Információbiztonsági tájékoztató

HolAzAutó Fleet rendszer

Impresszum

Jelen dokumentum célja a szolgáltatást igénybevevő előfizetők tájékoztatása azzal kapcsolatban, hogy a HolAzAutó Fleet rendszerben miként biztosítjuk az elektronikus formában kiállított bizonylatok - vonatkozó jogszabályoknak megfelelő - megőrzését.
A HolAzAutó Fleet rendszer a Mobile LBS Kft által fejlesztett szoftver rendszer melynek rövid leírását ezen dokumentum tartalmazza, a teljes funkcionalitás felhasználói leírása a szerződött ügyfelek felhasználói számára elérhető online súgóban olvasható.

A Mobile LBS Kft adatai:

Cégjegyzék szerinti elnevezése:	**Mobile LBS Korlátolt Felelősségű Társaság**
Székhelye:	**7625 Pécs, István utca 7. 1. em. 6. ajtó**
Cégjegyzékszám:	**02-09-078039**
Adószám:	**23560897-2-02**
E-mail:	**info@hola.hu**
Telefon:	**+36 80 296 890** (ingyenesen hívható)
Vezető tisztségviselő:	**Tóth Attila ügyvezető**
Általános szerződési feltételek:	**https://holazauto.hu/aszf/**
Adatvédelmi tájékoztató:	**https://holazauto.hu/adatkezelesi-tajekoztato/**

Bevezető

A 2000. évi C. törvény a számvitelről (továbbiakban Számviteli törvény) a 167. §-ban definiálja a könyvviteli elszámolást közvetlenül alátámasztó bizonylat általános alaki és tartalmi követelményeit, illetve a 169. §-ban rendelkezik a könyvviteli elszámolást közvetlenül vagy közvetetten alátámasztó bizonylatok megőrzéséről.
Az elektronikus formában kiállított bizonylat megőrzéséről a 169. § (5). pontjában rendelkezik: *"Az elektronikus formában kiállított bizonylatot – a digitális archiválás szabályairól szóló jogszabály előírásainak figyelembevételével – elektronikus formában kell megőrizni, oly módon, hogy az alkalmazott módszer biztosítsa a bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét"*
Nevezett rendelet az 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól ami az elektronikus formában kiállított bizonylatokkal kapcsolatban az alábbiak szerint rendelkezik:

- 3. §
    - (1) A megőrzésre kötelezett a megőrzési kötelezettség lejártáig folyamatosan köteles biztosítani, hogy az elektronikus dokumentum megőrzése olyan módon történjen, amely védi az elektronikus dokumentumot a törlés, a megsemmisítés, a véletlen megsemmisülés, az utólagos módosítás és sérülés, valamint a jogosulatlan hozzáférés ellen.

    - (2) A megőrzésre kötelezett köteles biztosítani, hogy az őrzött elektronikus dokumentum értelmezhetősége, olvashatósága - például a dokumentum megjeleníthetőségét lehetővé tevő szoftver- és hardverkörnyezet biztosításával - a megőrzési kötelezettség időtartama alatt megmaradjon.
- 6. §
    - (1) Az elektronikus dokumentum megőrzésére olyan zárt rendszer is használható, amely a dokumentum keletkezésének vagy a megőrzésre kötelezetthez történő megérkezésének időpontjától biztosítja a 3. § (1) bekezdésében foglalt követelmények teljesítését.
    - (3) A zárt rendszerű archiválást lehetővé tevő szoftver vagy informatikai megoldás fejlesztőjének írásban kell nyilatkoznia arról, hogy az maradéktalanul megfelel a jogszabályi előírásoknak.
    - (4) A zárt rendszerű archiválást lehetővé tevő szoftver vagy informatikai megoldás fejlesztője és a megőrzésre kötelezett egyetemlegesen felelnek azért, hogy az alkalmazott zárt rendszerű archiválási folyamat megfelel a 3. § (1) bekezdésében foglalt követelményeknek.
    - (5) A zárt rendszerű archiválást lehetővé tevő szoftvernek vagy informatikai megoldásnak olyan dokumentációval kell rendelkeznie, amely részletes tájékoztatást nyújt legalább az alábbiakról:
        - a) szoftver vagy informatikai megoldás működésére vonatkozó áttekintő folyamatok,
        - b) alkalmazott technológiák,
        - c) alkalmazott szabványok,
        - d) zárt rendszerű archiválást garantáló megoldások,
        - e) folyamatba épített és utólagos informatikai és belső ellenőrzési tevékenységek.

Szándékunk szerint jelen tájékoztató szolgál a fentiek alapján meghatározott, részletes tájékoztatást nyújtó dokumentumként

e-Menetlevél és útnyilvántartás (Journey form)

A HolAzAutó Fleet rendszer e-Menetlevél és Útnyilvántartás (fejlesztői kódnevén Journey form) modul automatikus, manuális, illetve hibrid módon képes előállítani a járművekbe szerelt GPS tracker által mért koordináták, menetdinamikai adatok és hozzá kapcsolódó perifériák alapján a járműhöz használni szükséges útnyilvántartás és menetlevél bizonylatokat.
Ezek az elektronikus formában kiállított bizonylatok a könyvviteli elszámolást közvetlenül vagy közvetetten alátámasztó bizonylatoknak minősülnek, így a számviteli törvényben előírt megőrzési és reprodukálhatósági követelmények érvényesek rájuk. A menetlevél ezzel együtt - a 261/2011. (XII. 7.) Korm. rendelet értelmében - szigorú számadású bizonylatnak minősül.
Ügyfeleink számára a rendszer működésével kapcsolatos online felhasználói kézikönyvet biztosítunk, melyet minden felhasználó elér az alkalmazás felületekről.
Jelen dokumentumban az kerül rögzítésre, hogy ezen elektronikus úton előállított dokumentumok esetében hogyan biztosítjuk a bizonylatok és az azokhoz kapcsolódó adatok

megőrzését, sérthetetlenségét, reprodukálhatóságát, illetve az ezekhez szükséges informatikai rendszer folytonos rendelkezésre állását.

A HolAzAutó rendszer rövid bemutatása

A HolAzAutó Fleet rendszer a Mobile LBS Kft által fejlesztett szoftver rendszer mely a gépjármű flottával (vagy akár egyetlen gépjárművel) rendelkező vállalkozások, intézmények illetve magánszemélyek részére biztosít a járművek üzemeltetésével kapcsolatos funkciókat.
A működés meghatározó alapja, egy a járműbe beszerelt, vagy hordozható módon csatlakoztatható, GPS koordináták és egyéb perifériák adatainak mérésére, továbbítására alkalmas eszköz (GPS tracker, mobil telefonkészülék vagy tablet) melynek nyers adatait a ***"receiver"*** kiszolgáló fogadja, majd az eszközhöz beállított szoftverrendszer felé továbbítja.
A fogadó rendszer - esetünkben a HolAzAutó Fleet - fogadja, illetve folyamatosan végzi a nyers adatokból az emberi agy számára feldolgozható, további feldolgozásra, képernyős vagy egyéb formátumban való megjelenítésre alkalmas adathalmazok előállítását ezekből a nyers adatokból.
A szoftverrendszert alkotó WEB-es és mobil alkalmazások többrétegű architektúrában csatlakoznak a rendszerhez, mely arcitektúrában különböző feldolgozási process-ek, az adatbázis és az üzleti logika teljesen elválik a kliensektől. A kliensek - authentikációt követően - különböző service-eken keresztül kérhetnek adatot a kiszolgálótól, melyektől kizárólag a már megjelenítendő adatokat kapják, azaz a klienseken üzleti logika nem került implementálásra.
A kliensek titkosított csatornákon (https, TLS, stb) kommunikálnak a kiszolgálóval.
A kliensek a szerver felé küldött adatokat digitális aláírással látja el. (A szerver felé küldött adatokból képzett hash-t titkosítja a saját privát kulcsával. A szerver oldala kulcs publikus párjával ellenőrzi az aláírást.)

A rendszert alkotó felhasználói szoftverek

- HolAzAutó WEB: A szerződött ügyfelek felhasználói számára elérhető WEB-es felhasználói felület
- HolAzAutó Android: A szerződött ügyfelek Androidos mobil készüléket használló userei számára elérhető alkalmazás
- HolAzAutó iOS: A szerződött ügyfelek Apple mobil készüléket használló userei számára elérhető alkalmazás
- GEO GPS Admin: A szolgáltató Mobile LBS Kft értékesítő, adminisztratív, fejlesztő és supportos kollégái számára elérhető adminisztrációs felület, melyen a rendszer, az előfizetők, az előfizetői szerződések, illetve a GPS eszközök paraméterezése, illetve a számlázással kapcsolatos tevékenységek végezhetők.
- HolAzAutó Support: A szolgáltató Mobile LBS Kft fejlesztő és supportos kollégái számára elérhető műszaki adminisztrációs felület, melyen a rendszer, illetve a GPS eszközök magasabb, technikai szintű paraméterezése történik.

Funkcionalitás

A rendszer - a teljesség igénye nélkül - az alábbi funkciócsoportokból, modulokból áll:

- Ügyfél és felhasználói profil adatok
- Flotta ellenőrzés

    - Aktuális pozíciók
    - Múltbéli pozíciók
    - Kiértékelés
    - Sofőr magatartás elemzés
    - Lekérdezések, riportok
- Szállítások, járatok modul
- Alapadatok, készletek kezelése
- Flotta események és költségek
- e-Menetlevél és útnyilvántartás
- szervíz asszisztens
- Szabálykezelő
- Jogosultságkezelés (object permisson)
- Eseményfigyelés
- Tachográf kiolvasás
- Parkolás rendszer
- Egyedi nyilvántartások
- Dokumentumtár
- Üzenetküldő rendszer (messenger)
- Ügyfélszolgálat

A modulok és funkciók teljes leírása angol és magyar nyelvű felületérzékeny online súgóban érhető el.

Liszenszelés

A szoftverrendszer a Mobile LBS Kft önálló szellemi terméke, melyet (szerződéstől függően havi, negyedéves, féléves, éves vagy egyéb módon meghatározott díjazással) szolgáltatásként értékesít természetes és jogi személyek részére.

A rendszer védelme, a zártságért tett intézkedések

Zárt rendszerű archiválást lehetővé tevő szoftver vagy informatikai megoldás értelmezése.

Az 1/2018. (VI. 29.) ITM rendelet nem határozza meg a zárt rendszerű archiválást lehetővé tevő szoftver vagy informatikai megoldás fogalmát.
A magyar jogban a zárt informatikai rendszer több jogszabályi rendelkezésben is előfordul, azonban a fenti fogalmat - hasonlóan az ITM rendelethez - nem definiálja egyik sem egzakt módon.

Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Kormányrendelet értelmezésében:

- **zárt védelem**: az összes számításba vehető fenyegetést figyelembe vevő védelem
- **zárt rendszer**: rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja, működése jogszabályon vagy meghatározott résztvevők közötti megállapodáson alapul, és harmadik felet nem érint

Az az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény értelmezésében:

- **zárt védelem**: az összes számításba vehető fenyegetést figyelembe vevő védelem

A pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Kormányrendelet szintén hivatkozik az informatikai zártságra, viszont azt általános értelemben nem definiálja, kizárólag a pénzügyi intézmények, biztosítók, befektetési vállalkozások és árutőzsdei szolgáltatók szigorú szabályozásához igazítva állít fel követelményrendszert a 5/B. §-ban.

Az informatikai rendszerek zártsági vizsgálatát és tanúsítását végző akkreditált szervezet (Certop Informatikai Tanúsítási Szolgáltatások Kft.) a tanúsítási eljárás során azt a szabályt követi, hogy
“Az elektronikus információs rendszer akkor felel meg az általános információbiztonsági zártsági követelményeknek, ha annak tervezése, implementálása és működtetése során az összes releváns veszélyt (fenyegetést) figyelembe vették és a szükséges adminisztratív, logikai és fizikai intézkedéseket megtették.”
(forrás: https://it.certop.com/informatikai-rendszer-zartsag-vizsgalat-szamlazasi-rendszer/)

Az állami és önkormányzati szervek esetében ezen adminisztratív, fizikai és logikai követelmények gyűjteményét a 41/2015. (VII.15.) BM rendelet határozza meg.

A nemzetközi jó gyakorlat jellemzően olyan állapotként határozza meg az informatikai zártságot, amely képes biztosítani a kezelt adatok bizalmasságát, integritását és rendelkezésre állását és a rendszer elemei teljes körű, a kockázatokkal arányos, folyamatos védelmet biztosítanak ezen adatoknak.

A fenti fogalom meghatározások és a rendeletek szövegezése alapján az az értelmezés látszik elfogadhatónak, amely szerint a zárt rendszerű archiválást lehetővé tevő szoftver vagy informatikai megoldás a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja azzal, hogy az archiválandó elektronikus dokumentum folyamatos, teljes körű és a kockázatokkal arányos bizalmasságát, integritását, rendelkezésre állását biztosítja.

Rendszerünket ennek szellemében terveztük és implementáltuk, jelen dokumentációt és 1. számú mellékletét képező **Jogszabályi megfelelőségi nyilatkozatot** fenti elvárások szerint fogalmaztuk meg.

Kockázatmenedzsment

Információbiztonsági tevékenységünk alapja a kockázatfelmérés, a kockázatelemzés alapján kialakított információbiztonsági eljárásrend és az alapján alkalmazott technológiák.

A kockázatfelmérés és elemzés során

- Meghatározzuk a vállalat működése és a szolgáltatás biztosítása szempontjából kritikus rendszereket.

- azonosítjuk az ezen rendszerek működését lassító vagy megakasztó veszélyforrásokat.
- elemezzük a veszélyforrások bekövetkezési valószínűségét.
- elemezzük a veszélyforrások által okozható kárt.
- az azonosított kockázatokat kategorizáljuk.

Ezek alapján
- Meghatározzuk az elviselhető kockázatokat
- védekezési stratégiákat dolgozunk ki a megelőzési (prevencion), az érzékelési (detection) és kijavítási (correction) szintekre.
- vészhelyzeti forgatókönyvet (DRP) alakítunk ki az üzletmenet folytonosság (BCP) érdekében.
- biztosítjuk az ezekhez szükséges technikai, pénzügyi és humán erőforrásokat

Fejlesztési irányelvek

Külön eljárásban került összefoglalásra, hogy a rendszer fejlesztése során milyen irányelveket, szabályokat kell követni. Az eljárásban az alábbi szabályok kerültek rögzítésre:
- Mely fejlesztőkörnyezet használható, illetve annak IDE beállítása
- verziókövetéssel kapcsolatos szabályok, GITLab használata
- commit és push szabályok
- Java osztályokkal, deklarációkkal kapcsolatos szabályok
- megtévesztő elnevezések mellőzése
- commit előtti fejlesztői teszt
- fejlesztői gépeken tesztkörnyezet kialakítása
- logger használata
- POM struktúra
- Artifact-ok kialakítása, felépítés
- verziószámok kezelése
- snapshot használata
- frissítési workflow
- hibák megelőzése

Többrétegű architektúra

A HolAzAutó rendszer többrétegű arhitektúrában került kialakításra.
A többrétegű architektúra a szoftverfejlesztésben alkalmazott kliens-szerver architektúra, melyben a megjelenítés, az adatkezelés és az üzleti logika különálló folyamatokra van bontva.
Az alkalmazás rétegekre bontásával egyrészt könnyen karbantartható és fejleszthető rendszert hoztunk létre, másrészt a rétegek elkülönítése nagyban védi a működést és a tárolt adatokat a rosszindulatú támadásokkal szemben, mivel kizárólag authentikációt követő webszervíz hívásokkal lehet adatokat kérni az adatbázis kiszolgálótól, semmilyen közvetlen hozzáférés nem lehetséges.

A réteges arhitektúrában minden réteg csak azokkal a más szolgáltatásokkal kommunikál, akitől adatot kér, vagy akinek adatot szolgáltat.

A rétegek közötti kommunikáció titkosított csatornákon történik.

Tesztelési metodika

Minden fejlesztés, legyen az bármilyen kicsi funkció módosítás vagy esetleges hibajavítás csak és kizárólag úgy kerülhet ki az éles környezetbe, hogy egy többszintű ellenőrzési (review) és tesztelési (testing) fázison megy keresztül.

- az elkészült funkciót, módosítást, javítást a fejlesztő saját környezetében futtatja, szükség szerint javítja a feltárt hibákat, automata teszteseteket.
- a code review-t egy másik fejlesztő vagy fejlesztői csoport hajtja végre, melynek során nem csak funkcionálisan vizsgálják, hanem atekintetben is hogy megfelel-e a forráskód a fejlesztési irányelveknek, megfelően vannak alkalmazva a programnyelv szintaktikai elemei, a kódszervezés és az átláthatóság megfelelő-e, illetve teljesíti a forráskód a funkcionális követelményeket. Elfogadott code review után kerülhet a tesztkörnyezetbe a fejlesztés, ennek hiányában a fejlesztőnek a javasolt módosításokat meg kell tennie
- a tesztkörnyezetben 4 féle tesztelés történik
    - manuális fejlesztői teszt, melynek során a programozó a saját maga által készített módosítást teszteli.
    - ezután következik a manuális funkcionális és logikai teszt, melynek során egy vagy több tesztelő tesztadatokkal tölti fel az adott modulhoz kapcsolódó adatkört, ezekre lekérdezéseket riportokat futtat. A tesztelés során a szükséges és előírt védelmi elemeket, felhasználói jogosultságogat, hozzáféréseket, a jogosultságok megadásával illetve megvonásával történő eseteket is vizsgálja.
    - automata tesztek futtatása: a tesztelő csoport minden rendszerfunkcióhoz automatikusan újrafuttatható teszt szrikpteket készít, melyeket minden publikálás előtt lefuttat a háttérrendszer. Bármilyen hiba esetén megáll a publikálási folyamat, csak akkor publikálható egy fejlesztés ha az automata tesztek minden szemaforja zöld jelzést mutat
    - manuális vagy automata terheléses tesztek, melynek során a tesztek arra vannak optimalizálva hogy nagy mennyiségű adat egyidejű lekérdezésével vizsgálja a rendszer terheltségét, performanciáját

Jogosultságkezelés

Általános felhasználói hozzáférés, jogosultságok

A rendszer kizárólag a szerződött előfizetők felhasználói számára elérhetők, mely felhasználókat a szerződésben meghatározott és aszerint korlátozott funkciójogokkal a Mobile LBS Kft support tevékenységében résztvevő ***“admin”*** felhasználói joggal rendelkező munkavállalói, illetve az előfizető úgynevezett ***“flotta admin”*** felhasználói tudják létrehozni. Önálló felhasználói regisztrációra nincs lehetőség.
A felhasználók számára a kapott / korlátozott funkciójogok mellett az úgynevezett ***“object permisson”*** jogosultsági rendszer lehetőséget ad arra hogy a rendszerben tárolt adatok bizonyos körére korlátozzuk le egyes felhasználók vagy felhasználó csoportok jogosultságait.

Erős jelszavak kikényszerítése

A rendszer biztonsága, az adatok illetéktelen felhasználásának megelőzése érdekében a HolAzAutó rendszer minden felhasználója számára kötelező az erős jelszavak használata. Ez azt jelenti hogy igyekszünk kizárni az olyan felhasználói jelszókat, melyek könnyen megfejthetők (ABC123, születési dátum, vagy gyermek neve, stb). Új felhasználók illetve jelszóváltoztatás esetén eleve olyan jelszót adhat meg a felhasználó, ami megfelel az “erős jelszó” követelményeinek. A régi, gyenge jelszóval rendelkező felhasználókat belépéskor figyelmeztetjük hogy változtassa meg a jelszavát, ha ezt nem teszi meg, egy bizonyos türelmi idő után a rendszer kikényszeríti a jelszóváltoztatást.

Funkciójogok és szerepkörök

A HolAzAutó rendszer minden felhasználója a szerződő előfizetői szerződése alapján valamilyen funkció jogosultsággal rendelkezik, aminek a maximuma az lehet amki a szerződésben le van fektetve.
Ezekből a jogosultságokból az adminisztrátorok, vagy az ügyfelek flotta adminja meg tud vonni, azaz bizonyos felhasználóknak csak bizonyos funkciókra is tud jogosultságot adni. A jogosultságok jogosultság csoportokba (szerepkörök) szervezhetők, ezzel segítve a hasonló jogosultságok kiosztását.

Object Permission

A funkció jogosultságon túl, lehetőség van arra, hogy az ügyfél felhasználói - ugyanazon funkcionális jogok birtokában - csak bizonyos objektumokhoz férjenek hozzá, csak azokkal kapcsolatos információkat tudjanak megjeleníteni, lekérdezni. Ha van például egy értékesítési csoportvezető, lehetőség van arra hogy csak a saját csoportjához tartozó járművek, munkavállalók utazásaival kapcsolatban jelenítsen meg adatokat, míg mondjuk a menedzsment, vagy a flottakezeléssel megbízott személyek a teljes flottára és az összes dolgozóra vonatkozóan meg tudják tenni ugyanezt.

Admin és fejlesztői jogosultságok

Az adatok biztonsága szempontjából kritikus munkakörökhöz (support, fejlesztő, tesztelő) tartozó felhasználói fiókokat, jogosultságokat és az azokkal kapcsolatos lehetőségeket szigorúan szabályoztuk.

- A rendszerek adminisztrációs felületeihez, szerverekhez, adatbázisokhoz tartozó felhasználónevek és azokhoz tartozó jelszavakat tilos bármilyen írott formában tárolni a felhasználók számítógépén, telefonján, vagy akár papírra vetve.
- a jelszavak kizárólag az “erős jelszó” kategóriába sorolható jelszavak lehetnek.
- a jelszavak tárolására egy kizárólag belső hálózatról elérhető, authentikációval elérhető jelszótároló rendszerben lehet tárolni.
- szükséges adatbázis műveleteknél kizárólag az adott művelet csoportra létrehozott felhasználóval szabad dolgozni.
- minden felhasználó kizárólag ahhoz az alrendszerhez és utilityhez fér hozzá, ami a munkájához szükséges.

Belső hálózat használata

Fontos és az adatok védelme szempontjából kritikus információk, adatbázisok, alkalmazások csak belső hálózatról érhetők el, illetve külső hálózaton kizárólag kettős authentikációval használható VPN-en keresztül. A kettős authentikáció lényege hogy a felhasználónév és jelszó használata mellett szükséges az adott fiókhoz beállított, a felhasználó telefonján futó authenticator alkalmazás, mely által kigenerált kóddal lehetséges a belépés.
Authenticatoron keresztül (ugrókódos) 2FA-val vagy más 2FA/MFA megoldással tudunk hozzáférni:

- redmine: project management eszköz (2FA Authenticator)
- git (self hosted): kódbázis és verziókezelés (2FA Authenticator)
- dockerhub: a git-en tárolt forráskódból és szintén itt tárolt docker konténer configurációs fájlokból hozunk létre dockeres image-t az applikációink számára. A buildelési folyamat ide tölti fel az imageket. Innentől forráskód szintű hozzáférés már nincsen. Viszont ezek az imagek bármelyik hostunkon (HYP) indítható. (2FA Authenticator)
- syspass jelszókezelő (2FA Authenticator)
- Duo Security admin felület (MFA, Cisco Duo app, sms stb)

Szerver architektúrák, konténerek

A host szerverekre, és az azokon futó konténerekre, virtuális gépekre csak a developer group fér hozzá erre dedikált hálózatból, vagy Cisco DUO-s MFA hitelesítésen keresztül VPN-ről.
A docker imagek úgy lettek felépítve hogy SSH után egy “jail” környezetbe kerül a felhasználó. Itt csak korlátozott parancsokat adhat ki.
A hostok és a konténerek közötti átjárhatóság a szükségesre van minimalizálva. Csak olyan eszköz érhető el egy adott környzetben, amire a működés biztosításához feltétlenül szükség van.

Adatmentés

A rendszer adatai egyidejűleg 2 db (master - slave kapcsolatban lévő) szervergép adatbázisában vannak tárolva, melyek folyamatos realtime adatbázis szinkronban vannak. Bármelyik szerver kiesik, ugyanazzal az adatbázis tartalommal tudjuk a másik szervert az éles kiszolgálásra átállítani. A szervertükrözés mellett napi mentések készülnek a szervergépekhez csatolt NAS-okra.

Vészhelyzeti forgatókönyv

A vállalat működésének fenntartása nagyban függ az üzleti folyamatokat támogató informatikai infrastruktúra rendelkezésre állásától. Ennek biztosítása mellett fel kell készülni azon esetekre is ha ez belső vagy külső körülmény hatására mégsem tartható fenn a normál munkamenet szerint.

Az ilyen jellegű események két folyamatot kell, hogy elindítsanak. Egyrészről a kiesett erőforrások visszaállítását (DRP), másrészről a kiesett erőforrások nélküli minimális funkcionalitást biztosító üzleti működést.
A DRP minden esetben elindul ha valamely, üzleti folyamatot támogató erőforrás kiesik, végrehajtása a ***"HolA - Vészhelyzeti forgatókönyv"*** szerint történik.

Adatvédelem (szabályzat, nyilatkozat)

A 2018. május 25-től alkalmazandó 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 (a továbbiakban: **GDPR**). A hazai szabályozást biztosító, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Adatvédelmi törvény) rendelkezéseivel együtt, így a szabályozás a korábbiaknál sokkal szigorúbban határozza meg a természetes személyek adatainak felhasználásával és azok védelmével kapcsolatos tevékenységeket.
A GDPR 35. cikke szerint, *„(1) Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik."*
A GDPR meghatározott esetekre kiemelt vizsgálatok lefolytatását is előírja, így többek között adatvédelmi hatásvizsgálatot ír elő ha *"természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek"*
Fentiek alapján a vállalat a természetes személyek adatainak védelmében

- adatvédelmi hatásvizsgálatot végzett mely alapján feltárta a személyes adatokkal kapcsolatos kockázatokat, azokat alacsony, közepes és magas kategóriákba sorolta
- a kockázatfelmérés alapján alakította ki a vállalat adatvédelmi szabályzatát, mely minden munkavállalóra és a személyes adatokkal kapcsolatba kerülő alvállalkozók, külső adatkezelőkre nézve is kötelező
- az adatvédelemmel kapcsolatos ügyféltájékoztatást a https://holazauto.hu/adatkezelesi-tajekoztato/ weboldalon tette közzé

Titoktartási megállapodás

A vállalat minden munkavállalójával, az információbiztonsági szempontból érintett alvállalkozójával, külső adatfeldolgozóival titoktartási megállapodást köt, mely része a jogviszonyt megalapozó munkaszerződésnek, illetve más együttműködési megállapodásnak.
A titoktartási kötelmek értelmében az érintett teljes felelősséggel tartozik a rábízott üzleti titkok, érzékeny és természetes személyeket érintő minden megkapott információért, adatért.

A rendelkezésre bocsátott eszközök használatának szabályai, azok ellenőrzése

A Mobile LBS Kft a munkakörhöz kapcsolódó feladatok elvégzése céljából munkahelyi számítógépet, laptopot vagy érintőképernyős hordozható számítógépet (tablet), mobiltelefont, egyéb informatikai eszközt, valamint elektronikus levelezési címet, továbbá hozzáférést biztosít a munkavállalók részére a vállalati hálózathoz, a használt nyilvántartásokhoz és alkalmazásokhoz, a fejlesztett teszt és éles rendszerekhez, illetve a vállalati internethez.
A vállalat alapvető gazdasági érdeke, hogy a munkavállalók a működésével kapcsolatos információkat bizalmasan kezeljék és munkaidejüket hatékony munkával töltsék, így szükségesnek tartja a munkavállalók ellenőrzését atekintetben, hogy a rendelkezésére bocsátott erőforrásokat, technikai eszközöket és fizetett munkaidőt megfelelően, a munkáltató érdekében használják fel.
Ezen gazdasági érdek alapján indokoltnak tartjuk a fentiek technikai eszközökkel és személyes betekintéssel megvalósított ellenőrzését. A munkavállalók tájékoztatva vannak ezzel kapcsolatban és tudomásul vették a vállalat a céges tulajdonú eszközöket és az azokon tárolt adatokat rendszeresen - a magánélethez való jog tiszteletben tartása mellett - ellenőrizheti.

Biztonsági kamerás megfigyelés

A Mobile LBS Kft székhelye Pécsett az István utca 7. szám alatt került kialakításra. Az egyes szervezeti egységek dolgozóinak, az ügyfelek, beszállítók és egyéb üzleti partnerek szabad mozgásának biztosítására, illetve a munka- és tűzvédelmi szabályok megfelelő alkalmazása miatt az ingatlan nyílászáróit munkaidőben csak csukott, de nem bezárt állapotban kell tartani, emiatt szükségesnek láttuk egy magasabb szintű, kamerás védelmi rendszer kiépítését.
Az elektronikus megfigyelőrendszer az emberi élet, testi épség, illetve személyiségi jogok védelme, valamint vagyonvédelem – így különösen a Mobile LBS Kft területén tárolt, jelentős értéket képviselő informatikai és egyéb technikai eszközök, illetve adatok, a raktárkészlet védelme, a dolgozók és látogatók értékeinek védelme - céljából kerül alkalmazásra.
A kamerarendszer használatát **Kamerarendszer működtetési szabályzatban** rögzítettük.

1. számú melléklet - Jogszabályi megfelelőségi nyilatkozat

A HolAzAutó rendszer Menetlevél és Útnyilvántartás moduljára.

A Mobile LBS Korlátolt Felelősségű Társaság (7625 Pécs, István utca 7. 1. em. 6. ajtó; Cégjegyzékszám: 02-09-078039; Adószám: 23560897-2-02), a továbbiakban Mobile LBS Kft., jelen nyilatkozattal igazolja, hogy a https://portal.holazauto.hu/fleet/ domain néven elérhető HolAzAutó rendszer Menetlevél és Útnyilvántartás modulja minden tekintetben megfelel a nyilatkozat készítésének napján hatályos jogszabályoknak.

Az alábbiak a rendszer felhasználó általi, a hatályos jogszabályoknak megfelelő egyedi beállításai, illetve a rendszer üzemszerű, az elektronikus módon itt elérhető felhasználói kézikönyvben leírt használata mellett előállított Tehergépjármű menetlevél és Útnyilvántartás bizonylatok esetében igazak.

A HolAzAutó rendszerrel előállított Útnyilvántartás:

- megfelel a 1995. évi CXVII. törvény a személyi jövedelemadóról
    - 5. számú melléklet, 7. Gépjármű-használati nyilvántartás (útnyilvántartás) fejezetben meghatározott, valamint
    - a 3. számú melléklet, II. Igazolás nélkül, költségként elszámolható tételek fejezetben meghatározott követelményeknek.
- alkalmas a 2007. évi CXXVII. törvény az általános forgalmi adóról jogszabály Adólevonási jog korlátozása alóli kivételek fejezet 125. §-ában foglaltak igazolására.
- megfelel a 60/1992. (IV. 1.) Korm. rendelet a közúti gépjárművek, az egyes mezőgazdasági, erdészeti és halászati erőgépek üzemanyag- és kenőanyag-fogyasztásának igazolás nélkül elszámolható mértékéről rendelet előírásainak
- megfelel a 2000. évi C. törvény a számvitelről
    - 167. §-ában előírt, a könyvviteli elszámolást alátámasztó bizonylat alaki és tartalmi feltételeinek, valamint
    - a 169. §-ában, a bizonylatok megőrzésével kapcsolatos követelményeknek

A HolAzAutó rendszerrel előállított Tehergépjármű menetlevél:

- megfelel a 1995. évi CXVII. törvény a személyi jövedelemadóról
    - 5. számú melléklet, 7. Gépjármű-használati nyilvántartás (útnyilvántartás) fejezetben meghatározott, valamint
    - a 3. számú melléklet, II. Igazolás nélkül, költségként elszámolható tételek fejezetben meghatározott követelményeknek.
- megfelel a 261/2011. (XII. 7.) Korm. rendelet a díj ellenében végzett közúti árutovábbítási, a saját számlás áruszállítási, valamint az autóbusszal díj ellenében végzett személyszállítási és a saját számlás személyszállítási tevékenységről, továbbá az ezekkel összefüggő jogszabályok módosításáról szóló kormányrendelet előírásainak
- megfelel a 60/1992. (IV. 1.) Korm. rendelet a közúti gépjárművek, az egyes mezőgazdasági, erdészeti és halászati erőgépek üzemanyag- és

kenőanyag-fogyasztásának igazolás nélkül elszámolható mértékéről rendelet előírásainak

- megfelel a 2000. évi C. törvény a számvitelről
    - 167. §-ában előírt, a könyvviteli elszámolást alátámasztó bizonylat alaki és tartalmi feltételeinek,
    - a 168. §-ában, a szigorú számadási kötelezettséggel kapcsolatos, valamint a
    - a 169. §-ában, a bizonylatok megőrzésével kapcsolatos követelményeknek
- megfelel a 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól szóló rendelet 3. § és 6. §-ában a dokumentumok megőrzésére és arhiválására vonatkozó előírásoknak.

A rendszerben tárolt, lezárt úti okmányok a lezárást követően nem módosíthatók.
Hibás bizonylatok kizárólag érvénytelenítéssel és újragenerálással javíthatók, melynek során mind az eredeti (érvénytelenített), mind pedig a megfelelően előállított példány megőrzésre kerül a szigorú számadású bizonylatokra vonatkozó előírások szerint.
A bizonylatok nyomtatási képe PDF fájlként is eltárolásra kerül, így a tárolás ideje alatt bármikor eredeti példányban, egyértelmű azonosításra alkalmas módon reprodukálható.

A hibás adatbevitelből eredő károkkal kapcsolatos felelősséget a Mobile LBS Kft. a felhasználóra hárítja át. A rendszerbe a felhasználók által bevitt adatok tartalmáért a Mobile LBS Kft. felelősséget nem vállal.

Pécs, 2023. augusztus 1.

Tóth Attila

ügyvezető

Mobile LBS Kft.