe vevőinek (a továbbiakban: Ügyfél) (a továbbiakban együttesen: Felek) jogait és kötelezettségeit.

Jelen felhasználási feltételek a Szolgáltató által, több szerződés megkötése céljából egyoldalúan, a másik fél közreműködése nélkül előre kerülnek meghatározásra, melyet a Felek egyedileg nem tárgyalnak meg. Szolgáltató Magyarországon bejegyzett jogi személy, így tagállami joga Magyarország joga – így jelen szerződési feltételekre irányadónak a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) vonatkozó rendelkezéseit határozza meg. A Szolgáltató felhívja az Ügyfél figyelmét, hogy a jelen ÁFF elfogadásával egyidejűleg azt az Ügyfél magára nézve kötelezőnek ismeri el és a megrendelés teljesítése során a jelen ÁFF rendelkezéseit irányadónak kell tekinteni.

Szolgáltató felhívja Ügyfele figyelmét, hogy a jelen felhasználási feltételek alapján igénybe vehető megrendelés elsődlegesen a magyar jogrendszer alapján lett kialakítva.

Az érintett felelőssége megvizsgálni, hogy számára a megrendelés saját személyi joga és támogatási keretei alapján is megfelelő-e a jelen ÁFF-ben részletezettek szerint. Ezekben a Konzorcium az elektronikus ügyfélkapcsolati rendszerén keresztül elérhető Tudástárban található dokumentumokon keresztül (pl. KKV checklist) támogatja, orientálja. Nem megfelelőség esetén fizetési kötelezettség áll be, támogatás érvényesen nem adható át.

Szolgáltató kijelenti, Ügyfél pedig magára nézve kötelezően elismeri, hogy a Felek közötti kommunikációs csatorna elsődlegesen digitális (pl. zárt elektronikus rendszeren keresztül és/vagy email útján valósul meg).

A Szolgáltató ezúton tájékoztatja az Ügyfelét, hogy:

- − az ÁFF alapján létrejövő egyedi szerződések a megrendelésen és teljesítési igazoláson meghatározott szereplők szerint elektronikus úton kerülnek megkötésre;
- − az ÁFF teljes terjedelmében a Konzorcium elektronikus ügyfélkapcsolati rendszerén keresztül érhető el, tölthető le.

A DigitalTech EDIH Konzorcium nem önálló jogi személy, tagjai külön-külön és együtt látják el a Támogatási Szerződésükben vállalt feladataikat, nyújtják különböző szolgáltatásaikat annak érdekében, hogy ügyfeleik digitális képességei épüljenek, bővüljenek a projekt futamideje alatt, ill. a későbbiekben is akár. A DigitalTech EDIH-nél a leendő ügyfelek igényeire szabott, komplex szolgáltatások sokrétű portfóliójának megvalósítását tervezzük, amely kiterjed a kiberbiztonságra, a digitális kompetenciákra (blokklánc-technológia, oktatástechnológia, digitális pénzügy), valamint a digitális átalakuláshoz kapcsolódó általános készségekre és megoldásokra. E szolgáltatások magukban foglalják:

- „Beruházás előtti próba” mind technológiai, mind üzleti szempontból;
- Finanszírozási lehetőségek (hazai és nemzetközi szinten);
- Képzési tevékenységek mind technológiával (kiberbiztonság, digitális készségek blokkláncban, pénzügyi technológia, oktatástechnológia és digitális transzformációs eszközök), mind üzletfejlesztéssel kapcsolatos kérdésekben;
- Hálózatépítési tevékenység;
- Információs szolgáltatások.

A projekt futamideje: 2022.10.01. – 2025.09.30.

Konzorcium tagjai, a Szolgáltatók adatai

1. **EIT DIGITAL HUNGARY NON PROFIT KFT (EIT Digital HU),**

székhely: 1117 Budapest Bogdánfy utca 10/a.
képviseli: dr. Trinh Anh Tuan

2. BUDAPESTI MŰSZAKI ES GAZDASÁGTUDOMÁNYI EGYETEM (BME)
székhely: 1111 Budapest, Műegyetem rakpart 3.
képviseli: Dr. Csákány Anikó

3 IVSZ – Digitális Vállalkozások Szövetsége
székhely: 1095 Budapest, Tinódi utca 1-3. C épület fsz. 2.
képviseli: dr. Vinnai Balázs János

4. EÖTVÖS LORÁND TUDOMÁNYEGYETEM (ELTE)
székhely: 1053 Budapest, Egyetem tér 1-3.
képviseli: Dr. Horváth Zoltán

5. BLOCKCHAIN MAGYARORSZÁG EGYESÜLET (BCME)
székhely: 1037 Budapest, Kisbojtár u. 24-26.
képviseli: Kalocsai Kornél

6. EDUTUS EGYETEM (Edutus Egyetem),
székhely: 2800 Tatabánya, Stúdium tér 1.
képviseli: Némethné Dr. Gál Andrea

7. INFOTÉR NONPROFIT KFT (Infotér),
székhely: 1062 Budapest, Aradi utca 8.
képviseli: Bencze György

8. KÖZEP-DUNÁNTÚLI REGIONÁLIS INNOVÁCIÓS UGYNOKSEG NONPROFIT KFT

(KDRIÜ),
székhely: 8000 Székesfehérvár, Seregélyesi u. 113.
képviseli: Dr. Szépvölgyi Ákos

9. DEBRECENI EGYETEM (DE),
székhely: 4032 Derecen, Egyetem tér 1.
képviseli: Prof Dr. Szilvássy Zoltán

10. PRIMOM SZABOLCS-SZATMÁR-BEREG MEGYEI VÁLLALKOZÁSÉLÉNKÍTŐ ALAPÍTVÁNY (PRIMOM),
székhely: 4400 Nyíregyháza, Váci Mihály u. 41.
képviseli: Mészáros Éva

11. DIGITÁLIS KORMÁNYZATI FEJLESZTÉS ÉS PROJEKTMENEDZSMENT KFT (DKF),
székhely: 1138 Budapest, Esztergomi út 31-39. HUB3. ép.
képviseli: Béke Tamás, Takács Gábor, Lótos Tibor Ádám

Fogalmak

De minimis: olyan, vállalkozások (vállalatok) részére nyújtott csekély összegű állami támogatás, amelyet az uniós tagállamoknak nem kell bejelenteniük az Európai Bizottság felé. Összege vállalkozásonként egy hároméves időszakra maximum 200 000 euró lehet.

Felek: Eladó, mint Szolgáltatást nyújtó szervezet és Vevő, a Szolgáltatást megrendelő szervezet együttesen.

Innovációs klaszter: önálló felek (pl. innovatív induló vállalkozások, kis-, közép- és nagyvállalkozások, valamint kutató-tudásközvetítő szervezetek, nonprofit szervezetek és egyéb kapcsolódó gazdasági szereplők) szervezett csoportja, amelyet abból a célból hoztak létre, hogy ösztönözze az innovatív tevékenységeket egyrészt a klaszterben részt vevő vállalkozások és egyéb szervezetek közötti létesítménymegosztás, ismeret- és tapasztalatcsere előmozdítása, másrészt a tudástranszferhez, kapcsolatépítéshez, ismeretterjesztéshez, valamint együttműködéshez való hatékony hozzájárulás révén.

Innovációs utalvány (voucher), innovációs támogatás: mikro-, kis- és középvállalkozások aktuális projektjeihez szükséges innovációs tudás és tanácsadás megvásárlását lehetővé tévő támogatott eszköz, amely a vevő vállalatok és beszállító tudásközpontok közötti tudásáramlást.

Ügyfél: **a vonatkozó támogatási szerződés szerinti kategóra érintetteje. Olyan KKV és/vagy PSO,** mely üzleti tevékenysége körében az elektronikus ügyfélkapcsolati rendszeren keresztül vételi ajánlatot tesz és szerződést köt a Szolgáltatás igénybe vétele céljából a szolgáltatást megrendelő szervezet nevében, képviseletében eljáró személyen keresztül.

PSO: olyan közigazgatási szervezet, közjogi szerv, mely hatáskör alapján, illetékességi területén, jogszabályban meghatározott közigazgatási feladatot lát el közhatalom birtokában.

KKV: fogalommeghatározásához iranyadó az Európai Bizottság hivatalos útmutatója (az Európai Unió Hivatalos Lapjában közzétett 2003/361/EK bizottsági ajánlás - HL L 124., 2003.5.20., 36. o.) és a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény.

Ügyfélkezelési rendszer: a jelen ügyfélkezelési rendszer, amely az egyedi szerződés megkötésére szolgál.

Szerződés: Eladó, azaz a Szolgáltatást nyújtó szervezet és Vevő, mint a Szolgáltatást igénybe vevő között az elektronikus ügyfélkapcsolati rendszer és elektronikus levelezés igénybevételével létrejövő szerződés, azaz visszaigazolt megrendelő.

Távollévők közötti kommunikációt lehetővé tévő eszköz: olyan eszköz, amely alkalmas a felek távollétében – szerződés megkötése érdekében – szerződési nyilatkozat megtételére. Ilyen eszköz a Szolgáltatás igénybe vételét szolgáló megrendelőlapot, a Szolgáltatás igénybevételének megtörténtét igazoló teljesítési igazolást, ill. a Szolgáltatást igénybevételének fedezetét rendező de minimis vagy innovációs támogatás nyilatkozatot továbbító email, zárt elektronikus csatorna.

Távollévők között kötött szerződés: olyan (fogyasztói) szerződés, amelyet a szerződés szerinti szolgáltatás nyújtására szervezett távértékesítési rendszer keretében a felek egyidejű fizikai jelenléte nélkül úgy kötnek meg, hogy a szerződés megkötése érdekében a szerződő felek kizárólag távollévők közötti kommunikációt lehetővé tévő eszközt alkalmaznak.

Vonatkozó jogszabályok, alapszerződések
A Szerződésre a magyar jogszabályok az irányadóak, különösen, de nem kizárólagosan az alábbi jogszabályok rendelkezéseire kell tekintettel lenni:

- 1997. évi CLV. törvény a fogyasztóvédelemről
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 45/2014. (II.26.) kormányrendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól
- 1999. évi LXXVI. törvény a szerzői jogról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/302 RENDELETE (2018. február 28.) a belső piacon belül a vevő állampolgársága, lakóhelye vagy letelepedési helye alapján történő indokolatlan területi alapú tartalomkorlátozással és a megkülönböztetés egyéb formáival szembeni fellépésről, valamint a 2006/2004/EK és az (EU) 2017/2394 rendelet, továbbá a 2009/22/EK irányelv módosításáról AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

Az ÁFF hatálya, elfogadása
A közöttünk létrejövő szerződés tartalmát – a vonatkozó kötelező érvényű jogszabályok rendelkezései mellett – a jelen Általános Felhasználási Feltételek (a továbbiakban: ÁFF) határozzák meg. Ennek megfelelően tartalmazza a jelen ÁFF az Önt és bennünket illető jogokat és kötelezettségeket, a szerződés létrejöttének feltételeit, a teljesítési határidőket, és fizetési feltételeket, a felelősségi szabályokat, valamint az elállási jog gyakorlásának feltételeit.

Ön a megrendelése véglegesítése előtt köteles megismerni és megrendelésével elfogadni a jelen ÁFF rendelkezéseit.

A felhasználási feltételek keretében nyújtott szolgáltatások igénybevételére (tanácsadás és képzés) nem jogosult az az érintett (ügyfél), amely

- nem minősül kis- és középvállalkozásnak,

- az államháztartásról szóló 2011. évi CXCV. törvényben (a továbbiakban: Áht.) foglaltak szerint nem felel meg a rendezett munkaügyi kapcsolatok követelményének,

- a részben (25%-ot nem meghaladó mértékben) köztulajdonban álló gazdasági társaság esetén, ha az Áht.-ban foglaltak szerint a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvényben foglalt közzétételi kötelezettségének nem tett eleget,

- olyan jogi személy vagy jogi személyiséggel nem rendelkező más szervezet, amely az Áht. 1. § 4. pontja szerint nem átlátható szervezet,

- a támogatási rendszerből való kizárás hatálya alatt áll,

- harmadik személy irányában olyan kötelezettsége áll fenn, amely a részére továbbadott támogatással szerzett szolgáltatás céljának megvalósulását meghiúsíthatja,

- a továbbadott támogatás igénybevételére vonatkozó jogosultság megállapításakor, vagy az igénybevételt követő három évig terjedő időszak alatt, a továbbadott támogatás megítélését vagy annak felhasználását befolyásoló valótlan, hamis vagy megtévesztő adatot szolgáltatott vagy ilyen nyilatkozatot tett,

- jogerős végzéssel elrendelt felszámolási, csőd-, végelszámolási vagy egyéb - a megszüntetésére irányuló, jogszabályban meghatározott - eljárás alatt áll,

- az Áht. 50. § (3) bekezdés alapján nem részesíthető költségvetési támogatásban.

Továbbá az alábbi szempontok szerint nem nyújtható továbbadott támogatás:

  - azon támogatást igénylő részére, amellyel szemben a Nemzeti Adó- és Vámhivatal (NAV) által indított végrehajtási eljárás van folyamatban a továbbadott támogatás igénybevétele időpontjában;

  - azon támogatást igénylő részére, amely vállalkozás esetében a www.szechenyi2020.hu weboldalon található „Általános tájékoztatás 1. Kizáró okok” című pontjában foglaltak valamelyike fennáll.

A szerződés nyelve, a szerződés formája
A jelen ÁFF hatálya alá tartozó szerződések nyelve a magyar nyelv.

Árak
Az árak forintban és/vagy euróban értendők, adott szolgáltatástól és arra vonatkozó nyilatkozatoktól függően. Az átváltási árfolyamról minden egyes esetben az egyedi szerződésben foglaltaknak megfelelően rendelkeznek a felek, azt fizetési kötelezettségtől függően pl. a ’de minimis” vagy innovációs támogatás nyilatkozatban feltüntetik. Az árak minden esetben sávosan, piaci alapon kerülnek meghatározásra. A DigitalTech EDIH Konzorcium Támogatási Szerződése alapján specifikált indikátorokban vállalt továbbadott szolgáltatásokat piaci áron nyújtjuk. A piaci ár meghatározásánál figyelembe vesszük, a hasonló szolgáltatások piaci árát, a szolgáltatásokat nyújtó munkatársak kiemelkedő innovációs, kutatási és nemzetközi együttműködési tapasztalatait, a Magyar Mérnöki Kamara vonatkozó nettó mérnöki díjszabási ajánlását. A DigitalTech EDIH jelen ÁFF-ben a szolgáltatásainak irányárát rögzíti, amelyek a piaci igények függvényében változhatnak. Az egyes szolgáltatások árát befolyásolja az adott tanfolyam/konzultáció tartalma, illetve a tanácsadási, tesztelési vagy befektetés támogatási szolgáltatás – ügyféllel egyeztetett – összetettsége, így a

DigitalTech EDIH részéről delegált csapat mérete és szakembergárdája is, tekintettel arra, hogy egy adott szolgáltatás mögött nem egy szakember, hanem több szakember állhat, tréningeket, konzultációkat, test before invest szolgáltatást egyaránt nyújthatunk. Ezért

- tréningek esetén: 240-600 euró/nap - 96.000-240.000 HUF/nap
- konzultáció esetén: 800-2000 euró/nap – 320.000-800.000 HUF/nap
- test before invest szolgáltatás esetén: 1000-2500 –euró/nap – 400.000-1.000.000 HUF/nap

irányárakat alkalmazunk.

Fentiekkel összhangban felhívjuk ismételten a figyelmet arra, hogy az árak tájékoztató jellegűek. Nem zárható ki annak a lehetősége, hogy üzletpolitikai okból az Eladó az árakat módosítsa. Az árak módosítása nem terjed ki a már megkötött szerződésekre. Amennyiben Eladó az árat hibásan tüntette fel, és megrendelés érkezett a szolgáltatásra, de szerződést még nem kötöttek a felek, úgy az ÁFF „hibás ár" pontja alapján jár el az Eladó.

Panaszügyintézés és jogérvényesítési lehetőségek
A fogyasztó **írásban közölheti a panaszát**. Az írásbeli panaszra vonatkozóan az alábbiak szerint köteles eljárni. **Az írásbeli panaszt a szolgáltató** – ha az Európai Unió közvetlenül alkalmazandó jogi aktusa eltérően nem rendelkezik – a beérkezését követően **harminc napon belül köteles írásban érdemben megválaszolni és intézkedni annak közlése iránt**. Ennél rövidebb határidőt jogszabály, hosszabb határidőt törvény állapíthat meg. A panaszt elutasító álláspontját a vállalkozás indokolni köteles. A telefonon vagy elektronikus hírközlési szolgáltatás felhasználásával közölt szóbeli panaszt a szolgáltató köteles egyedi azonosítószámmal ellátni. A panaszról felvett jegyzőkönyvnek tartalmaznia kell az alábbiakat:
1. a fogyasztó neve, lakcíme,
2. a panasz előterjesztésének helye, ideje, módja,
3.a fogyasztó panaszának részletes leírása, a fogyasztó által bemutatott iratok, dokumentumok és egyéb bizonyítékok jegyzéke,
4.a szolgáltató nyilatkozata a fogyasztó panaszával kapcsolatos álláspontjáról, amennyiben a panasz azonnali kivizsgálása lehetséges,
5. a jegyzőkönyvet felvevő személy és - telefonon vagy egyéb elektronikus hírközlési szolgáltatás felhasználásával közölt szóbeli panasz kivételével - a fogyasztó aláírása,
6. a jegyzőkönyv felvételének helye, ideje,
7. panasz egyedi azonosítószáma.

A szolgáltató a panaszról felvett jegyzőkönyvet és a válasz másolati példányát köteles megőrizni, és azt az ellenőrző hatóságoknak kérésükre bemutatni.

A szerzői jogról szóló 1999. évi LXXVI. törvény (továbbiakban: Szjt.) 1. § (1) bekezdése értelmében az ügyfélkezelési rendszerünk szerzői műnek minősül, így annak minden része szerzői jogi védelem alatt áll. Az Szjt. 16. § (1) bekezdése alapján tilos a ügyfélkezelési rendszeron található grafikai és szoftveres megoldások, számítógépi programalkotások engedély nélküli felhasználása, illetve bármely olyan alkalmazás használata, amellyel a ügyfélkezelési rendszer, vagy annak bármely része módosítható. A ügyfélkezelési rendszerről és annak adatbázisából bármilyen anyagot átvenni a jogtulajdonos írásos hozzájárulása esetén is csak a ügyfélkezelési rendszerre való hivatkozással, forrás feltüntetésével lehet.

A digitális adattartalom működése, műszaki védelmi intézkedések

A ügyfélkezelési rendszer üzemeltetéséről, a rendszer támogatásáról bővebben itt tájékozódhat: https://digitaltechedih.hu/impresszum/. Az ügyfélkezelési rendszeren megjelenő adatokat szolgáltató

szerverek elérhetősége megfelelő. Rendszeresen mentés készül a teljes adattartalomról, így probléma esetén az eredeti adattartalom visszaállítható. A megjelenő adatokat biztonságos adatbázisban tároljuk. Az érzékeny adatok megfelelő erősségű titkosítással vannak tárolva, kódolásukhoz processzorba épített hardveres támogatást használunk.

A szolgáltatások lényeges tulajdonságaira vonatkozó tájékoztatás

Az elektronikus ügyfélkapcsolati rendszeren keresztül megrendelhető szolgáltatások lényeges tulajdonságairól az egyes szolgáltatásokra vonatkozóan az ÁFF függelékében szereplő általános leírásokban adunk tájékoztatást.

Az adatbeviteli hibák javítása - Felelősség a megadott adatok valóságáért

Önnek a megrendelés során a megrendelés véglegesítése előtt folyamatosan lehetősége van az Ön által bevitt adatok módosítására. Felhívjuk a figyelmét, hogy az Ön felelőssége, hogy az Ön által megadott adatok pontosan kerüljenek bevitelre, hiszen az Ön által megadott adatok alapján kerül nyílvántartásba, ellentételezésre, illetve teljesítésre. Felhívjuk a figyelmét arra, hogy a rosszul megadott e-mail cím vagy a postafiókhoz tartozó tárhely telítettsége a visszaigazolás kézbesítésének hiányát eredményezheti és meggátolhatja a szerződés létrejöttét.

Hibás ár

Nyilvánvalóan hibásan feltüntetett árnak minősül: 0 Ft-os ár, kedvezménnyel csökkentett, de a kedvezményt tévesen feltüntető ár (pl.: 1000 Ft-os szolgáltatás esetén a 20 %-os kedvezmény feltüntetése mellett 500 Ft-ért kínált szolgáltatás). Hibás ár feltüntetése esetén Eladó felajánlja a szolgáltatás valós áron történő megvásárlásának lehetőségét, mely információ birtokában a Vásárló eldöntheti, hogy megrendeli valós áron a szolgáltatást vagy minden hátrányos jogkövetkezmény nélkül lemondja a megrendelést.

Az ügyfélkezelési rendszer használata, a megrendelés folyamata

Az oldalon regisztrációval lehet szolgáltatást rendelni, vásárolni, egyedi szerződéseket generálni, melyet egy kifejezetten ezt a célt támogató elektronikus rendszer segít elő a digitális szerződéskötést elősegítendő.

Az alábbi adatokat szükséges megadni a megrendelés elküldéséhez:
Személyes adatok:
Név, Email cím, Telefonszám
Cég esetén cégadatok: Cég vagy vállalkozó neve, cégjegyzékszám, adószám

Megjegyzést is küldhet nekünk.

A hírlevélre való feliratkozás és a regisztráció ügyfélkezelési rendszerünkon opcionális.

Rendelés véglegesítéséhez kattintson a **Megrendelés elküldése** gombra, ami fizetési kötelezettséggel jár. Tényleges fizetési kötelezettség az adott Vevő de minimis vagy innovációs támogatási keretétől függően állhat be. A megrendelő elküldésével a Vevő igazolja a jelen ÁSZF és a Szolgáltató Adatvédelmi és Adatkezelési Szabályzat elolvasását, megértését és elfogadását.

Fontos, ügyeljen az adatok pontosságára, hiszen a megadott adatok alapján történik a teljesítés és az ellentételezés.

Bármilyen módosítás, személyes kérés esetén e-mail- ben: info [kukac] digitaltechedih.hu cím keressen meg bennünket. Egy rendelést akkor tekintünk részünkről befogadottnak, amint a kollégáink ellenőrizték és e-mailben visszaigazolták azt. **Minden esetben várja meg kollégáink részéről a visszaigazoló e-mailt.**

A rendelés menete (ajánlattétel)
Amennyiben Ön meggyőződött arról, hogy a kosár tartalma megfelel az Ön által megrendelni kívántaknak. Az ügyfélkezelési rendszeren keresztül közölt információk az Eladó részéről szerződés megkötésére vonatkozó ajánlati felhívásnak, az Ön által megküldött megrendelők ajánlatnak minősülnek.
Ön a „Megrendelés elküldése" gomb megnyomásával kifejezetten tudomásul veszi, hogy az ajánlatunkat megtettnek kell tekinteni, és nyilatkozata – az Eladó jelen ÁFF szerinti visszaigazolása esetén - fizetési kötelezettséget vonhat maga után a vonatkozó innovációs támogatási, ill. de minimis keretétől függően.

Rendelés feldolgozása, a szerződés létrejötte

Az Eladó az Ön ajánlatának elküldését követően e-mail útján visszaigazolja azt. A szerződés akkor jön létre, amikor azt mindkét fél elfogadta, azaz az Ön ajánlata visszaigazolása megtörtént. A teljes folyamat leírását külön, erre vonatkozó függelék tartalmazza.

Eladó fenntartja magának a jogot, hogy az adott Szolgáltató által nyújtott tréningek tekintetében az általánostól eltérő egyedi módon kezelje a megrendeléseket, melyekről a Vevőt előzetesen megfelelően tájékoztatja.

Az ÁFF hatályos ettől a naptól: 2023.08.01.

Függelék:

1. számú függelék: szolgáltatások általános tájékoztató jellegű leírása
2. számú függelék a közös adatkezelésre vonatkozó tájékoztatóról
3. számú függelék: szerződéskötés menetének leirata

Függelék a szolgáltatások általános tájékoztató leírásáról

Általános Felhasználási Feltételek – Általános tájékoztató leírás

KIBERBIZTONSÁG

1. **Kiberbiztonsági útmutatás**

A szolgáltatás célja az érdeklődő kliensek segítése a számukra releváns kiberbiztonsági kockázatok azonosításában és tanácsadás a kiberbiztonsági problémák megoldására használható korszerű módszerek, eszközök, és folyamatok kiválasztásában. Az olyan kliensek, akik esetleg nincsenek teljes mértékben tisztában a saját kiberbiztonsági kitettségüknek, érettségi szintjüknek, és felkészültségüknek, arra használhatják ezt a szolgáltatást, hogy jobban megértsék a kiberbiztonsági alapfogalmakat, szakterületeket, és megoldásokat, és ezáltal jobban lássák, hogy használhatóak mindezek a saját problémáik megoldásában. Miután a fenti megértés megszületett, az érdeklődő kliensek igénybe vehetik a DigitalTech EDIH fókuszáltabb tanácsadói szolgáltatásait egyedi problémáik megoldása érdekében.

2. **Kiberbiztonsági kockázatelemzés**

A szolgáltatás célja az érdeklődő ügyfelek segítése a kiberbiztonság kockázatkezelési nézőpontjának elsajátításában. Az olyan kliensek, akik nem rendelkeznek kockázatkezelési háttértudással, arra használhatják ezt a szolgáltatást, hogy jobban megértsék a kiberbiztonsági kockázatkezelési alapfogalmakat: irányítás, értékelés, kezelés és monitorozás, a kapcsolódó ajánlásokat, és hogy milyen módon tudják ezeket alkalmazni a saját rendszereikben. A tanácsadás igény szerint érintheti az ipari vezérlő (OT) rendszerek specifikus kockázatkezelési nehézségeit, a fenyegetettség modellezést, illetve a kiberbiztosítást, mint kockázatátruházási megoldást is. A konzultáció után az érdeklődő kliens igénybe veheti a DigitalTech EDIH műszaki megoldás fókuszú tanácsadói szolgáltatásait a műszaki kockázatkezelés implementálása érdekében.

3. **Kiberbiztonsági hatásanalízis**

A digitalizáció kulcsa a termelő és szolgáltató rendszerek intelligenssé tétele IT alapú adatfeldolgozás és vezérlés alkalmazásával. Az IT rendszerek egyfelől drasztikusan javítják a felügyelt rendszer működése egészének hatékonyságát, ugyanakkor az IT rendszerben fellépő szándékos, illetve véletlen hibák hatása a folyamaton végig terjedve drasztikus sőt katasztrofális mértékig erősödhet.
A biztonsági, illetve szolgáltatásbiztonsági célú hatásanalízis célja az, hogy a lokálisan fellépő véletlen vagy szándékos hibák rendszerszintű hatásának vizsgálatára egzakt módszert adjon.
A hatásanalízis alapja az, hogy a rendszer funkcionális működését és felépítését leíró modellben a jellegzetes támadásokat, illetve meghibásodásokat beinjektáló mutációkat generálunk és azokon kimerítő vizsgálattal végig követjük az egyes hibák terjedését és a rendszer működésére gyakorolt hatását. A vizsgálat végeredménye támogatja a rendszerrel szembeni biztonsági és üzembiztonsági követelmények megfogalmazását, sőt alkalmas a tervezett védelmek hatékonyságának elemzésére is.

4. **Adatvédelmi kockázatbecslés és hatáselemzés**

Ennek a tanácsadási szolgáltatásnak az a célja, hogy segítse az ügyfeleket főbb adatvédelmi kockázataik azonosításában, és útmutatást adjon arra vonatkozóan, hogyan lehet ezeket a kockázatokat csökkenteni a legkorszerűbb adatvédelmi technológiákkal. Azokat az ügyfeleket, akiknek nincs világos elképzelésük szolgáltatásuk lehetséges adatvédelmi vonatkozásairól, és adatvédelmi hatásvizsgálat elvégzésével szeretnének megfelelni a GDPR előírásainak, arra biztatjuk,

hogy használják ezt a szolgáltatást, hogy megismerjék az adatvédelmi kockázatértékelés módszertanát és azt, hogy hogyan alkalmazzák ezt konkrét termékekre és szolgáltatásokra. Amint jobban megértik a szolgáltatással kapcsolatos adatvédelmi kihívásokat, az ügyfelek dönthetnek úgy, hogy a DigitalTech EDIH által kínált, célzottabb tanácsadási szolgáltatásokat veszik igénybe, amelyek segíthetnek nekik a kihívások kezelésében.

5. **Kiberbiztonsági szabályozás, szabványok, legjobb gyakorlatok és megfelelőség**

Az utóbbi évtizedben, fontos lépések történtek a kiberbiztonsággal kapcsolatos jogalkotás és szabályozás területén (pl. megjelent az EU NIS direktívája és a nemzeti információbiztonsági törvény (Ibtv)). Egyes szakterületeken működő szervezeteknek meg kell felelniük az új törvényeknek és szabályozásoknak, és ennek érdekében célszerű alkalmas kiberbiztonsági szabványokat és legjobb gyakorlatokat alkalmazniuk és követniük. Ez a szolgáltatás segíti a klienseket abban, hogy azonosítsák a számukra releváns törvényeket és szabályozásokat, és az alkalmazható kiberbiztonsági szabványokat és legjobb gyakorlatokat. Azon kliensek számára, akiknek jogszabályi megfelelőségi kötelezettségeknek vagy általánosan elfogadott iparági követelményeknek kell eleget tenniük, segítünk azonosítani a megfelelőség biztosítására használható módszereket, eszközöket, és folyamatokat.

6. **Adatvédelmi megfelelőség előírásoknak és rendeleteknek**

Ennek a tanácsadási szolgáltatásnak az a célja, hogy segítse ügyfeleit az Általános Adatvédelmi Szabályzat (GDPR) betartásában. Ez magában foglalja azt, hogy útmutatást adunk a személyes adatok azonosításához egy szolgáltatásban, mik azok a személyes és érzékeny adatok, és hogyan kell végrehajtani a GDPR alapelveit, ideértve az érvényes hozzájárulás kérését, az adatok minimalizálását és az adatfeldolgozási cél korlátozását, az elszámoltathatóság bizonyítását, valamint a személyes adatok biztonságának és pontosságának garantálását. Azoknak az ügyfeleknek, akiknek nincs világos elképzelésük a GDPR-követelményekről és azok következményeiről, és szeretnének megfelelni a GDPR-nak, javasoljuk, hogy használják ezt a szolgáltatást a GDPR alapelveinek és definícióinak megismerésére. Amint jobban megértik ezeket a követelményeket ebben a szolgáltatásban, az ügyfelek dönthetnek a DigitalTech EDIH által kínált, célzottabb tanácsadási szolgáltatások igénybevétele mellett, amelyek segíthetnek azonosítani a személyes adatok védelmét szolgáló technológiát és eszközöket, és így megfelelni a GDPR előírásainak.

7. **Kiberbiztonság-érettségi felmérés**

A kiberbiztonság egy sokarcú, összetett terület, amihez sokféle ajánlás, szabályozás és lehetséges cél érhető el. A kliens által biztosított adatokat áttekintve ez a konzultációs szolgáltatás segít azonosítani, hogy a kliens számára a kiberbiztonság milyen vetületei lehetnek kiemelten fontosak, milyen hiányosságok vannak a jelenlegi üzletmenetben és folyamatokban, majd ezek alapján további, irányított konzultációs szolgáltatásokat javasol a DigitalTech EDIH portfoliójából.

Egy tipikus első konzultációs alkalmon először közösen áttekintjük a klienssel a kezdeti kiberbiztonsági kérdőívre adott válaszokat, majd azonosítjuk, hogy milyen jellegű további adatokra lenne szükség a kiértékelés elvégzéséhez (pl. üzleti folyamatok leírása, használt szoftverfejlesztési életciklus). A megadott adatok vizsgálata után egy következő közös konzultációs alkalmon bemutatjuk az előzetes vizsgálatok eredményét, azonosítjuk, hogy melyik területeket javítására érdemes fókuszálni, és további, célzott konzultációs szolgáltatásokat javaslunk. Figyelem: ez a konzultációs szolgáltatás nem foglalja magában a tanúsítást vagy bármilyen szabvány szerinti formális felmérést, mert az ilyen típusú jóval hosszabb tevékenységek kívül esnek a DigitalTech EDIH hatókörén.

8. **Kiberbiztonsági programok létrehozása**

Ezt a szolgáltatást azoknak az ügyfeleknek ajánljuk, akik már meghatározták kiberbiztonsági érettségi szintjüket (pl. a mi érettségi szint felmérését célzó szolgáltatásunkat használva) és tovább szeretnének lépni jelenlegi érettségi szintjük növelésében. Ezeknek az ügyfeleknek segítünk meghatározni a reálisan elérhető magasabb érettségi szintet és azonosítani azokat a lépéseket, melyeket meg kell tenniük céljuk elérése érdekében. Mindez általában azt jelenti, hogy az ügyfélnek létre kell hoznia és végre kell hajtania egy kiberbiztonsági programot, mely szisztematikusan vezeti végig az ügyfelet a szükséges folyamatokon és lefedi a kiberbiztonsági fejlesztések minden aspektusát. Segítünk az

érdeklődő ügyfeleknek felépíteni egy ilyen programot, beleértve a célok és a mérhető teljesítménymutatók meghatározását, a megfelelő módszerek, eszközök, és folyamatok azonosítását, és a program végrehajtása költségeinek becslését.

9. **Kiberbiztonsági technológiák áttekintése és összehasonlító elemzése**

Ezt a szolgáltatást olyan ügyfelek részére nyújtjuk, melyek új kiberbiztonsági megoldást szeretnének bevezetni rendszerükbe vagy szolgáltatásukba, és ennek megvalósítására több biztonsági technológiát is lehetségesnek tartanak és figyelembe kívánnak venni. Elvégezzük ezen biztonsági technológiák részletes elemzését, azonosítva előnyeiket és hátrányaikat, és összehasonlítjuk őket egymással. Ez az összehasonlító elemzés segíti az ügyfelet a megfelelő technológia kiválasztásában. A szolgáltatás maga tartalmaz egy ügyfél-interjút, ami segít definiálni a tanácsadás pontos célját és terjedelmét, amit intenzív kutatás és elemzés követ, majd végül készül egy írott riport vagy előadás az ügyfél részére.

10. **Kiberbiztonsági projekt-tervek szakértői bírálata**

A kiberbiztonsági, illetve biztonságossági szempontokból kritikus folyamatok esetén már idáig is szabványok hívták elő a fejlesztési- ellenőrzési és üzemeltetési folyamatok felépítését és végrehajtását. Ez a termék- és szolgáltatáskör az Európai Parlamenthez beterjesztett „A digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről” törvényjavaslat alapján a közeljövőben várhatóan jelentősen kibővül lefedve lényegében a teljes IT bázisú spektrumot. A várható új törvény alapvető feladatává teszi az ilyen termékek és szolgáltatások nyújtóinak a kiberbiztonság folyamatos garantálását, ideértve annak karbantartását is. A felhasználó oldalán ugyanakkor ezen kiberbiztonsági szolgáltatások fogadására és a felhasználói rendszer működtetésébe integrálására fel kell készülni. A konzultáció mind az IT alapú termékek és szolgáltatások nyújtóinak, mind pedig felhasználóinak segítséget kínál a fejlesztési- ellenőrzési és üzemeltetési feladatok megfelelő kialakításában.

11. **Koncepció igazolásához kapcsolódó szolgáltatás**

A konzultációs szolgáltatás célja, azon ügyfelek támogatása, akik már felmérték termékükkel, szolgáltatásukkal vagy informatikai rendszerükkel kapcsolatos biztonsági elvárásokat, rendelkeznek az elvárásoknak és biztonsági alapelveknek megfelelő tervvel. A szolgáltatás célja egy adott rendszer tervéhez kapcsolódó prototípus (proof of concept) implementációs kérdéseinek megvizsgálása. A proof of concept a teljesség igénye nélkül modellezi egy rendszer működését, mely alapján eldönthető, hogy érdemes -e befektetni egy teljes, éles környezetben alkalmazható rendszer fejlesztésébe. A proof-of-concept az érdekelt felek, például a projektmenedzserek, a vezetők és a potenciális befektetők számára egy vázlatot ad a végtermékről.

12. **Komponens kiberbiztonsági tesztelése tesztkörnyezetben**

A szolgáltatás célja az ügyfelek által fejlesztett komponensek korai biztonsági tesztelése egy közel valós környezetben. A környezetben különféle valódi és virtuális eszközöket lehet telepíteni, például hálózati eszközöket (kapcsolók, útvonalválasztók, tűzfalak stb.), változatos szolgáltatásokat futtató virtuális gépeket, különféle gyártók változatos PLC-it, különböző gyártók IoT eszközeit. A tesztkörnyezet egy valóshoz közeli környezetet teremt a vizsgált eszköz teszteléséhez. A környezetben különféle vizsgálatokat lehet a fejlesztés korai fázisában elvégezni, mint például funkcionális, teljesítmény vagy biztonsági tesztelés. Az ügyfélnek olyan módon kell meghatároznia a környezetet, hogy az automatikusan felépíthető legyen. Példák a szolgáltatásra: új IoT tűzfal vagy ipari rendszerekre tervezett behatolásdetektáló rendszer korai tesztelése. A szolgáltatás eredménye egy jelentés a tesztelt komponens tulajdonságairól.

13. **Kiberbiztonsági követelmények definiálása**

A konzultációs szolgáltatás célja, hogy segítsen azoknak az ügyfeleknek, akiknek kérdéseik vannak a termékek, szolgáltatások vagy számítógépes rendszerek biztonsági specifikációival kapcsolatban. A szolgáltatás keretében konzultációs jellegű támogatást nyújtunk a mechanizmusok vagy rendszerelemek biztonságos működéséhez szükséges elvárások meghatározásával kapcsolatban, melyek a tervezési és implementációs szolgáltatás alapja. A szükséges biztonsági követelmények meghatározásához összegyűjtjük a fenyegetéseket és a lehetséges támadási forgatókönyveket. A specifikációk részletes leírása révén ez a szolgáltatás lehetővé teszi az ügyfél számára a rendszer fontos biztonsági szempontjainak mélyebb megértését és feltárását. E konzultáció keretében lehetőség

van egy konkrét termékre, illetve szolgáltatásra vonatkozó követelménylista összeállítására, valamint olyan összefoglalók átbeszélésére, melyek a legkorszerűbb rendszerek specifikációit méri fel. Ezen specifikációk segítségével az ügyfelek jobb megértést szereznek, és igénybe vehetik a DigitalTech EDIH által kínált egyéb célzott tanácsadási szolgáltatásokat.

14. **Biztonsági megoldásokkal kapcsolatos tervezés, modellezés**

A konzultációs szolgáltatás célja, hogy segítséget nyújtson azoknak az ügyfeleknek, akik már rendelkeznek termékeikre, szolgáltatásaikra vagy számítógépes rendszereikre vonatkozó kiberbiztonsági specifikációval. A megadott specifikációk alapján a szolgáltatás tervezéssel kapcsolatos kérdésekben nyújt segítséget szoftver- és rendszertervezés területén, beleértve az interaktív kommunikációs folyamatokat is. A tervezési elvek alkalmazása szükséges ahhoz, hogy az alkotóelemek, valamint az általuk alkotott teljes rendszer is ellenálljon a támadásoknak. A konzultáció keretében egy konkrét termék- vagy szolgáltatás tervével, valamint korszerű rendszerek tervezési szempontjainak áttekintésével kapcsolatos egyeztetések történnek. A biztonságos tervezési koncepciók megértése után az ügyfelek igénybe vehetik a DigitalTech EDIH által kínált egyéb célzott tanácsadási szolgáltatásokat.

15. **Biztonságos szoftverek fejlesztése**

A digitális átalakulás következtében sok vállalkozást érint a szoftverfejlesztés, de sokan még mindig nem tudták a biztonságot integrálni a szoftverfejlesztési életciklus (SDLC) modelljükbe. Sokan úgy gondolnak a biztonságra, mint szükséges rosszra, ami arra kényszeríti a fejlesztőket, hogy újra elővegyék véglegesnek vélt programjaikat, és kijavítsák benne a biztonsági szakemberek által azonosított sérülékenységeket. Továbbá, a biztonsági követelményeket sokszor a hasznos program funkcionalitás akadályának tekintik. Ezzel ellentétben a helyes hozzáállás az lenne, hogy a biztonsági követelményeket a fejlesztési életciklus minden szintjén figyelembe vesszük és megpróbáljuk kielégíteni őket, illetve a biztonság minden új program funkcionalitás kialakításánál fontos szempont kellene legyen. Ebben a szolgáltatásban segítünk az ügyfeleknek azonosítani a fejlesztési folyamataik biztonsági hiányosságait, és tanácsot adunk a hiányosságok kiküszöbölésére, pl. biztonságos programozási módszertanok alkalmazására.

Olyan szolgáltatásokat is nyújtunk a szoftverbiztonság kérdéskörében, mellyel rávilágítunk az ügyfelek számára a statikus elemzések jelentőségére és segítünk kiválasztani az igényeiknek leginkább megfelelő biztonsági elemzést. Megtanítjuk, hogyan kell az eszközöket használni, az eredményeit értelmezni és hogyan kell a biztonsági szempontokból relevánsakat megtalálni és kijavítani.

Statikus elemzés során a szoftvereket annak futtatása nélkül elemezzük, nincs szükség egy esetlegesen drága tesztkörnyezet felállítására, csupán a forráskódot vesszük alapul. Ennek eredményeképpen már a tesztelési fázis előtt, hamar visszajelzést kaphatunk a forráskód állapotáról, a benne fellelhető biztonsági problémákról. Manapság ez az egyik elsődlegesen használt eszköz. Mivel számos kódolási szabály és biztonsági előírás ellenőrző eszköz létezik, nem mindig egyértelmű, hogy mikor melyiket kell használni. Ez függhet a használt programozási nyelvtől, a kódbázis méretétől, a szoftver jellegétől, stb. A legmegfelelőbb eszköz kiválasztásához statikus elemzési szakértelemre van szükség, illetve az ügyfél rendszerének, fejlesztői környezetének az ismeretére.

16. **Integrált rendszerek és szolgáltatások biztonsága**

A modern IT rendszerek egyre több belső és külső szolgáltatást használnak céljaik elérése érdekében. Emiatt egy rendszer biztonsága ma már jelentősen függ az általa használt és integrált szolgáltatások biztonságától. Ezen szolgáltatások integrálásának kérdését figyelembe kell venni egy fejlesztési folyamat vagy bármilyen biztonsági analízis során. Ez a konzultációs szolgáltatás segít azonosítani, hogy a kliens által használt üzleti és technológiai környezetben milyen jellegű szolgáltatási függőségek kritikusak, valamint milyen minőségi tulajdonságokat fontos definiálni és folyamatosan mérni ezen szolgáltatásokhoz. Ezek után a konzultáció során átnézzük a jelenlegi szolgáltatásintegrálási, naplózási és mérési gyakorlatokat, és javaslunk olyan további jó gyakorlatokat, amik relevánsak lehetnek az ügyfél számára.

17. **Informatikai rendszerek biztonságos üzemeltetése**

Tanácsadói szolgáltatást nyújtunk IT infrastruktúrák biztonságos üzemeltetése témakörben, ideértve (de nem kizárólag erre limitálva) Windows és Linux szerverek és munkaállomások, lokális hálózatok, és alapvető szolgáltatások (pl. Active Directory, virtuális magánhálózatok, és DHCP) működtetését. Ezen kívül, tanácsot adunk kiberbiztonsági incidensek hatásos kezelésével kapcsolatban, elsősorban a megelőzésre fókuszálva, azaz például a szükséges műszaki előkészületi lépésekkel és egy incidens-kezelő csapat felállításával kapcsolatban, de érintve az incidens elemzés fázisban használható módszereket és eszközöket is. Fontos kihangsúlyozni, hogy nem nyújtunk incidenskezelés szolgáltatást (pl. nem állítunk vissza adatokat egy zsarolóvírus támadás után), csupán tanácsot adunk azzal kapcsolatban, hogy hogyan lehet hatásosan felkészülni egy kiberbiztonsági incidensre (pl. zsarolóvírus támadásra). Ez a szolgáltatás minden olyan ügyfél számára hasznos, mely IT infrastruktúrát üzemeltet, függetlenül annak méretétől és az alkalmazott technológiáktól.

18. **Projekt és termék adatok analízise**

Az informatikai termékek és szolgáltatások fejlesztése, karbantartása és üzemeltetése során számos olyan adat keletkezik, amelyek részletes elemzése alapvető hozzájárulást jelenthet a fejlesztési és karbantartási folyamat hatékonyságának, valamint a termék és szolgáltatás minőségének és biztonságának javításához. A fejlesztési folyamat oldalán az ilyen analízis képes feltárni a hatékonyság és a szolgáltatásminőség szempontjából kritikus szűk keresztmetszeteket és hibaforrásokat. A végtermék üzemeltetéséhez kapcsolódóan a naplózott adatokból vizsgálható a szokásos időkorlátokra és átbocsátóképességre vonatkozó követelmények teljesülése, sőt kimutathatóak az idő- és teljesítmény jellemzőket érintő szándékos és véletlen hibák hatásai is. A konzultáció kiterjed az ezekhez szükséges adatgyűjtési, - tárolási és feldolgozási folyamatokra, valamint adatvizualizációk/ dashboardok tervezésére is.

19. **A gépi tanulás biztonsága**

Ennek a tanácsadási szolgáltatásnak az a célja, hogy segítse az ügyfeleket a gépi tanuláson alapuló szolgáltatásaik és termékeik fő biztonsági és adatvédelmi kockázatainak azonosításában, valamint útmutatást adjon arra vonatkozóan, hogyan lehet ezeket a kockázatokat a legmodernebb technológiákkal mérsékelni. Azokat az ügyfeleket, akiknek nincs világos elképzelésük szolgáltatásaik lehetséges biztonsági kockázatairól, de szisztematikus kockázatértékeléssel meg akarnak felelni a GDPR-nak vagy a közelgő mesterségesintelligencia-rendeletnek, arra biztatjuk, hogy használják ezt a szolgáltatást gépi tanulásuk titkossági, integritási és elérhetőségi problémáinak megismerésére, és hogyan lehet azonosítani az ilyen kockázatokat, valamint hogyan lehet ezeket a kockázatokat különböző védekezési technikákkal kezelni anélkül, hogy a szolgáltatásuk hasznosságát veszélyeztetné.

20. **Alkalmazott kriptográfia**

Ezen szolgáltatás keretében, a kriptográfiai algoritmusok és protokollok különböző alkalmazásaival kapcsolatban adunk tanácsot. A kriptográfia számos hatékony eszközt nyújt információ-biztonsági problémák megoldására, ugyanakkor könnyű ezeket az eszközöket rosszul használni, aminek az lehet a következménye, hogy a kriptográfiára épülő rendszerben sérülékenységek keletkeznek. A tanácsadás keretében segítünk megérteni a leggyakoribb hibákat, és megmutatjuk a helyes használat főbb szempontjait. A szolgáltatás nem csak szigorú értelemben vett kriptográfiai algoritmusokkal foglalkozik, hanem lefedi a kulcsmenedzsment, a véletlenszám generálás, és a side-channel támadások kérdésköreit is, valamint foglalkozik a gyakorlatban használt kriptográfiai protokollok (pl. TLS, IPsec) kérdéseivel is.

21. **Személyes adatok védelmét elősegítő technológiák**

Ennek a tanácsadási szolgáltatásnak az a célja, hogy segítse az ügyfeleket az adatvédelmet elősegítő technológiákkal kapcsolatos ismereteik további bővítésében, és útmutatást adjon ezeknek az úgynevezett PETs-eknek a szervezeten belüli hasznosításához. Azokat az ügyfeleket, akiknek nincs egyértelmű elképzelésük az adatvédelemről, arra biztatjuk, hogy először jelentkezzenek be a DigitalTech EDIH által kínált, azonos nevű (azaz „Személyes adatok védelmét szolgáló technológiák") kompetenciafejlesztési szolgáltatásba. A résztvevők a részvétellel olyan főbb PETs fogalmakkal ismerkednek meg, mint az adatvédelmet segítő kriptográfiai technikák és alkalmazások, a gépi tanulás adatvédelemmel kapcsolatos módszerei, az adatbázisokkal kapcsolatos anonimizálási és

azonosítási mechanizmusok, stb. Ezen tanácsadás során az ügyfelek áttekintést kapnak a meglévő PETs megközelítésekről és alkalmazásokról, hogy kitalálják, hogyan segíthetik ezek a rendszereiket, a szolgáltatásaikat, a szervezetüket és a környezetüket. Amennyiben az ügyfélnek más, az adatvédelemmel kapcsolatos további információra van szüksége, akkor javasoljuk a DigitalTech EDIH által kínált, további adatvédelemmel kapcsolatos tanácsadási szolgáltatásait, mint például az „Adatvédelmi kockázatértékelés és hatáselemzés" vagy „Adatvédelmi jogszabályok, szabványok, irányelvek és megfelelés".

22. **Beágyazott rendszerek biztonsága**

Környezetünket beágyazott rendszerek teszik egyre intelligensebbé, szenzorok, aktuátorok, és beágyazott vezérlők segítségével, melyek lehetővé teszik a környezet paramétereinek érzékelését és az arra adott adaptív reakciót. Az ilyen rendszereket sokszor kiber-fizikai rendszereknek is nevezik, mert bennük számítógépek fizikai folyamatokat felügyelnek vagy vezérelnek. Ezek a rendszerek éppen úgy ki vannak téve a kibertámadások veszélyének, mint más hálózatba kötött rendszerek, ugyanakkor a kibertámadásoknak itt fizikai hatása lehet, mely balesetekhez, vagy akár emberélet elvesztéséhez is vezethet. Ebből kifolyólag a kiberbiztonság alapvető fontosságú a kiber-fizikai rendszerekben, de számos kihívás teszi nehézzé a feladatok megoldását. Olyan ügyfeleknek nyújtunk tanácsadást, akik kiber-fizikai rendszereket (pl. IoT rendszereket, ICS/SCADA rendszereket, járművek közötti kommunikációs protokollokat) terveznek, implementálnak, vagy működtetnek: segítünk azonosítani a fő biztonsági követelményeket és a követelmények kielégítését lehetővé tevő módszereket és eszközöket. A szolgáltatásunk lefedi a biztonsági architektúrák átnézését, beágyazott szoftverek biztonságával kapcsolatos tanácsadást, és a beágyazott világban elterjedt biztonsági mechanizmusok (pl. biztonságos boot, megbízható végrehajtási környezetek, biztonságos távoli szoftver-frissítés) használatával kapcsolatos tanácsadást.

23. **Blockchain alkalmazása IT infrastruktúra biztonságossá tételéhez**

A digitalizált szolgáltatások helyes és biztonságos működésének alapja az infrastruktúra megfelelő működése. A nemzetközi tapasztalatok alapján mind a támadások mind a véletlen meghibásodások szempontjából a legkritikusabb következményekkel azok járnak, amelyek az infrastruktúrát, illetve annak menedzsmentjét érintik.

A mai komplex digitalizált szolgáltatások esetében maga az infrastruktúra is egy rendkívül komplex, gyakran elosztott és több szolgáltató által működtetett részrendszerek együttese. Mind az ezekhez való hozzáférés, mint pedig a menedzsment ennek megfelelően legtöbbször a kritikus elemek közé tartozik.

Az elosztott, több résztvevőre kiterjedő alkalmazások területén rohamosan területet nyer a blokklánc technológia. Ez többek között magas fokú biztonságot és megbízhatóságot garantál akár kooperatívan működtetett alkalmazások esetében is. A konzultáció keretében arra kínálunk segítséget, hogy az hardver-szoftver IT infrastruktúra és a szolgáltatásintegráció keretében milyen alkalmazási lehetőségei vannak a blokklánc technológiának.

A szolgáltatás kiterjed az ismert általános blokklánc használati esetekre és az eseti alkalmazhatóság elemzésére és támogatására is. Előbbiek között kiemelten szerepelnek a rendszerbiztonság blokklánc alapú decentralizált komponens-identitásokkal (DID) támogatása; konfiguráció és hozzáférés kooperatív menedzsmentje és követése; valamint a kritikus infrastruktúra-események naplózása.

24. **Formális verifikáció**

A tesztelés és a különböző kód átvilágítási technikák a szoftveralapú rendszerek minőségének mérésére és javítására szolgáló általános módszerek. A kritikus alkalmazási területeken (pl. autóipari, orvosi, pénzügyi vagy energetikai rendszerek) azonban néha további bizalmi szintre van szükség. A formális verifikációs technikák olyan precíz matematikai algoritmusokon alapuló technikák, amelyek segítségével bizonyítani lehet egy rendszer valamilyen fontos tulajdonságát, vagy példákat lehet mutatni arra, hogy a rendszer hogyan hibásodhat meg. Ezek a technikák előzetes munkabefektetést igényelnek a rendszer modellezéséhez és elemzéséhez, de később olyan problémákra is fényt deríthetnek, amelyeket a hagyományos módszerekkel különösen nehéz feltárni. A BME több évtizedes múltra tekint vissza a formális verifikáció különböző alkalmazási területeken történő használatában, és saját nyílt forráskódú formális verifikációs eszközökkel rendelkezik.

Egy tipikus konzultációs alkalmon 1) megbeszéljük az ügyféllel, hogy a formális verifikáció alkalmazható-e a termékeire vagy rendszereire, 2) közösen azonosítjuk az ügyfél rendszerének azon részeit, amelyek jó jelöltek lehetnek a formális verifikációra, és 3) a BME kisebb példákat mutat a verifikálható tulajdonságokra és a formális verifikáció alkalmazásának potenciális előnyeire. Ha a kezdeti konzultáció ígéretesnek tűnik, egy lehetséges következő lépés lehet a "tesztelés a beruházás előtt" szolgáltatás igénylése.
Ez egy haladó téma. Javasoljuk, hogy előtte vegyen részt egy másik, általánosabb konzultációs szolgáltatásban (pl. "Kiberbiztonsági érettségi felmérés").

25. **Posztkvantum kriptográfia**

A szakértők szerint a nem túl távoli jövőben lehetségessé válik a gyakorlatban is használható kvantum-számítógép létrehozása. Jól ismert, hogy a jelenleg használt aszimmetrikus kulcsúó kriptográfiai algoritmusok (pl. RSA, ECDSA) hatékonyan feltörhetők kvantum-számítógép segítségével. Ezért a kriptográfusok új algoritmusokan kezdtek el dolgozni, melyek hagyományos számítógépeken futnak, de ellenállnak egy kvantum-számítógéppel rendelkező támadónak. Az USA nemzeti szabványügyi szervezete, a NIST pedig egy versenyt írt ki új poszt-kvantum kripográfiai algoritmusok számára, és ennek keretében igyekszik néhány kiválasztott algoritmust szabványosítani. Ráadásul egy nemrég elfogadott magyar törvény szerint néhány szektorban kötelező lesz az átállás a poszt-kvantum sémákra.
Ennek a folyamatnak óriási hatása lesz az IT rendszereinkre, és fel kell készülni ezen új szabványok alkalmazására mindenféle rendszerben, szolgáltatásban, és folyamatban. Ebben a tanácsadói szolgáltatásban segítünk ügyfeleinknek a poszt-kvantum kriptográfia alapjainak megértésében, és feltárjuk előttük, hogy hogyan befolyásolhatja ez az új iránya a kriptográfiának az ő életüket, valamint hogyan tudnak felkészülni az új generációs aszimmetrikus kulcsú kriptográfiai algoritmusok bevezetésére rendszereikbe és szolgáltatásaikba.

26. **Ipari vezérlőrendszerek biztonsága**

A kritikus infrastruktúra-rendszerek (KIR) összetett, ember alkotta elosztott rendszerek, amelyek erőforrásokat állítanak elő, továbbítanak és elosztanak, vagy olyan szolgáltatásokat nyújtanak, amelyek a modern társadalmak megszokott működéséhez létfontosságúak, például víz, élelmiszer, villamos energia, közlekedés, kormányzat, kritikus termelés. Az ipari vezérlőrendszerek (IVR) lehetővé teszik a KIR-kezelők számára, hogy érzékelőkön keresztül figyeljék rendszereiket, vezérlési döntéseket hozzanak és a folyamatváltozókat aktuátorokon keresztül módosítsák. Az operatív technológia (OT) egy gyakran használt kifejezés ezen a területen, amely többnyire átfedésben van az ipari vezérlőrendszerekkel. Az IVR-ek biztonságáról hagyományosan azt gondoltuk, hogy mivel ezek a rendszerek zárt környezetben működtek, azáltal biztonságosak voltak ("biztonság az ismeretlenség által"). Az információs és operatív technológiák (IT-OT) konvergenciájában (vagyis szorosabb összefonódásában) a modern IVR több kapcsolatot létesít az üzleti hálózatokkal. Ez üzleti előnyökkel jár, de növeli az IVR támadási felületét. Egyre növekszik a kibertérből származó, a fizikai térben kárt okozó ismert támadások száma. Ezekben a támadásokban a hackerek hozzáférnek az IVR környezethez, és nemkívánatos változtatásokat hajtanak végre a vezérlőváltozókban, amelyek ezt követően berendezések meghibásodásához, személyi sérülésekhez és környezeti károkhoz vezethetnek. Az IVR felügyelet és a (kiberbiztonsági) helyzetfelismerés általában kulcsfontosságú követelmény. A jogalkotók fokozatosan növelik a kiberbiztonsági érettség elvárt szintjét és a biztonsági ellenőrzések körét, amelyeket a KIR üzemeltetőknek alkalmazniuk kell. Európában a NIS2 Directive kiterjeszti azon KIR üzemeltetők körét, amelyek megfelelő biztonsági ellenőrzéseket kell, hogy alkalmazzanak. Ezzel összefüggésben ez a tanácsadó szolgáltatás képzést és szaktanácsadást nyújt a különféle kritikus infrastruktúra/ipari vezérlőrendszerek tulajdonosainak és üzemeltetőinek.

BLOKKLÁNC

1. **Digitális bizalommal kapcsolatos általános jogi és üzleti szolgáltatások**

A digitális bizalommal kapcsolatos általános jogi és üzleti szolgáltatások: Blockchain/token alapú fejlesztésekhez/vállalkozásokhoz kapcsolódó tanácsadói szolgáltatások, amelyek az adatvédelemre, a

szellemi tulajdon védelmére, a fogyasztóvédelemre és a pénzpiaci szabályozási szempontokra, valamint az ehhez kapcsolódó jogi keretrendszerre öszpontosítanak. Mindez kiegészül a közigazgatás számára nyújtott igény szerinti jogszabályi fejlesztési javaslatokkal, esetleg országbenchmarkokkal. Az előzőekhez kapcsolódó auditok lefolytatása.

2. **Szolgáltatások a digitális bizalom speciális jogi követelményrendszerében**

Szolgáltatások a digitális bizalom speciális jogi követelményrendszerében: Jogi tanácsadás a blokklánc technológiával kapcsolatos területeken (pl. token típus meghatározása, okos szerződések jogi értékelése, kriptoeszközök szabályozási szempontjainak értékelése stb.). A vonatkozó audit lefolytatása.

3. **Szolgáltatások a digitális bizalom gazdasági és pénzügyi követelményeivel kapcsolatban**

Blockchain/token alapú vállalkozásokhoz kapcsolódó tanácsadói szolgáltatások, amelyek segítséget nyújtanak ezen vállalkozások gazdasági és pénzügyi folyamataihoz (cash-flow, fenntarthatóság, stb.)

4. **A digitális bizalmi token gazdaság feltételeihez kapcsolódó szolgáltatások**

A DigitalTech EDIH e szolgáltatás keretében segít felkészíteni az EDIH ügyfeleket az új (token) gazdaság funkcionalitására. Ebben az új (token) gazdasági mechanizmusban (token gazdaságban, sőt web3-ban is) egy kkv-nak vagy a közszférának újfajta gazdasági és jogi környezetre van szüksége a mindennapi működésében. A tokengazdaság kifejezés minden olyan tevékenységet magában foglal, amely tokenekkel és közgazdaságtannal kapcsolatos. Ilyen pl. ha token kibocsájtás történik, akkor mennyi tokent érdemes kibocsájtani, milyen kategóriákkal (security, pénzügyi, stb.) vagy pl. a tokenek értékesítése milyen formában (private/public) és ütemben történjen.

5. **Digitális üzleti folyamatok szolgáltatástervezése, meglévő folyamatok átalakítása, termékfejlesztés**

A digitalizálás alatt álló KKV üzleti folyamatai a digitális térben markánsan másképp fognak kinézni, mint a fizikai térben. Így amikor egy üzleti folyamatot a digitális térre terveznek, annak üzleti logikája más lesz. Szolgáltatásainkkal támogatjuk a digitális termékhez szükséges termékfejlesztési folyamatokat, beleértve a szolgáltatástervezést, az UX tervezést és egyéb kapcsolódó tervezési folyamatokat. A folyamat fő lépései 1) előzetes felmérések, 2) fejlesztési terv készítése, 3) tanácsadói szolgáltatások elvégzése.

Szakterületi audit módszertanok elkészítése (jogi: általános jogi, blokklánc, GDPR, fogyasztóvédelem, szabadalom. Pénzügyi/közgazdasági: általános)

6. **Speciális kriptoeszközök (pl. NFT) létrehozásával kapcsolatos szolgáltatások**

Még egy kriptovaluta modellezése és létrehozása is nagyon speciális tudást igényel, több mint egy évtizedes fennállásuk ellenére. Ezzel szemben a különleges kriptoeszközöket, amelyek egész iparágak forradalmasításának ígéretét hordozzák, a közvélemény még kevésbé érti. Például. fontos példa a művészet digitális jogainak védelmére használt NFT-k, amelyeket egyre gyakrabban alkalmaznak különböző területeken (pl. zenészek). Ez a szolgáltatás tanácsadói szolgáltatásokat nyújt az ilyen megoldások létrehozására.

7. **EBSI – üzleti tervezés támogatása az európai blokklánc szolgáltatási infrastruktúrát célzó alkalmazásokhoz**

EBSI – az Európai Blokklánc Szolgáltatási Infrastruktúrát célzó alkalmazások üzleti tervezési támogatása: Bár az EBSI jelenleg a közszféra szolgáltatásaira összpontosít, hosszú távú célja a felhasználók szélesebb körét is elérni. Az egész EU-ra kiterjedő megoldásokat létrehozni kívánó kkv-knak érdemes felmérniük az EBSI által kínált jelenlegi és közeljövőben rejlő lehetőségeket.

8. **Közigazgatási tanácsadás**

Közigazgatási tanácsadási szolgáltatások keretében a közigazgatás számára speciális szaktanácsadási tevékenységet folytatunk, amely során kiemelt figyelmet fordítunk az EU által kiemelt szolgáltatási területekre: eID, eSignature, eDelivery, e Invoicing. Ezen kívül az EBSI-n futó az Európai Bizottság által elkészített megoldások implementálásához kapcsolódó tanácsadás is ezen szolgáltatás keretében valósul meg.

9. **Blockchain alkalmazhatósági elemzés és tipikus használati esetek**

Tanácsadási szolgáltatásokat nyújtunk annak eldöntésére, hogy a blokklánc/elosztott főkönyvi technológia (DLT) alapú megközelítések alkalmazása előnyös-e egy konkrét digitalizálási vagy innovációs cél elérése, illetve a várható üzleti előnyök szempontjából. A KKV szektor számára az ötletelés és a tervezési gondolkodás megkönnyítése érdekében „csomagokat" állítunk össze tipikus innovációs esetekből, mint adathitelesítés, ellátási lánc és eszközkövetés, intelligens szerződések, identitáskezelés.

10. **Követelmény és üzleti modell vezérelt platform kiválasztása és műszaki tervezés**

A blokklánc-hálózat típusának (nyilvános vagy az együttműködő szervezetek között teljesen zárt hálózat) és az adott technológiai platform kiválasztása döntő lépés a sikeres blokklánc alapú megoldások tervezésében. Tanácsadói és szakértői szolgáltatásokat nyújtunk ezen döntések meghozatalában, az üzleti és extrafunkcionális (teljesítmény, megbízhatóság, rugalmasság, biztonság, titoktartás/adatvédelem) követelmények szisztematikus elemzése alapján. Az alapplatform kiválasztását követően további tanácsadói szolgáltatást nyújtunk egy életképes műszaki koncepció kialakításához.

11. **Meglévő együttműködések és folyamatok áttelepítése blokkláncba, „blokkláncosítás"**

A blokklánc és az elosztott főkönyvi technológiák egyik tipikus alkalmazási területe egy már meglévő digitalizált vállalati/szervezeti (együtt)működés áttelepítése egy új, „biztonságos, hitelességet és letagadhatatlanságot biztosító platformra. Egy ilyen migráció/fejlesztés megnövekedett bizalomhoz, az üzleti folyamatok felgyorsulásához és az egyeztetési/adminisztrációs folyamatok/igények, valamint a vitás helyzetek számának radikális csökkenéséhez vezethet. Szakértői és tanácsadói szolgáltatásokat nyújtunk a megfelelő módszertan kidolgozásához, és annak végrehajtásához. A szervezetközi üzleti folyamatok migrációs aspektusai (kooperatív munkafolyamatok végrehajtása, „érkeztetett" üzenetküldés, közösen kezelt adatok stb.) a „blokkláncosítás" különösen jól ismert és hasznos alkalmazási esetei. Tanácsadási szolgáltatásokat és szakértői útmutatást nyújtunk ebben a témában, a kifejezetten folyamatmodellként rögzített folyamatokhoz (pl. Business Process Model and Notation – BPMN – formátumban) pedig gyors prototípuskészítési lehetőségeket kínálunk.

12. **Blokklánc integráció tervezése és megvalósítása**

Egy tipikus, több szervezetet átfogó blokklánc-alkalmazásnak integrálódnia kell a résztvevő szervezetek meglévő rendszereivel és folyamataival. Ennek az integrációnak számos kritikus szempontja körültekintő és szisztematikus tervezést igényel; fontos példa az eltérő adatmodellek fogalmi harmonizációja a közös főkönyvi modell létrehozásához. Egyre inkább igaz az is, hogy a blokklánc alapú megoldásokhoz több blokklánc-hálózat integrálása szükséges (például nyilvános hálózat és privát „oldallánc" összekapcsolása). Tanácsadási és szakértői szolgáltatásokat nyújtunk a megfelelő integrációs megközelítés és technológia kiválasztásában a projekthez és az integrációs tervezéshez.

13. **Self-Sovereign Identity (SSI), Európai Blockchain Services Infrastructure (EBSI)**

Technológiai értékelési és alkalmazási szolgáltatásokat nyújtunk az EBSI, illetve tágabb összefüggésben a decentralizált identitáskezelés és a Self-Sovereign Identity (SSI) számára.

14. **Platform szakértői szolgáltatások és oktatás (műszaki)**

Szakértői szolgáltatásokat nyújtunk a meghatározó blokklánc platformokhoz, mint A Hyperledger Fabric és az Ethereum. Fabric esetén a szolgáltatás rendszermérnöki aspektusokra is kiterjed, a hálózattervezéstől az intelligens szerződés-végrehajtáson át a teljesítmény biztosításáig.

15. **Blockchain teljesítmény, teljesítőképesség és megbízhatóság biztosítás (műszaki)**

Azon megbízások esetében, ahol már rendelkezésre állnak a tervezési prototípusok, PoC-k vagy MVP-k, empirikus teljesítmény- és megbízhatóságelemzési szolgáltatásokat nyújtunk (amely nagymértékben automatizált hatáselemzésen alapul), amelynek eredményei felhasználhatóak a Test before Invest szolgáltatás keretében is. A kiváltó okok elemzését is elvégezzük, és szükség szerint javaslatokat teszünk a javításra. A szolgáltatás a Hyperledger Fabricre összpontosít, de elérhető Ethereum, valamint Ethereum-kompatibilis/származott platformokon is. Nagyon kritikus felhasználási esetekben validációs célú hibainjektálási kampányok tervezését is elvégezzük.

FINTECH

1. **A szolgáltatástudomány és a vállalati architektúra alkalmazása a pénzügyi szolgáltatások területén:**
   - A célvállalat üzleti elemzése, és hogy szüksége van-e a pénzügyi szolgáltatási technológiákhoz kapcsolódó digitális szolgáltatásokra.
   - A megállapítások és a vállalat igénye alapján a megfelelő módszertanok alapján kidolgozott javaslat: Business Canvas, Context Map, Janus Cones, Customer System, Co-opetition, Value Curve.
   - A célvállalat számára "tennivaló" ajánlás készül arról, hogy a változásmenedzsment módszertan segítségével hogyan lehet a változásokat bevezetni.
   - Támogatás az ajánlás végrehajtásához.

2. **FinTech megoldások, fizetési rendszerek:**
   - Üzleti elemzés a célvállalatról, és arról, hogy szüksége van-e pénzügyi szolgáltatási technológiákon alapuló digitális fizetési szolgáltatásokra.
   - A megállapítások és a vállalat igénye alapján a megfelelő módszertanok alapján kidolgozott javaslat: Business Canvas, Context Map, Janus Cones, Customer System, Co-opetition, Value Curve, Innovative Service Design.
   - A célvállalat számára "tennivaló" ajánlás készül arra vonatkozóan, hogy a változásmenedzsment módszertan segítségével hogyan lehet a változásokat bevezetni.
   - Támogatás az ajánlás megvalósításához.

3. **Az üzleti folyamatok digitális átalakítása a pénzügyben, a blokklánc technológia integrálása az üzleti folyamatokba és munkafolyamatokba:**
   - A célvállalat üzleti elemzése, a problémás területek azonosítása a digitális átalakulás és a pénzügyi technológiai szolgáltatások szempontjából.
   - A digitális átalakulás és a digitális pénzügyek elemzésének alkalmazása.
   - Az Innovatív szolgáltatástervezés módszerének alkalmazása a célvállalatnak szóló, a végrehajtandó feladatokra vonakozó javaslat elkészítése.
   - Az Enterprise Architecture, Business Canvas és a kapcsolódó feltáró technológiák elemzésének alkalmazása javaslatok készítéséhez.
   - Az Innovatív szolgáltatástervezés módszerének alkalmazása a célvállalatnak szóló To-Do javaslat elkészítéséhez.
   - Az ajánlás végrehajtásának támogatása.

4. **Vezetői információs rendszerek – Pénzügyi és vezetői üzleti intelligencia műszerfal:**
   - A célvállalat üzleti elemzése, a problémás területek azonosítása a vállalati erőforrásrendszerek, a döntéstámogató rendszerek és a vezetői információs rendszer modulja (adattárház, műszerfal, vezérlőpanel, valós idejű adatfeldolgozás, felhőszolgáltatások) szempontjából.
   - Az ERP információs rendszerekre vonatkozó követelményelemzés módszerének alkalmazása.
   - Az információs rendszerekre vonatkozó követelményelemzés módszerének alkalmazása.
   - A megállapítások alapján ajánlás készül a célvállalat számára a megfelelő MIS bevezetésének módjára vonatkozóan.
   - Az ajánlás megvalósításának támogatása.

5. **Adatelemzés a pénzügyekben, trendek, előrejelzés:**
   - Üzleti elemzés a célvállalatról, hogy szüksége van-e pénzügyi elemzésre a piaci trendekről, a versenytársakról és a saját üzleti tevékenységéről, és hogyan.
   - Az igényelemzés módszerének alkalmazása az adattudomány alkalmazásához.
   - A megállapítások alapján a tenni valókról ajánlás készül a célvállalat számára arra vonatkozóan, hogy hogyan lehet a gyakori használatra (napi alkalmazások) megfelelő módszereket és algoritmusokat bevezetni.
   - Az ajánlás megvalósításának támogatása.

EDTECH - Szolgáltatásaink később válnak elérhetővé

ÜZLETFEJLESZTÉS

1. **Pénzügyi terv**

Minden vállalkozásnak szüksége van arra, hogy egy alulról felépített pénzügyi tervvel tudja modellezni működését. Ez az alapja minden további tervezésnek, finanszírozásnak és célok felállításának. Személyre szabott tanácsadással állunk a rendelkezésére.

2. **Üzleti terv**

Az üzleti terv a vállalkozás piaci környezetének, versenytársainak, potenciáljának elemzése. Ennek helyes elkészítésében segítünk személyre szabott tanácsadással.

3. **Kockázati- angyal tőke bevonás**

A dinamikus növekedő, innovatív vállalkozások egyik fő finanszírozási módja a kockázati-, vagy angyal tőke. Ebben a speciális folyamatban segítünk személyre szabott tanácsadással.

4. **Pályázati forrás**

Legyen szó nemzeti vagy uniós finanszírozásról, egyedi tanácsadással segítünk annak eldöntésében, melyik a releváns és elérhető a vállalkozás számára. Melyiket és hogyan érdemes igénybe venni, milyen feltételekkel és kötelezettségekkel jár.

5. **Mikrohitel**

A vállalkozások egyik kézenfekvő finanszírozási módja a mikrohitel. Egyedi tanácsadással segítünk annak eldöntésében, melyik a releváns és elérhető a vállalkozás számára. Melyiket és hogyan érdemes igénybe venni, milyen feltételekkel és kötelezettségekkel jár.

6. **Piacelemzés**

A piacelemzés során a piacméretet, az üzleti modellt, a külső hatásokat, a piac dinamikáját vizsgáljuk. Tanácsadóink segítenek vállalkozásának a piac elemzésében - legyen szó piaci terjeszkedésről, tőkebevonásról vagy pályázati célról.

7. **Versenytárselemzés**

A piaci versenyhelyzet és a vállalkozás esélyeinek megítélésében nyújt segítséget tanácsadói csapatunk. A direkt- és indirekt versenytársak helyes feltérképezése fontos feladat a vállalkozás szempontjából - mint ahogy annak naprakészen tartása is.

8. **Célközönség elemzés**

A helyes perszóna alkotás, az adott célközönséghez a szolgáltatások és várható előnyök rendelése fontos feladat a vállalkozás sikerének érdekében. Tanácsadóink segítenek ebben a feladatban.

9. **Piacralépési stratégia**

A piacelemzés, a versenytársak feltérképezése, majd a helyes célközönség azonosítása után a piacralépési stratégia megalkotása következik. Ebben segítenek tanácsadóink.

10. **Termék stratégia**

A piacelemzés, a versenytársak feltérképezése, majd a helyes célközönség azonosítása alapján készül el a termékstratégia. Ez a célközönség problémáihoz igazítja a termék különböző képességeinek elkészülési sorrendjét és fontosságát. Módszertant ad a továbblépéshez és a termék versenyképességének megőrzéséhez.

11. **Környezet vizsgálat**

A vállalkozás környezetének vizsgálata politikai, gazdasági, szociális, technológiai, környezeti és jogi szempontból fontos tevékenység. Akárcsak az ügyfelek és a beszállítók alkuerejének felmérése. Közreműködésünkkel a vállalkozás a megfelelő módszerrel tudja elkészíteni ezt az elemzést.

12. **Üzleti modell**

A megfelelő üzleti modell kiválasztása kritikus lépés a vállalkozás életében. A korábbi elemzési feladatok eredményeinek felhasználásával segítünk azonosítani és kiválasztani a megfelelő üzleti modellt vállalkozásának.

13. **Ötletgenerálás, validáció**

Elég jó ez az ötlet, hogy projektet indítsunk rá? Hogyan győződhetünk meg róla, hogy valós piaci problémát oldunk meg? Tanácsadóink segítségével validációs technikákkal ismertetjük megy ügyfeleinket, valamint segítünk az ötletek kidolgozásában is.

14. **A termékfejlesztés első lépései**

Az agilis, lean folyamatok a sikeres termékfejlesztés záloga. Tanfolyamunkon és workshopjainkat ezzel ismertetjük meg ügyfeleinket, személyre szabottan, az aktuális problémához és célhoz igazodva.

15. **Az első felhasználók megszerzése**

Az első korai ügyfelek megszerzése, az innovációk korai befogadóinak felkutatása kritikus egy új termék vagy szolgáltatás esetében, hiszen ez a valódi validáció. Ezek azonosításában, elérésében segít tanfolyamunk és workshopunk!

16. **Az első fizető ügyfelek megszerzése**

A korai ügyfelek után fizető ügyfelek következnek. Itt kerül felépítésre az értékesítési- és marketing folyamat, a háttér rendszerek és minden, ami a jövőben a bevételtermelést segíti. Ebben nyújt segítséget tanácsadó csapatunk.

17. **A megvalósító csapat felépítése**

Egy cég különböző fázisaihoz különböző csapat szükséges. Az elején alkotók, később működtetők és növekedést serkentők. Hogy az adott szervezetnek mikor mi a legjobb, ebben segít tanácsadói csapatunk.

Függelék a közös adatkezelésről

AZ ADATKEZELŐK KÖZÖS TÁJÉKOZTATÁSA AZ ADATKEZELÉS TÁRGYÁRÓL, CÉLJÁRÓL ÉS ALAPVETŐ NYILATKOZATAIK

1. Az adatkezelők kijelentik, hogy közös adatkezelésük során a tevékenységük körében megszerzett adatokat a mindenkor hatályos jogszabályoknak megfelelően kezelik. Az adatkezelők tiszteletben tartják az érintettek személyes adatait. A tudomásukra jutó valamennyi adatot és tényt bizalmasan kezelik, azokat kizárólag az adatkezelési céloknak megfelelően használják fel. Az adatkezelők az adatkezelését kizárólag az elektronikus hírközlésről szóló 2003. évi C. törvény, az elektronikus kereskedelmi szolgáltatások, az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, valamint az Európai Unió előírásainak (pl. GDPR) megfelelően és egyéb jogszabályi kötelezettségeiknek elvégzésének céljából végeznek. Adatkezelés jogszerűsége és az adatkezelés alapelvei összhangban vannak az adatvédelemmel kapcsolatos hatályos jogszabályokkal. Amennyiben jogszabályi feltételei fennállnak, hatósági felszólításra, az adatkezelők a személyes adatok szolgáltatására és kiadására kötelesek.

2. Az adatkezelést jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzik az adatkezelők. A Felek a kezelt adatok körét elsősorban a fenti jogszabályokban foglaltakra korlátozzák, kiegészítve az ugyancsak jogszabályi kötelezés alapján kezelt személyes adatokkal. Az adatkezelés során érvényesül az adattakarékosság elve, mely alapján az adatkezelés célja szempontjából megfelelő és relevánsnak kell lennie, és a szükségességre kell korlátozódjon. Az adatkezelésnek pontosnak és szükség esetén naprakésznek kell lennie. E körben az adatkezelők minden ésszerű intézkedést megtesznek annak érdekében, hogy a pontatlan adat haladéktalanul törlésre vagy helyesbítésre kerüljön. A személyes adatok korlátozott, az adatkezelés céljának eléréséhez szükséges ideig kerülnek tárolásra. Az adatkezelők iktatásra kötelezettek, ezért az adatok tárolási meghatározott időtartamok a jogszabályoknak megfelelően meghatározottak. A személyes adatok kezelése során az adatkezelők biztosítják az adatok jogosulatlan vagy jogellenes kezelésével és véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet.

3. Az adatkezelők mindent megtesznek annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsák. Ennek értelmében az adatkezelők adatkezelési tájékoztatókat alkottak és hoztak nyilvánosságra. Ezek a tájékoztatók elérhetőek a Felek által működtetett elektronikus csatornákon, rendszereken keresztül. Az adatkezelési tájékoztatók mellett, a Felek által megjelölt adatvédelmi tisztviselők bevonásával az érintettek kérdéseire adandó egyedi válaszokkal tesznek eleget tájékoztatási kötelezettségüknek. Az adatkezelési

folyamatokban résztvevő munkavállalókat és az adatfeldolgozókat titoktartási kötelezettség terheli.

4. Az adatkezelők úgy állapodnak meg, hogy az érintettek, az Adatkezelőkről, a kezelt adatok köréről, céljáról, az őket megillető jogokról és azok érvényesítési lehetőségeiről elsősorban a nyilvánosságra hozott Adatkezelési tájékoztatókból informálódhatnak. Ezen felül a Konzorciumi Tagok által adott egyedi tájékoztatást kapnak

a) hozzáférési jog: az adatkezelés folyamatában az érintett jogosult hozzáférni a róla tárolt adatokhoz, és tájékoztatást kapni a róla kezelt, illetve feldolgozott adatok céljáról, jogalapjáról, tárolásáról és tárolás időtartamáról. A tájékoztatási jog kiterjed a személyes adatok helyesbítésére, törlésére, kezelés korlátozására, illetve a felügyeleti hatósághoz címzett panasz benyújtásának lehetőségéről való tájékoztatásra. Az adatkezelők az érintett jogai gyakorlására irányuló kérelme teljesítése érdekében lehetőség szerint mindent megtesznek. Az adatkezelők az érintett jogainak gyakorlását, a személyének egyértelmű beazonosításához kötik.

b) helyesbítéshez való jog: az érintett jogosult kérni, hogy a rá vonatkozó pontatlan, vagy hiányos adatokat az adatkezelők helyesbítsék

c) törléshez (elfeledtetéshez) való jog az érintett kérelmére az adatkezelők törölik az érintettről tárolt adatokat, ha az alábbi indokok valamelyike fennáll: a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték; az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok a további adatkezelésre; Az adatkezelő által kezelt személyes adatokat az adatkezelés jogalapjának megszűnését, követő rövid időn belül – az Adatvédelmi Szabályzatban foglaltaknak megfelelően - törölni kell. Az adatkezelés kapcsán az érintett csak akkor élhet a törléshez való jogával, ha az Adatkezelőkre ruházott közfeladat végrehajtásához az adat nem szükséges. Az iktatott anyagoknak az őrzési idő végéig a levéltárba adandó iratok vonatkozásában az adatok törlése az iratok integritásának sérelme nélkül nem valósítható meg, ezért a törlési kérelem e vonatkozásban nem teljesíthető.

d) adatok zárolásához való jog: Az adatkezelők zárolják a személyes adatot, ha az érintett ezt kéri, vagy ha a rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adat kizárólag addig kezelhető, ameddig fennáll az adatkezelési cél, amely a személyes adat törlését kizárta.

e) korlátozáshoz való jog: ha felmerül az érintettről kezelt személyes adatok pontatlansága, jogellenessége, szükségtelensége, vagy az érintettnek az adatkezelésre vonatkozó tiltakozása, az érintett kérheti, hogy korlátozzák az adatkezelők ezen adatok vonatkozásában az adatkezelést.

g) tiltakozáshoz való jog: Az érintett bármikor tiltakozhat az adatkezelés ellen, ha álláspontja szerint az Adatkezelők a személyes adatát az adatkezelési tájékoztatóban megjelölt céllal összefüggésben nem megfelelően kezelték. Ebben az esetben az Adatkezelőknek kell igazolnia, hogy a személyes adat kezelését olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és

szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak

5. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. Az adatkezelők az informatikai biztonságra vonatkozó szabályzataik szerint járnak el. A személyes adatokkal kapcsolatos adatvédelmi incidensek esetére adatvédelmi incidenskezelési tervet fogadnak el az adatkezelők. A szerveren tárolt adatokhoz az adatkezelők és az adatfeldolgozó munkatársai a saját szabályzataikban és az adatfeldolgozási szerződésben foglaltaknak megfelelően férnek hozzá, feladatukkal összefüggésben és arra korlátozottan. A hozzáférés jelszóval védett. A szerveren végrehajtott műveleteket a szerver tárolja. Az adatkezelők munkatársait az közös adatkezelés során titoktartási kötelezettség terheli. Az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt az adatkezelők kötelesek megtéríteni. Ha az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát az adatkezelők együtt, vagy külön megsértik, az érintett sérelemdíjat követelhet. A felsorolt esetekben az érintettel szemben és a Nemzeti Adatvédelmi és Információszabadság Hatóság kötelezése esetén az adatkezelők felelőssége egyetemleges.

Függelék a szerződéskötés menetéről

Szerződés megkötésének folyamata képzési szolgáltatás esetén

Jelen pont szerint a leendő Ügyfél Ajánlattevőnek minősül. Ajánlattevőt bárki képviselheti a regisztráció során, Ajánlattevő képviselőjének nem kell cégképviseletre jogosult személynek lennie, de Szolgáltató jogosult vizsgálni azt, hogy a felhasználó rendelkezik-e az Ajánlattevőtől érvényes meghatalmazással az ajánlat megtételére. Ajánlattevő képviselője automatikusan kapcsolattartóvá válik – ettől a Felek a megrendelőben foglaltak szerint eltérhetnek. Az ajánlat megtételéhez a képviselő köteles a megrendelőben kért adatokat megadni.

A Szolgáltatást megrendelő szervezet tudomásul veszi, hogy a Szolgáltatást nyújtó szervezet részére a megrendelő elküldésével olyan ajánlatot tesz, amely ajánlati kötöttséggel jár. Az ajánlatnak a Szolgáltatást nyújtó jelen Általános Felhasználási Feltételei a részét képezik. A Szolgáltatást megrendelő szervezet elfogadja, hogy a Szolgáltatást nyújtó szervezet jelen Általános Felhasználási Feltételeit köteles előzetesen megismerni, azt követően elfogadni.. A Szolgáltatást nyújtó szervezet Általános Felhasználási Feltételei akkor is az ajánlat alapján létrejövő szerződés részét képezik, ha a Szolgáltatást megrendelő szervezet eltérő tartalmú szerződési feltételeket kommunikál a Szolgáltatást nyújtó szervezet felé.

Szerződés megkötésének folyamata képzési szolgáltatás esetén

A DigitalTech EDIH esemény weboldalán történt sikeres felhasználói fiókregisztráció és bejelentkezés után, a képzések aloldalán lehetőségünk van a képzésekre regisztrálni képzések aloldalán. A résztvevők számának beállítása után, megadjuk a részvevők adatait, majd a „Mentés és véglegesítés” gombra kattintva összesítve láthatjuk a jelentkezés részleteit, amit az Általános felhasználási feltételek elfogadásával véglegesíthetünk. Jelentkezés után a résztvevőket a képzés tartó intézmény munkatársa felkeresi elektronikusan, hogy a Felnőttképzési törvénynek megfelelően képzési szerződés írjanak alá a képzés résztvevőjével. A szerződés a képzést tartó intézmény és a résztvevő, mint magánember között jön létre. A szerződéskötés után a résztvevő jogosult a képzésen való részvételre.

Tanácsadás – regisztráció folyamata

A felhasználó (minden esetben a szerződéskötő Vevő) a DigitalTech EDIH weboldalán meglátogatja a szolgáltatások aloldalakat vagy a jelentkezés aloldalt.

A szolgáltatások aloldalakon a „Jelentkezés” gombra kattintva eljut a regisztrációs űrlapig.

Megadja a regisztrációs űrlapon kért információkat, majd elfogadja a DigitalTech EDIH adatvédelmi tájékoztatóját, a program általános felhasználási feltételeit és a szervezetére vonatkozó nyilatkozattételt majd a „Beküldés” gombra kattintva sikeresen leadja jelentkezését a DigitalTech EDIH programba.

A sikeres jelentkezés tényét a rendszer rögtön visszajelzi a visszaigazoló képernyőképet, továbbá a rendszer egy visszaigazoló emailt küld a megadott kapcsolattartó és a cégképviseletre jogosult személy email címére. A jelentkezés önmagában még nem egyenlő a regisztráció sikerességéről.

A kapcsolattartó visszaigazolást kap a feldolgozott információk bekerülésének sikerességéről, a cégjegyzésre jogosult személy pedig értesítő emailt kap a jelentkezés tényéről.

A jelentkezési igény feldolgozása után, amennyiben a cég/szervezet jogosult a programban való részvételre, úgy a DigitalTech EDIH munkatársa felkeresi a kapcsolattartót, hogy időpontot egyeztessenek az orientációs értekezletre.

Az orientációs értekezleten az ügyfél megismerkedik a DigitalTech EDIH kapcsolattartójával és egyeztetik a regisztrációkor megadott adatokat, illetve közösen felmérik az ügyfél igényeit, amely alapján közösen meghatározzák azokat a szakterületeket, amelyek szolgáltatásait igénybe veszi az ügyfél.

Az orientációs értekezlet után az ügyfél email értesítést kap az orientációs értekezleten közösen meghatározott szolgáltatásokról.

Az orientációs értekezlet után a DigitalTech EDIH szakterületi munkatársa keresi meg az ügyfél kapcsolattartóját, amely során időpontot egyeztetnek a szakterületi mély interjúra.

A szakterületi mélyinterjú során az ügyfél megismerkedik az adott szakterület szakembereivel és részletekbe menően felmérik pontosan az ügyféligényt, amely alapján megrendelő készülhet.

A mélyinterjú után az ügyfél megkapja a De Minimis/innovációs támogatás keretre elszámolandó megrendelő az adott szakterületi szolgáltatótól.

A megrendelő elfogadása aláírással történik az cég/szervezet képviselője, vagy az általa írásban meghatalmazott személy által.

A megrendelő elfogadása után elkezdődik a szolgáltatás.

A szolgáltatás teljesítésével a DigitalTech EDIH munkatársa egy teljesítési igazolást állít ki, amelyet kiküld a megadott kapcsolattartó és a cégképviseletre jogosult személy email címére. A teljesítési igazolást az ügyfél alá kell írja, és az vissza kell juttassa a DigitalTech EDIH munkatársa részére.

A teljesítési igazolás aláírásával a szolgáltatás hivatalosan is lezártnak tekintendő.

A DigitalTech EDIH munkatársa a teljesítési igazolás alapján kiállítja a De Minimis/Innovációs támogatás igazolást, amely szükséges a könyvelésben való elszámoláshoz. A De Minimis/Innovációs támogatás igazolást emailben küldi ki az ügyfél részére.

A De Minimis/innovációs támogatás igazolás kiállítása után az ügyfélnek a DigitalTech EDIH ügyfélkezelő rendszere automatikusan kiküld egy elégedettséget felmérő kérdőívet, amelyet az ügyfélnek a DigitalTech EDIH általános felhasználási kötelezettsége alapján ki kell töltenie.

A De Minimis/innovációs támogatás igazolás kiállítása után az ügyfélnek a DigitalTech EDIH ügyfélkezelő rendszere egy év eltelte után automatikusan kiküld egy digitális érettséget felmérő kérdőívet, amelyet az ügyfélnek a DigitalTech EDIH általános felhasználási kötelezettsége alapján ki kell töltenie.

A digitális érettséget felmérő kérdőív kitöltésével az ügyfélnek a DigitalTech EDIH programban való részvétele hivatalosan is lezárul.

Képzés – regisztráció folyamata

A felhasználó a DigitalTech EDIH elektronikus ügyfélkapcsolati rendszerén meglátogatja a képzések oldalt.

A képzések oldalon a „Jelentkezés” gombra kattintva a felhasználó átirányításra kerül a DigitalTech EDIH rendezvényeit és képzéseit kiszolgáló aloldalra, ahol megtalálja a képzésre vonatkozó elérhető összes információt.

A képzések aloldalán a „Jelentkezés” gombra kattintva a felhasználó eléri a regisztrációs űrlapot.

Megadja a regisztrációs űrlapon kért információkat, majd elfogadja a DigitalTech EDIH adatvédelmi tájékoztatóját, a program általános felhasználási feltételeit és a szervezetére vonatkozó nyilatkozattételt majd a „Beküldés” gombra kattintva sikeresen leadja jelentkezését a DigitalTech EDIH programba.

A regisztrációs űrlap kitöltésével a DigitalTech EDIH ügyfélkezelő rendszere létrehoz egy felhasználói fiókot, amelyről értesítési emailt küld a bejelentkezéssel kapcsolatos adatokkal. A felhasználói fiók segítségével gyorsíthatja a jövőbeli képzésre való jelentkezés adminisztrációját.

A felhasználói fiókba való bejelentkezés után lehetőség van az adott képzésrekre való jelentkezésre. A jelentkezés során több részvevő is megadható.

A jelentkezés után a DigitalTech EDIH ügyfélkezelő rendszere visszaigazoló emailt küld a képzésre való jelentkezés sikerességéről. Továbbá információs emailt küld ki a jelentkezés során megadott résztvevők email címére.

Jelentkezés után a képzést tartó szervezet munkatársa felkeresi az ügyfelet a megadott elérhetőségeken a képzésre vonatkozó szerződés megkötése céljából.

A szerződés aláírása után az ügyfél jogosult a képzésen való részvételre.

A képzés előtt az ügyfél emlékeztető emailt kap a képzés részleteiről.

A képzés időpontjában az ügyfél jelenléti íven adminisztrálja magát, csak így lesz jogosult a De Minimis igazolás kiállítására.

A képzés után a DigitalTech EDIH ügyfélkezelő rendszere a jelenléti ív alapján kiállítja a De Minimis igazolást, amelyet emailben küld ki résztvevő részére.

A De Minimis igazolás mellett a rendszer egy elégedettségi kérdőívet is kiküld a résztvevőnek.

A képzést tartó szervezet kiállítja a képzéshez tartozó oklevelet, amelyet emailben küld ki a résztvevőnek.

A képzésen való részvétel után a résztvevő személy által képviselt cég/intézmény a DigitalTech EDIH általános felhasználási feltételei alapján ki kell töltsön egy úgynevezett digitális érettséget felmérő tesztet. Erről a DigitalTech ügyfélkezelő rendszere emailt küld a cég/intézmény kapcsolattartójának.

A digitális érettséget felmérő teszt kitöltése után hivatalonsan is zárul az ügyfél DigitalTech EDIH programban való részvétele.