Elektronikusan aláírta:
Hradszki László
Szignó

**Hiventures Kockázati Tőkealap-kezelő Zártkörűen Működő Részvénytársaság**

# Adatvédelmi és Adatbiztonsági Szabályzat

**2025.**

# I. Általános rendelkezések

## *1. A szabályozás célja*

Jelen szabályzat (a továbbiakban: Szabályzat) célja, hogy

- a Hiventures Kockázati Tőkealap-kezelő Zártkörűen Működő Részvénytársaság (a továbbiakban: Hiventures vagy Társaság) – mint adatkezelő – tevékenységével összefüggésben biztosítsa – 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 szóló Európai Parlament és a Tanács (EU) 2016/679 rendeletében, továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011.évi CXII. törvényben meghatározottak szerint – a Társaság tevékenysége során a személyes adatok védelméhez fűződő információs önrendelkezési jog érvényesülését,
- biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság fokozott követelményeinek érvényesülését,
- orientálja és mindezek alapján szabályozza a Hiventures szervezeti egységeinél történő – személyes adatok kezelésére vonatkozó – adatkezelés rendjét.

## *2. A Szabályzat személyi és tárgyi hatálya*

A Szabályzat személyi hatálya kiterjed a Hiventures szervezeti egységeire, munkavállalóira, valamint a Hiventures-el szerződéses jogviszonyban álló természetes és jogi személyre, jogi személyiséggel nem rendelkező szervezetre, a velük kötött szerződésben, illetve titoktartási nyilatkozatokban rögzített mértékben.

Tárgyi hatálya kiterjed a Hiventures szervezeti egységeinél folytatott minden olyan adatkezelési és adatfeldolgozási tevékenységre, amely személyes adatra vonatkozik, függetlenül attól, hogy az adatkezelés, illetve adatfeldolgozás teljesen, vagy részben automatizált eszközzel, vagy manuális módon történik.

*A Szabályzat módosítása*

A Szabályzat elfogadásra, és szükség szerinti módosításra történő előkészítése a Hiventures adatvédelmi tisztviselőjének (a továbbiakban: Adatvédelmi Tisztviselő) a feladata.

## *3. Kapcsolódó jogszabályok és belső szabályozási dokumentumok*

Kapcsolódó jogszabályok:

- 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: általános adatvédelmi rendelet vagy GDPR);
- Magyarország Alaptörvényének VI. cikke;
- 2013. évi V. törvény a Polgári Törvényről (a továbbiakban: Ptk.);
- 2012. évi I. törvény a Munka törvénykönyvéről (a továbbiakban: Mt.);
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.);
- 2009. évi CLV. törvény a minősített adat védelméről;

- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (a továbbiakban: Szvtv.)
- 272/2014. (XI. 5.) Korm. rendelet a 2014-2020 programozási időszakban az egyes európai uniós alapokból származó támogatások felhasználásának rendjéről

Kapcsolódó belső szabályozási dokumentumok:

- a Társaság Működési Szabályzata
- a Társaság Informatikai Biztonsági Szabályzata
- a Társaság Befektetéskezelési szabályzatai
- a Társaság Érdekeltségi Rendszeréről, Jóléti és Szociális Juttatásairól szóló Szabályzata
- a Társaság Vagyonnyilatkozat-tételi és -kezelési szabályzata
- a Társaság Pénzmosás és Terrorizmus Finanszírozása Megelőzéséről és Megakadályozásáról szóló szabályzata
- a Társaság Hivatalos Külföldi Kiküldetésekről szóló szabályzata
- a Társaság Gépjárműhasználati Szabályzata
- a Társaság Iratkezelési Szabályzata
- a Társaság Pénz-és Likviditáskezelési Szabályzata
- a Társaság Kockázati Kontroll Szabályzata
- Nem vezető állású munkavállalók javadalmazásának módjáról és mértékéről szóló szabályzat hatályba léptetéséről szóló vezérigazgatói utasítás
- A bennfentes információ kezeléséről, valamint a bennfentes kereskedelem, a bennfentes információk jogosulatlan közzététele és a piaci manipuláció tilalmáról szóló vezérigazgatói utasítás
- 5/2022. (10.27.) számú vezérigazgatói utasítás A céges mobiltelefonok használatáról
- Az 5/2024. számú Csoportszintű Irányelv A kapcsolt személyekkel szembeni kockázatvállalásról szóló vezérigazgatói utasítás

## *4. Értelmező rendelkezések*

A Szabályzat alkalmazása során – összhangban a vonatkozó jogszabályok előírásaival – a következőkben meghatározott fogalmak irányadók:

**Adatkezelő:**
Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

**Adatkezelés:**
A személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

**Adattovábbítás:**
Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

**Személyes adatok határokon átnyúló adatkezelése:**

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy

b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket.

**Adattörlés:**
Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

**Adatmegjelölés:**
Az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

**Adatkezelés korlátozása:**
A tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

**Adatmegsemmisítés:**
Az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

**Adatfeldolgozás:**
Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.

**Adatfeldolgozó:**
Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

**Adatvédelmi incidens:**
A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

**Álnevesítés:**
A személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

**Anonimizálás*:***
Olyan technikai eljárás, amely biztosítja az érintett és az adat közötti kapcsolat helyreállítási lehetőségének végleges kizárását.

**Biometrikus adat:**
Egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.

**Cookie (sütik):**
A felhasználó böngészőjén keresztül annak winchesterére kerülő információs (általában egyszerű szöveg) file, ami egyértelműen azonosítja a felhasználót a következő látogatás alkalmával.

**Címzett:**
Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.

**Direkt marketing (közvetlen üzletszerzési) tevékenység*:***
Azoknak a közvetlen megkeresés módszerével végzett tájékoztató tevékenységeknek és kiegészítő szolgáltatásoknak az összessége, amelyeknek célja az érintett részére termékek vagy szolgáltatások ajánlása, hirdetések továbbítása, a fogyasztók vagy kereskedelmi partnerek tájékoztatása, üzletkötés (vásárlás) előmozdítása érdekében.

**Egészségügyi adat:**
Egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

**Érintett/ügyfél**
Bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül, vagy közvetve – azonosítható természetes személy.

**Genetikai adat:**
Egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

**Harmadik fél:**
Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

**Harmadik ország:**
Minden olyan állam, amely nem EGT-állam.

**Az érintett hozzájárulása:**
Az érintett akaratának önkéntes, konkrét, megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

**Nyilvánosságra hozatal:**
Az adatot bárki számára történő hozzáférhetővé tétele.

**IP cím:**
Valamennyi hálózatban, amelyben a kommunikáció a TCP/IP-protokoll szerint folyik, a szervergépek IP-címmel, azaz azonosítószámmal rendelkeznek, amelyek az adott gépek hálózaton keresztüli azonosítását teszik lehetővé. Tudvalévő, hogy minden hálózatra kapcsolt számítógép rendelkezik IP címmel, amelyen keresztül beazonosítható.

**Különleges adat:**
A személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

**Kötelező adatkezelés:**
A kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg.

**Megfelelő tájékoztatás:**
Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

**Nemzeti Adatvédelmi és Információszabadság Hatóság:**
Rövidítve: NAIH, akinek a jogállását és feladatait az Info tv. 38.§-a határozza meg (a továbbiakban: Hatóság).

**Nyilvántartási rendszer:**
A személyes adatok bármely módon – centralizált, decentralizált, funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

**Nyilvános adat:**
Minden olyan tény, adat, információ, amelyek bárki számára hozzáférhetők. Személyes adat nyilvánosságáról kizárólag törvény rendelkezhet.

**Nyilvánosságra hozatal:**
Az adat bárki számára hozzáférhetővé tétele.

**Profilalkotás:**
Személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul.

**Személyes adat:**
Azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

**Személyes adat-gazda:**
Egy adott szervezeti egységnél kezelt személyes adatok tekintetében a szervezeti egységet irányító vezető, aki felelős a szervezeti egysége által kezelt valamennyi személyes adat jelen szabályzatnak megfelelő kezelésért (továbbiakban: adatgazda). Amennyiben IT rendszerben kezelt személyes adattal kapcsolatos döntés meghozatala szükséges, és az érinti az adatgazda felelősségét, akkor az adatgazda hozza meg döntését.

**Természetes személyazonosító adatok:**
Az érintett családi- és utóneve, születéskori neve, anyja neve, születési helye és ideje.

**Tiltakozás:**
Az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

**Tilalmi lista*:***
Azon érintettek név- és lakcímadatainak a nyilvántartása, akik megtiltották, illetve – a közvetlen üzletszerző szerv erre irányuló előzetes megkeresése ellenére – nem járultak hozzá, hogy személyes adataikat kapcsolatfelvétel vagy üzletszerzési lista céljából felhasználják, vagy megtiltották azok e célból történő további kezelését.

**Üzletszerzési lista:**
A reklámok közlése céljából a kapcsolatfelvételt és kapcsolattartást szolgáló, kizárólag az ügyfél nevét, nemét, születési helyét és idejét, az ügyfél érdeklődési körére vonatkozó információt tartalmazó lista.

**Üzleti titok:**
A Hiventures gazdasági tevékenységéhez kapcsolódó, titkos - egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja

**Vállalkozás:**
Gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő Társaságokat és egyesületeket is.

**VPN (Virtual Private Network – virtuális magánhálózat):**
Olyan informatikai hálózat, amely nyilvános kommunikációs csatornák és eszközök segítségével valósul meg, de az azokon zajló egyéb forgalomtól logikailag elkülönülő, mások számára nem hozzáférhető egységet képez. A VPN az adatok védelmére, a hitelesítés mellett, titkosítást is alkalmaz, miáltal lehetőséget biztosít a Hiventures számára, hogy a belső hálózat meghatározott elemeit kívülről elérhetővé tegye az erre feljogosított (pl. zárt felhasználói csoport, illetve távmunkát végző) felhasználók számára.

**Védendő információ:**
A minősített adat, az üzleti titok, a know-how (védett ismeret), a személyes adat (zártan kezelendő), a nem nyilvánossá, vagy belső használatúvá nyilvánított adat, a döntés-előkészítő dokumentum, továbbá a munkakör betöltésével összefüggésben a munkavállaló tudomására jutott egyéb olyan információ, amelynek illetéktelen személy számára történő hozzáférhetővé tétele törvényi előírást sért, a munkáltató, vagy más személy számára hátrányos következményeket hordozhat, továbbá a Hiventures által kezelt azon adatok, amelyek bizalmasságához, sértetlenségéhez, rendelkezésre állásához a Hiventures-nek érdeke fűződik, kivéve, ha a nyilvánosságra hozatalt jogszabály, illetve belső utasítás írja elő, továbbá azt az arra jogosult korábban már nyilvánosságra hozta.

**Zártan kezelendő:**
A személyes adatot tartalmazó dokumentumok általános védelmi előírása. Amennyiben az adathordozóról nem állapítható meg egyértelműen adattartalmának védendő jellege, vagy a Hiventures külön ki kívánja emelni a kezelés zártságának követelményét, abban az esetben ezt kezelési utasításként kell a dokumentumon feltüntetni.

## *5. A személyes adatok kezelése és védelme*

### *Alapelvek és alapvető rendelkezések*

A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha a Társaság rendelkezik azokkal a technikai feltételekkel, amelyek a kapcsolat helyreállításához szükségesek.

A Társaság kizárólag az Európai Unió, illetve Magyarország jogszabályai által meghatározott előírások betartásával kezel személyes adatot („*jogszerűség elve*”). Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.

A Társaság által folytatott adatkezelések mind az érintettek, mind pedig a Társaság számára érthetőek, átláthatóak („*átláthatóság elve*”) és tisztességesek (nem megtévesztőek). A Társaság az érintettek irányába a munkaviszony alatt a Társaság belső hálózatán folyamatosan elérhető tájékoztató, egyéb érintettek esetében a tájékoztatás és a hozzáférés iránti kérelmek haladéktalan kivizsgálásával, míg a szervezeten belül az adatkezelésekről vezetett naprakész nyilvántartás útján gondoskodik az átláthatóság követelményének megvalósulásáról.

Személyes adat kizárólag meghatározott célból, jog gyakorlása vagy kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának („*célhoz kötöttség elve*”).
Amennyiben a korábbi hozzájárulástól eltérő célra kívánják az adatokat felhasználni, ugyanazon adatok ismételt felhasználása új adatkezelési célnak minősül, melyre az új adatkezelések meghatározására vonatkozó szabályok alkalmazandók.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas („*adattakarékosság elve*"). Személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető („*korlátozott tárolhatóság elve*").

Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani („*pontosság elve*").

A Társaság már az adatkezelés tényleges megkezdése előtt – például a projekt-előkészítés időszakában – is figyelmet fordít az adatvédelmi előírások betartására („*beépített adatvédelem [privacy by design] elve*"). Az adatkezelés feltételeinek való megfelelés, valamint az érintettek jogai gyakorlásának elősegítése és támogatása a személyes adatok kezelésének teljes életciklusát felöleli.

A Társaság a technológia mindenkori állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembevételével mind az adatkezelés módjának meghatározásakor (például a személyes adatok kezelését végző rendszerek üzleti specifikációjában, rendszertervében), mind pedig az adatkezelés során megfelelő technikai és szervezési intézkedésekkel biztosítja

- a személyes adatok titkosítását (hozzáférési jogosultság kontrollal);
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegét, integritását, rendelkezésre állását és illetéktelen hozzáférésekkel szembeni ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását megfelelő időben vissza lehessen állítani;
- a kezelt adatok kategorizálását (személyes adat, különleges adat stb.), megőrzési idejük, kezelésük, céljuk rögzítését;
- a kezelt személyes adatok módosításának módjának és idejének rekonstruálhatóságát;
- a tárolt személyes adatoknak az őrzési idő elteltével, illetve jogos törlési igény, törlésre kötelező határozat esetén az éles rendszerben történő végleges hozzáférhetetlenné tételét.

A Társaság és az általa megbízott adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy a Társaság vagy az adatfeldolgozó irányítása mellett eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag a Társaság utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

Az informatikai fejlesztési folyamat során a személyes adatok kezelését érintő rendszerek üzleti specifikációinak, illetve rendszertervének elkészítésébe, véglegesítési folyamatába az Adatvédelmi Tisztviselőt be kell vonni.

A tervezett, személyes adatok kezelését is érintő folyamatot, a tervezett adatkezelést előzetesen véleményeztetni kell

- az Adatvédelmi Tisztviselővel az adatvédelmi előírásoknak való megfelelés tekintetében;
- a jogi szakterülettel az egyéb kapcsolódó jogszabályoknak (polgári jog, EU támogatások normái stb.) való megfelelés céljából;
- a compliance szakterülettel a megfelelőségi kockázatok elemzése, kezelése céljából;

- az informatikai szakterülettel a határműveletek megfelelőségének szempontjainak érvényesülésének érdekében, valamint
- az Informatikai Biztonsági Felelőssel a szakterületi szempontjai érvényesülése céljából.

A Társaságnak képesnek kell lenni annak igazolására, hogy a személyes adatkezeléssel járó műveletek megtervezése és végrehajtása során mindent megtett az adatkezelés jogszerűsége érdekében („*elszámoltathatóság elve*”).

A Társaság

- az általa folytatott adatkezelésekről naprakész nyilvántartás vezetésével,
- az érintettek átlátható, teljes körű tájékoztatásával,
- az Adatvédelmi Tisztviselői pozíció megfelelő szakértelemmel rendelkező személy általi betöltésével,
- a szerződéses partnereinek (adatfeldolgozóinak) adatvédelmi szempontú kiválasztásával és ellenőrzésével, megfelelően implementált adatbiztonsági kontrollmechanizmusok alkalmazásával,
- naprakész adatkezelési és adatbiztonsági szabályzat megalkotásával és hatályban tartásával,
- az adatkezelésben érintett alkalmazottai tudatosságát fokozó képzések rendszeres tartásával,
- az adatvédelmi hatásvizsgálat elvégzésével, valamint
- a beépített adatvédelem elvének üzleti és operatív folyamataiba implementálásával

válik adatvédelmi szempontból elszámoltathatóvá.

### *6. Az adatkezelés jogalapjai*

Személyes adatot a Hiventures akkor kezelhet, ha:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, melyben az érintett az egyik fél, vagy a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés az adatkezelő vagy egyéb harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

Különleges adatot a Hiventures kizárólag meghatározott esetekben kezelhet, ha:

- az érintett *kifejezett* hozzájárulását adta;
- az adatkezelőre vagy az érintettre vonatkozó foglalkoztatási, szociális biztonsági és védelmi kérdéseket szabályozó jogszabályok rendelkezései alapján kötelező;

- az érintett vagy más természetes személy létfontosságú érdekei miatt szükséges, ha az érintett cselekvőképtelensége miatt képtelen ehhez a hozzájárulását adni;
- az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- az adatkezelés valamilyen jogi igény érvényesítéséhez elengedhetetlen;
- az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján;
- erre megelőző munkahelyi egészségügyi célokból van szükség (képesség meghatározás, diagnózis felállítás, kezelés nyújtása), és megfelelő egészségügyi szakértelemmel kijelölt szerv vagy személy felelőssége és titoktartása mellett történik az adatkezelés;
- az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem;
- az adatkezelés közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges.

Amennyiben az érintett a Hiventures-szel írásban kötött szerződés teljesítése érdekében adja meg személyes adatait, akkor a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét és címzettjeit. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul az adatai szerződésben meghatározottak szerinti kezeléséhez.

### *7. Az adatbiztonság követelménye*

A Hiventures az adatkezelés során mindvégig köteles gondoskodni a kezelt személyes adatok észszerűen elvárható legmagasabb szintű biztonságáról (adatbiztonság elve). Az informatikai rendszerekben megvalósuló adatkezelések során a Hiventures mindenkor a kezelt személyes adatok mennyiségéhez és minőségéhez alkalmazkodó kockázatokkal arányos adatbiztonsági intézkedések megvalósítására törekszik.
A Hiventures köteles az adatkezelési műveleteket a kezdetektől úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek magánszférájának védelmét.
A Hiventures illetőleg tevékenységi körében a vele kapcsolatban álló adatfeldolgozó köteles gondoskodni az adatok megfelelő szintű biztonságáról, továbbá köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatbiztonsági előírásokra vonatkozó jogszabályok és a belső informatikai biztonsági szabályzatban megfogalmazottak érvényre juttatásához szükségesek.
Ennek keretében az adatgazdák az adott szervezeti egység által kezelt személyes adatok tekintetében kötelesek:

- az adatkezelés időtartama alatt az adatok biztonságos felvételére és tárolására, az őrzési időtartam lejártával az adatállomány törlése, fizikai megsemmisítése vagy anonimizálása érdekében a szükséges intézkedéseket megtenni;
- az adatokat megfelelő belső intézkedésekkel védeni kell a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint

a véletlen megsemmisítés és sérülés, továbbá a Hiventures által alkalmazott technika megváltoztatásából fakadó hozzáférhetetlenné válás ellen;
- gondoskodni arról, illetve azt folyamatosan ellenőrizni, hogy a jelen Szabályzatot, valamint a feladatkörükben kiadott külön, a személyes adatok kezeléséről szóló rendelkezéseket az irányításuk alatt dolgozók megismerjék és betartsák;
- ellenőrizni, hogy a szervezeti egységében kezelt adatok továbbításukat követően is olyan adatkezelőhöz, adatfeldolgozóhoz kerülnek, aki vagy amely az adatok biztonságos kezeléséről megfelelően gondoskodni tud, ezzel összefüggő kérdésekben jogosult kérni az Adatvédelmi Tisztviselő állásfoglalását.

A Hiventures valamennyi munkavállalója köteles a személyes adatokat tartalmazó iratokat és a munkavégzéshez szükséges segédleteket a munkavégzés befejezését követően – ahol biztosított – zárható lemez- vagy páncélszekrényben, biztonsági zárral ellátott fiókban, szekrényben tárolni. Ahol ezek a feltételek nem biztosítottak ott is törekedni kell az adatok legalább zárral ellátott fiókban, szekrényben történő biztonságos tárolására. Az íróasztalokon a munkavégzés befejezését követően személyes adatokat tartalmazó iratok tárolása tilos.
Az adatokat a Társaságnak védenie kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá a Hiventures által alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.
A személyes adatok automatizált feldolgozása során biztosítania kell a jogosulatlan adatbevitel megakadályozását, annak ellenőrizhetőségét, hogy a személyes adatokat mely szerveknek továbbították, a személyes adatokat mikor és ki vitte be az adatfeldolgozó rendszerbe, a telepített rendszerek üzemzavara esetén az adatok helyreállíthatóságát, valamint azt, hogy a fellépő hibákról jelentés készüljön.
Az elektronikusan kezelt adatállományok védelme érdekében a Hiventures megfelelő technikai megoldással köteles biztosítani, hogy a különböző nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.
A Hiventures munkavállalóinak adatai, függetlenül attól, hogy egy közös, vagy osztott adatbázisban szerepelnek, a munkavállaló szempontjából egy nyilvántartásnak tekintendők.
A Hiventuresnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene a Hiventuresnek.

## *8. Adatfeldolgozás*

A Hiventures az NTH Nemzeti Tőkeholding Zrt.-vel (a továbbiakban: NTH Zrt.) fennálló szolgáltatási szerződés alapján az alábbi szolgáltatásokat veszi igénybe az NTH Zrt.-től:

- Gazdasági funkció
- HR funkció
- Stratégia és digitalizáció funkció
- Jogi funkció
- Marketing és Kommunikációs funkció
- Titkárság funkció

Ezen tevékenységek ellátása során az NTH Zrt. adatfeldolgozónak minősül.
A Hiventures a munkaviszonyból, illetve gazdasági tevékenységének ellátásából származó kötelezettségek teljesítése céljából (irattárazás, küldemények kezelése, szükséges szoftverek, stb.)

az adatszolgáltatás céljának megjelölésével, a munkavállalók, illetve ügyfelek személyes adatait adatfeldolgozó számára átadhatja, amelyről az érintetteket előzetesen tájékoztatni kell.
A Hiventures határozza meg az általa megbízott adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatkezelésre vonatkozó jogszabályi előírások keretei között.
Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Hiventures rendelkezései szerint dolgozhatja fel, és ezek felhasználásával saját céljára adatfeldolgozást nem végezhet, továbbá köteles a személyes adatokat a Hiventures rendelkezései szerint tárolni és megőrizni.
A Hiventuresnek az adatfeldolgozásra vonatkozó szerződéseit írásba kell foglalnia. A szerződésnek tartalmaznia kell minden olyan információt, amely a személyes adatok kezelése szempontjából releváns, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, az adatfeldolgozás célját, a kezelendő adatok biztonságával kapcsolatos elvárásokat, az adatok kezelésének ellenőrzési lehetőségét. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben akár közvetett, akár közvetlen módon érdekelt. A szerződés kidolgozása során biztosítani kell az Adatvédelmi Tisztviselő véleményezési jogát.
Az adatfeldolgozó tevékenységének ellátása során további adatfeldolgozót a Hiventures rendelkezései alapján vehet igénybe. Amennyiben az adatfeldolgozó további adatfeldolgozót kíván megbízni egyes adatfeldolgozási műveletek elvégzésével, ehhez a Hiventures előzetes írásbeli hozzájárulására van szükség. Az adatkezelésben érintettek vonatkozásában olyan szerződéses kötelezettségeket kell meghatározni, amely az adatkezelés teljes folyamatában biztosítja a megfelelő védelmi szintet. A szerződés kidolgozása során biztosítani kell a Hiventures Adatvédelmi Tisztviselőjének véleményezési jogát.

## *9. Az érintettek jogai és érvényesítésük*

A Hiventures biztosítani köteles, hogy a munkavállaló, ügyfél a róla kezelt adatokat megismerhesse, a kezelt adatokat tartalmazó iratokról másolatot vagy kivonatot kaphasson.
Az érintett az adatkezelést végző szervezeti egység vezetőjénél kezdeményezheti:

- *tájékoztatását* a személyes adatainak kezeléséről;
- a személyes adatainak *helyesbítését, törlését* vagy *zárolását*;
- személyes adatainak *más adatkezelőhöz hordozását*;
- az adatkezelés *korlátozását*;

továbbá

- *tiltakozhat* az adatkezelés ellen;
- *visszavonhatja* az adatkezeléshez adott hozzájárulását.

Az érintett kérésével az Adatvédelmi Tisztviselőhöz is fordulhat.

*Az érintettek tájékoztatása*
Az érintettel (munkavállalóval, ügyféllel, szállítóval) az *adatkezelés megkezdése előtt* az adatkezelést végzőnek megfelelő tájékoztatást kell adnia az adatkezelés valamennyi körülményéről.
Kötelező (törvényi) adatkezelés esetén nem szükséges az érintett hozzájárulásának a beszerzése és nem kell az érintettel adatvédelmi nyilatkozatot aláíratni, mert az adatkezelés jogalapja a törvényi felhatalmazás és nem az érintett hozzájárulása. Ugyanakkor ebben az esetben is tájékoztatni kell az érintettet az adatkezelés alapvető lényeges körülményeiről.
Az adatkezelés megkezdése előtt az adatkezelést végzőnek az érintettet – kérés nélkül is – előzetesen egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen

- az adatkezelés milyen jogalappal történik;
- az adatkezelésre milyen cél elérése érdekében van szükség;
- az adatkezelő személyéről, adatfeldolgozás esetén az adatfeldolgozó(k) kilétéről,
- az adatkezelés időtartamáról;
- a kezelt adatok köréről;
- az adattovábbítás címzettjeiről;
- az érintett jogairól;
- a jogorvoslati lehetőségekről, így ekként az adatvédelmi hatósághoz, bírósághoz forduláshoz lehetőségről;
- azok köréről, akik megismerhetik az adatokat.

Kötelező adatkezelés esetén a tájékoztatás megtörténhet a fenti információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

Az érintett bármikor jogosult arra, hogy megfelelő tájékoztatást kapjon arról, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, akkor érintett jogosult arra, hogy hozzáférjen az Társaság által tárolt személyes adataihoz, és azokról másolatot kérhet, illetve tájékoztatást kérhet arról, hogy miként kezeli a Társaság személyes adatait.
A Társaság a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül, az érintett erre irányuló kifejezett kérelmére írásban adja meg a kért tájékoztatást

- az általa kezelt, illetőleg az általa megbízott adatfeldolgozó által feldolgozott adatairól;
- az adatkezelés adatainak forrásáról, céljáról, jogalapjáról, időtartamáról;
- az adatfeldolgozó nevéről, címéről (székhelyéről), az adatkezeléssel összefüggő tevékenységéről;
- adattovábbítás esetén annak jogalapjáról és címzettjéről;
- a jogorvoslati lehetőségről (az érintett a Hatósághoz panasszal fordulhat).

A tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet még nem nyújtott be a Társasághoz. Egyéb esetekben a Társaság a tájékoztatás-kérés megválaszolásával kapcsolatban felmerült, indokolt és igazolt költségeinek megtérítését kérheti a tájékoztatást kérőtől. Az érintett tájékoztatását a Társaság csak a GDPR-ban és a vonatkozó adatvédelmi jogszabályokban meghatározott esetekben tagadhatja meg. A tájékoztatás megtagadása esetén a Társaság írásban közli az érintettel, hogy a felvilágosítás megtagadására milyen indok alapján került sor.

*A személyes adatok helyesbítése, zárolása*
Ha a személyes adat a valóságnak nem felel meg, és a valóságnak megfelelő személyes adat a Társaság rendelkezésére áll, a személyes adatot a Társaság helyesbíti. A Társaság zárolja a személyes adatot, ha az érintett ezt kéri. A Társaság megjelöli az általa kezelt személyes adatot, ha az érintett vitatja annak helyességét vagy pontosságát, de a vitatott személyes adat helytelensége vagy pontatlansága nem állapítható meg egyértelműen.
A Társaság a helyesbítésről és zárolásról az érintettet, továbbá mindazokat értesíti, akiknek korábban az adatot adatkezelés céljára továbbította. Az értesítés mellőzhető, ha ez az adatkezelés céljára tekintettel az érintett jogos érdekét nem sérti.

*A törléshez való jog*
Az érintett kérheti, hogy a Hiventures indokolatlan késedelem nélkül törölje bizonyos általa tárolt személyes adatait, amennyiben

- az adatokra nincs többé szükség;
- az érintett visszavonta az adatok kezelésére adott hozzájárulását;
- az érintett tiltakozik az adatkezelés ellen;

- azt jogellenesen kezelték;
- jogszabály alapján kell törölni.

A Hiventures törlési kötelezettsége nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni, továbbá a személyes adatok törlésére nincs lehetőség, amennyiben a GDPR 17. cikk (3) bekezdésében meghatározott esetek valamelyike fennáll (a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából, a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából, stb.).

*Az adatkezelés korlátozásához való jog*

Az adatkezelés korlátozása a kezelt személyes adatok időbeli felhasználhatóságára vagy az adatkezelés módjára vonatkozik.

A Társaság az alábbi esetek bármelyikének bekövetkezése esetén – törlés helyett – korlátozza az érintett személyes adatainak kezelését:

- az érintett vitatja a személyes adatai pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Társaság ellenőrizze a személyes adatok pontosságát (adatkezelés időbeli korlátozása);
- az adatkezelés jogellenessége esetén az érintett adatai törlése helyett csupán azok felhasználásának korlátozását kéri a Társaságtól (adatkezelés módbeli korlátozása);
- a Társaságnak már nincs szüksége a személyes adatokra, azonban az érintett jogi igények előterjesztéséhez, érvényesítéséhez igényli azok rendelkezésre bocsátását a Társaságtól (adatkezelés módbeli korlátozása);
- az érintett tiltakozott a Társaság vagy harmadik személy jogos érdekén alapuló adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelést megalapozó jogos érdek elsőbbséget élvez-e az érintett érdekeivel, illetve jogaival és szabadságaival szemben (adatkezelés időbeli korlátozása).

Az adatkezelés korlátozása esetén a személyes adatokat a tároláson túlmenően csak az érintett hozzájárulásával vagy jogi igények előterjesztéséhez, érvényesítéséhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve Magyarország fontos közérdekéből lehet kezelni.

A Társaság a korlátozás feloldása előtt tájékoztatja a korlátozást kezdeményező érintettet.

*A személyes adatok hordozhatóságához való jog*

Az érintett ezen joga alapján jogosult arra, hogy a rá vonatkozó, és egy adatkezelő rendelkezésére bocsátott személyes adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket a személyes adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta. Ezt a jogát akkor gyakorolhatja, ha az adatkezelés hozzájáruláson vagy szerződésen alapul és az adatkezelés automatizált módon történik.

*Tiltakozás a személyes adatok kezelése ellen*

Az érintett tiltakozhat személyes adatának kezelése ellen, ha

- a személyes adatok kezelése vagy továbbítása kizárólag a Társaság vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, illetve, ha a személyes adatok kezelése jogi igények előterjesztéséhez, érvényesítéséhez szükséges;

- a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés céljából történik.

A Társaság a tiltakozást a kérelem benyújtásától számított legrövidebb időn, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.

Ha a Társaság az érintett tiltakozását megalapozottnak tartja, az adatkezelést – beleértve a további adatfelvételt és adattovábbítást is – megszünteti, és az adatokat zárolja, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik szintén kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

Ha az érintett a Társaság döntésével nem ért egyet, illetve, ha a Társaság 15 napon belül sem vizsgálja meg a kérelmet, az érintett – a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül – választása szerint – a lakóhelye vagy tartózkodási helye szerinti törvényszék előtt pert indíthat a Társasággal szemben.

*A hozzájárulás visszavonásához való jog*
Amennyiben a személyes adatok – beleértve a különleges adatokat is – kezelése az érintett hozzájárulásán alapul, az érintett a Társaságnak elektronikus levélben, illetve postai úton címzett nyilatkozat útján bármikor visszavonhatja az adatkezeléshez adott hozzájárulását, melynek következtében a Társaság nem kezeli tovább az érintett személyes adatait. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a hozzájárulás visszavonása előtt már megkezdett adatkezelés jogszerűségét.

*Az automatizált döntéshozatallal kapcsolatos érintetti jogok*
A Társaság a Szabályzat hatályba lépésének időpontjában nem alkalmaz automatizált döntéshozatali eljárást.

*Az érintetti jogok teljesítésének rendje*
Az adatok törlésről, a helyesbítésről, a korlátozásról, a megjelölésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban azt adatkezelés céljára továbbították. Az értesítés abban az esetben mellőzhető, ha az – tekintettel az adatkezelés céljára – nem sérti az érintett jogos érdekét. A kérelem elutasítása esetén az adatkezelő a kérelem kézhezvételét követő 30 (harminc) napon belül írásban közli az elutasítást alátámasztó ténybeli és jogi indokait, továbbá tájékoztatja az érintettet a bírósági jogorvoslat, valamint a Hatósághoz fordulás lehetőségéről. A kérelmezői minőségre vonatkozó megalapozott kétség esetén a Társaság jogosult a kérelmezőt személyazonosságának igazolására felhívni.

*Jogorvoslathoz való jog*
Jogsérelem esetén az érintett panaszt nyújthat be a Hatósághoz, melynek elérhetőségei:
Nemzeti Adatvédelmi és Információszabadság Hatóság
Székhely: 1055 Budapest, Falk Miksa u. 9-11.
Levelezési cím: 1363 Budapest, Pf. 9.
Telefon: +36-1-391-1400
E-mail: ugyfelszolgalat@naih.hu
Honlap: http://www.naih.hu

Az érintett élhet bírósági jogorvoslati jogával, a lakó- vagy tartózkodási helye szerint illetékes törvényszék előtt (http://birosag.hu/torvenyszekek).

*Tilalmi nyilvántartás*

A marketing adatgazda által felügyelt területnek tilalmi nyilvántartást kell vezetni

a) azoknak az érintetteknek a név- és elérhetőségi adatairól, akik a direkt marketing tevékenység tekintetében megtagadták az együttműködést, illetőleg

b) kérték adataik az adott célból történő kezelésének megszüntetését, vagy

c) ahhoz nem járultak hozzá.

A tilalmi nyilvántartás célja annak biztosítása, hogy a rajta szereplő érintettek adatai ismételten ne kerüljenek átvételre, harmadik személynek átadásra, illetőleg új listára való felvételre. A tilalmi nyilvántartásban szereplő érintettek részére direkt marketing céljából küldemény nem küldhető, kivéve, ha a tilalom más meghatározott célra vonatkozik.

Amennyiben az érintett a tilalmi nyilvántartásba kerülését megalapozó nyilatkozata nem az adatgazda által felügyelt területhez érkezik, a nyilatkozatot vagy tájékoztatást haladéktalanul meg kell küldeni az illetékes marketing adatgazda által felügyelt terület részére.

A tilalmi nyilvántartásban az érintett ismert természetes személyazonosító adatain kívül amennyiben az érintett nyilatkozata alapján ez megállapítható – szerepelnie kell azon konkrét direkt marketing tevékenységnek is, amelyre a tiltó nyilatkozat vonatkozik.

A tilalmi listán szereplő adatok nem törölhetők.

## *10. Adattovábbítás*

*Az adattovábbítás általános feltételei*

A személyes adatok akkor továbbíthatóak harmadik – az érintetten, a Társaságon és az adatfeldolgozón kívüli – személy részére, ha ahhoz az *érintett kifejezetten hozzájárult*, vagy azt a GDPR, vagy vonatkozó adatvédelmi jogszabály lehetővé teszi.

EGT tagállamba irányuló adattovábbítást a hatályos adatvédelmi jogszabályok alapján úgy kell tekinteni, mintha Magyarország területén belül történne az adattovábbítás, így az alapító MFB Invest Zrt. részére történő adattovábbításra is az általános adatvédelmi előírások irányadók. A Társaság személyes adatot nem EGT államba (harmadik országba) csak akkor továbbít, ha ehhez az érintett kifejezetten hozzájárult és a harmadik országban *biztosított a személyes adatok megfelelő szintű védelme*. A személyes adatok megfelelő szintű védelme akkor biztosított, ha az Európai Unió kötelező jogi aktusa azt megállapítja. A Társaság az Amerikai Egyesült Államokba való adattovábbításra a EU-USA adatvédelmi keret szerint jogosult.

*Hatósági megkeresésre történő adattovábbítások*

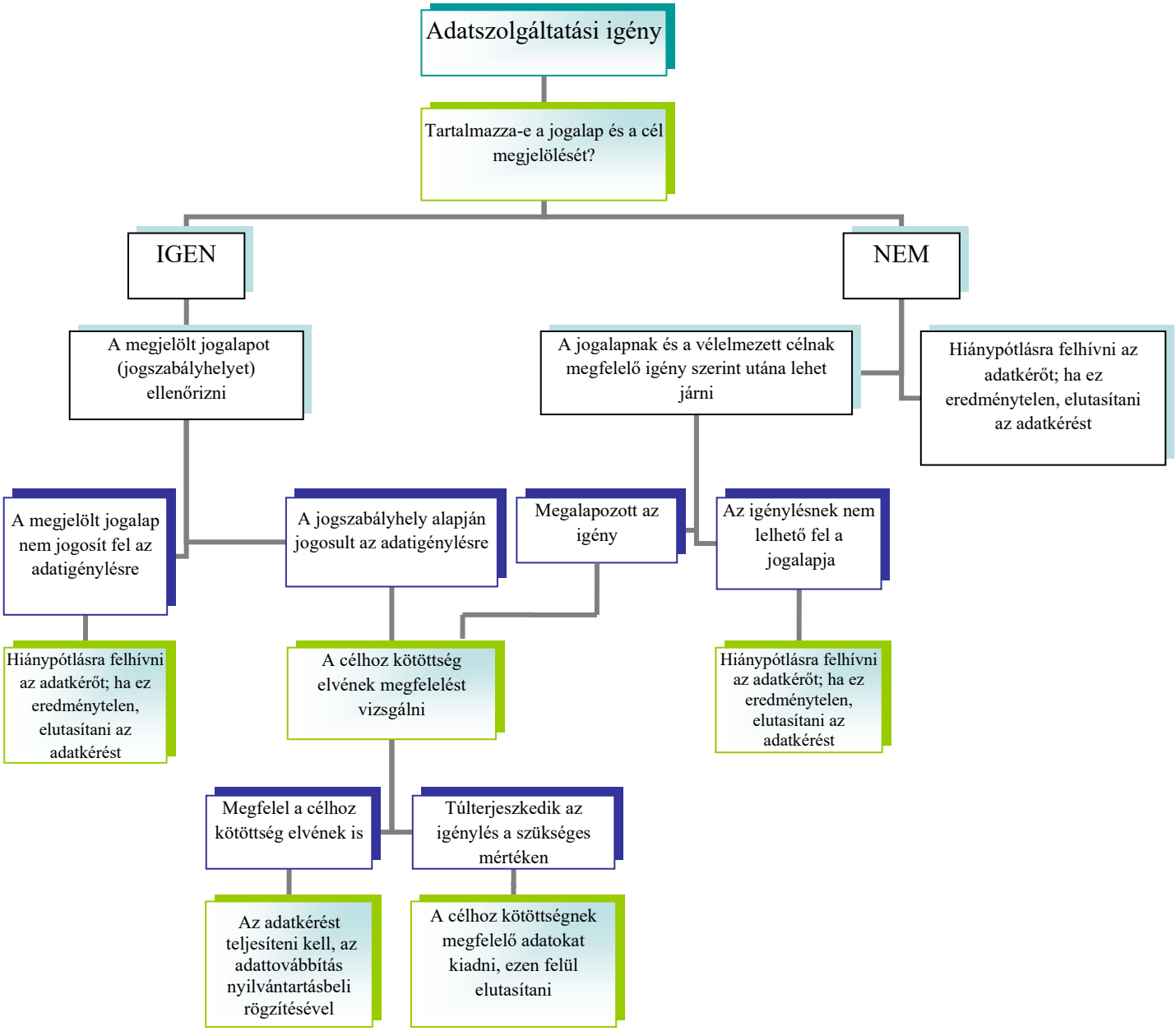
A Társaság segíti a hatóságok munkáját személyes adatok megfelelő módon és a jelen Szabályzatban leírtaknak megfelelően történő átadásával vagy hozzáférés biztosításával.

Minden hatósági adatigénylést, beleértve a nem írásbeli igényeket is, valamint az adott igények felmérésének szempontjából releváns tényeket megfelelő módon írásban rögzíteni kell. Releváns tények lehetnek többek között:

- az adatigénylés rövid leírása az igénylő hatóság nevével (ha lényeges, akkor az érintett szervezeti egység megjelölésével);
- az adatigényléssel foglalkozó személyek neve;
- az összes kapcsolódó folyamatlépés teljes naplózása;
- az adatigénylés jogalapjára vonatkozó megállapítás.

A hivatalos szervektől – bíróság, közigazgatási szerv – érkezett, személyes adatokat érintő adatszolgáltatást az illetékes szervezeti egység a megkeresésben megadott határidőig, ennek hiányában 15 (tizenöt) napon belül teljesíti.
A nyomozó hatósági adatkéréseket a hatósági adatkérésben illetékes szervezeti egység teljesíti.
Ha a megkeresés alakisága, a megkereséssel érintett adatkör kiadhatósága aggályos, az illetékes szervezeti egység az Adatvédelmi Tisztviselő soron kívüli állásfoglalását kéri. Ha a megkeresés jogszerűségét az Adatvédelmi Tisztviselő is aggályosnak tartja, köteles az ügyben a Hatóság sürgősségi eljárását kezdeményezni.
A megkeresés ez esetben a Hatóság állásfoglalásától függően teljesíthető, kivéve, ha az állásfoglalás a megkeresésben megadott határidő alatt nem érkezik meg a Hiventures részére. Ez esetben a megkeresést a megadott határidőben a Hiventures kijelölt szervezeti egysége teljesíti.

Amennyiben valamely hatóságtól személyes adat kiadására adatszolgáltatási kérelem érkezik, az adatszolgáltatás teljesítésére jogosult személy a következő eljárást köteles alkalmazni:




*Adattovábbítási nyilvántartás*

A Hiventures adattovábbítást végző adatkezelőinek nyilvántartást kell vezetnie az általuk végrehajtott adattovábbítások jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából, amelynek tartalmaznia kell a kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását.
A nyilvántartás papír alapon, és elektronikus úton is vezethető.
A felállított adattovábbítási nyilvántartásról, annak papír alapú, vagy elektronikus jellegéről az Adatvédelmi Tisztviselőt tájékoztatni kell. A tájékoztatás tartalmazza a létrehozás idejét, helyét, kezelőjét stb.
Nem szükséges külön adattovábbítási nyilvántartás készítése amennyiben az adatok a rendszerből lekérdezés útján egyértelműen kimutathatók. A nyilvántartásban az adatokat öt évig, különleges adatok esetében húsz évig meg kell őrizni.

## *11. Az adatkezelésben közreműködők és feladataik*

*A Vezérigazgató*

A Vezérigazgató irányítja és ellenőrzi az adatvédelemmel kapcsolatos feladatok végrehajtását.

*Adatvédelmi Tisztviselő*

- ellenőrzi az adatkezelésre vonatkozó jogszabályok, valamint a jelen Szabályzat rendelkezéseinek betartását; ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is. Adatvédelmi incidens esetén közreműködik a vizsgálatban, amelyben számba veszi az incidens körülményeit, hatását, javaslatot tesz az adatkezelő számára az intézkedésekre;
- ellátja a Hiventures szervezeti egységei adatvédelmi tevékenységének szakirányítását és szakfelügyeletét;
- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- kivizsgálja a személyes adatkezeléssel összefüggésben hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
- felügyeli a belső adatvédelmi nyilvántartások vezetését;
- támogatja az adatkezelőt a jogszabályi előírások teljesítésében, kapcsolatot tart a Hatósággal a Hiventurest érintő adatvédelmi ügyekben;
- koordinál az egyes szervezeti egységek között az egységes adatvédelmi szemlélet megvalósítása érdekében;
- részt vesz az adatvédelmi incidensek kivizsgálásában, segíti az incidensek vizsgálatát, koordinálja a résztvevő szervezeti egységeket;
- tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére a GDPR, valamint az egyéb uniós vagy magyar adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
- szakmai tanácsokkal segíti a hatásvizsgálat készítése közben az érintett szervezeti egységeket, valamint nyomon követi a hatásvizsgálat GDPR 35. cikk szerinti elvégzését;
- véleményezi a részére megküldött, adatvédelmi kérdéseket érintő belső szabályozási dokumentumok tervezetét;
- az adatvédelmi kérdésekkel összefüggésben az adatvedelem@hiventures.hu e-mail címen fogadja a Hiventures munkavállalóinak konzultációs kérdéseit és azzal érdemben foglakozik;
- az adatvédelmi kérdésekkel összefüggésben tájékoztatja a Hiventures vezetését;
- a tárgyévet követő év január 31-ig gondoskodik az Infotv. 71/D. § (4) bekezdésében előírt, a Hatóság irányába fennálló adatszolgáltatási kötelezettség teljesítése iránt.

*Személyes adatokat kezelő munkavállaló*

A Hiventures, illetve – szolgáltatási szerződés alapján a Hiventures-nek egyes szolgáltatásokat nyújtó – NTH Nemzeti Tőkeholding Zrt., mint közös adatkezelők azon munkavállalója, aki személyes adatok kezelésével kapcsolatos tevékenységet végez, köteles gondoskodni arról, hogy

- az adatkezelés teljes folyamatában maradéktalanul érvényesüljenek az adatvédelmi előírások;
- indokolt esetben a személyes adatot tartalmazó adathordozókon és dokumentumokon a „Zártan kezelendő” kezelési jelölés feltüntetésre kerüljön;

- az informatikai eszközök adathordozóján tárolt személyes adatok törlése esetén azok a későbbiekben ne legyenek visszaállíthatók;
- a személyes adat indokolt esetben törlésre, illetve zárolásra kerüljön.

## *12. Az adatkezelés részletes szabályai, a Hiventures által kezelt adatcsoportok*

Személyes adatok a Hiventures szervezeti keretein belül a következő csoportokban kezelhetők:

- ügyféladatok, beleértve a Hiventures szolgáltatásait igénybe vevő ügyfélkapcsolati adatokat is (ügyfél nyilvántartás);
- a Hiventures-nál egyéb szerződéses kapcsolatban álló természetes személyek adatai (partnernyilvántartás);
- a Hiventures munkavállalóinak adatai (beleértve a toborzással kapcsolatban keletkező, nem munkavállalókhoz kapcsolódó adatokat, valamint az érintett munkavállaló kérelmére indult eljárásban keletkező adatokat);
- a Hiventures direkt marketing, piackutatási tevékenységével kapcsolatos adatok, adatnyilvántartások, tilalmi nyilvántartások;
- hatósági adatszolgáltatások;
- belső adatvédelmi nyilvántartás;
- adattovábbítási nyilvántartás
- adatvédelmi incidensek kezelése, nyilvántartása.

## *13. Külső érintettek adatkezelése*

### *13.1. Ügyféladatok kezelése*

A Hiventures által nyújtott gazdasági üzleti tevékenység keretében nyújtott szolgáltatások (pl.: kollektív befektetési szolgáltatások, stb.) igénybevételére irányuló, a vonatkozó jogszabályban kötelezően meghatározott adatok, valamint az érintett természetes személyazonosító adatain kívül kizárólag olyan adatok szerepelhetnek, amelyek a szerződés teljesítése, és az ügyfél tartozásával kapcsolatos követelések érvényesítéséhez, az üzleti kockázatok felméréséhez és jogszabályban meghatározottak alapján elengedhetetlenül szükségesek.
Amennyiben az érintett ezen adatokat a szerződéskötés során szolgáltatni nem kívánja, a szerződéskötés megtagadható. Ezen adatok kezeléséhez a szerződés megkötését, a Hiventures jogszerű érdekeinek érvényesítését és kivételesen a hozzájárulást, vagy más egyéb jogszabályi jogalapot kell figyelembe venni. Kétség esetén a szerződéskötéshez kérhető adatok köréről az Adatvédelmi Tisztviselő állásfoglalását kell kérni.
Az igénylés feltételéül szabható az is, hogy az érintett közokirattal vagy teljes bizonyító erejű magánokirattal igazolja, hogy az általa szolgáltatott adatok a valóságnak megfelelnek. Az adatok valóságának igazolása érdekében bemutatott iratokról másolat csak az ügyfél azonosítása során készíthető.
Az igénylés során az érintett által szolgáltatott adatok kizárólag a szerződésből fakadó jogok gyakorlásához és kötelezettségek teljesítéséhez használhatók fel, és az adatokhoz való hozzáférés csak ilyen célra engedélyezhető. Kivételt jelentenek ez alól azok az adatok, amelyek beszerzésére a Hiventures jogos érdekének érvényesítése miatt került sor, ezek az adatok a külön adatkezelési tájékoztatókban szereplő célra és módon használhatók fel.
Ha az adatkezelés időtartama alatt az érintett adatainak változását bejelenti, vagy az adatok megváltozását a Hiventures vagy az adatfeldolgozó észleli, az adatokat a változásnak megfelelően haladéktalanul módosítani kell, illetve ki kell egészíteni. Ebben az esetben a módosításra kerülő korábbi, valamint a módosítást, kiegészítést követő új adatokat egyaránt fel kell tüntetni a

nyilvántartásban, oly módon azonban, hogy a nyilvántartásból az adatok aktív, illetve inaktív állapota egyértelműen megállapítható legyen.
Amennyiben a Hiventures vagy az érintett ügyfél az igénye érvényesítése iránt eljárást indít, az adatok az egyeztetés folyamán, valamint a bírósági, hatósági eljárás befejezéséig nyilvántarthatók.
Ha az érintett és a Hiventures közötti jogviszonyban számla kibocsátására kerül sor, a számlán szereplő adatok a számviteli- és adójogszabályokban meghatározott határidőkig tarthatók nyilván.
A törlésig a Hiventures az ügyfelek szerződésében szereplő adatait papír- és elektronikus formában is nyilvántartja.

### *13.2. A Hiventures PPC alapú online marketing, piackutatási tevékenységével kapcsolatos adatkezelés, adatnyilvántartás*

A Hiventures által végzett PPC alapú online marketing tevékenység tekintetében az adatgazda a Marketing és Kommunikációs funkció, akinek az irányítása alatt álló egységnél a fenti tevékenységekre kerül sor. E tevékenységhez a következő forrásokból gyűjthetők és használhatók fel személyes adatok:

- ügyféladatok;
- partner-nyilvántartás.

A Hiventures az általa végzendő direkt marketing tevékenység során az érintettek következő személyes adatait használhatja fel, valamint igényelheti más személyektől, illetve nyilvántartásból:

- név;
- elektronikus levélcím.

A direkt marketing tevékenység üzletszerzési lista összeállításával kezdődik. A nem kereskedelmi célú események szervezése esetén az abban részt vevő személyek által átadott adatok csak akkor használhatók fel üzletszerzési lista összeállításához, ha az érintettek figyelmét felhívták arra, hogy adataikat közvetlen üzletszerzés céljára is fel kívánják használni, és ehhez írásban hozzájárultak.
A címzett reklámküldeményben reklám természetes személy, mint a reklám címzettje részére közvetlen üzletszerzés útján a címzett előzetes és kifejezett hozzájárulásának hiányában is küldhető, a reklámozó és a reklámszolgáltató azonban köteles biztosítani, hogy a reklám címzettje a reklám küldését bármikor ingyenesen és korlátozás nélkül megtilthassa. Megtiltás esetén az érintett személy részére reklám közvetlen üzletszerzés útján a továbbiakban nem küldhető.

### *13.3. Elektronikus megfigyelőrendszer*

Elektronikus megfigyelőrendszer törvény alapján működtethető, valamint a működés jogalapját az adatkezelő jogszerű érdekének igazolása teremti meg
A Hiventures vonatkozásában a megfigyelés törvényi alapját az Szvtv. biztosítja, egyéb esetekben a munkavégzésre és a személyes adatkezelésekre vonatkozó jogszabályok előírásai irányadók.
Az elektronikus megfigyelő rendszernek felvételt is lehetővé tevő formája a következő esetekben alkalmazható:

a) az emberi élet, a testi épség, a személyi szabadság védelme;
b) a veszélyes anyagok őrzése;
c) az üzleti, bank- és értékpapírtitok védelme; valamint
d) a vagyonvédelem érdekében.

A felvételt, valamint más személyes adatot csak az arra jogosult személy jogosult megismerni, akinek ez a szerződésből fakadó kötelezettségei érvényesítéséhez szükséges, és a jogsértő cselekmény megelőzése vagy megszakítása érdekében mellőzhetetlen.
Ügyfelek számára megnyitott területeken, illetve munkaterületeken figyelemfelhívó jelzést, ismertetést kell elhelyezni a megfigyelt területen, jól látható helyen, jól olvashatóan, a területen

megjelenni kívánó harmadik személyek tájékozódását elősegítő módon. Az adatkezelés jogszerű érdek alapján történik, amelyet az érintettek megfelelő tájékoztatása alapoz meg.

### *13.4. Hiventures Hírlevele*

A Hiventures honlapján lehetőség van hírlevél szolgáltatás igénybevételére, vagy más értesítésre történő feliratkozásra. Az adatok kizárólag a szolgáltatással kapcsolatosan használhatóak fel, harmadik fél részére nem adhatók át.
A Hiventures a hírlevél szolgáltatás felmondására lehetőséget biztosít, amely során a korábban felvett adatokat törlésre kerülnek. A honlapon korábban elhelyezett nyilatkozatokat a Kommunikációs és Marketing funkciónak naprakészen kell tartania.

### *13.5. A Hiventures honlapját látogatók számítógépén cookie elhelyezéséről*

Az elektronikus hírközlésről szóló törvény szabályozza a cookie (a továbbiakban: süti) használatát, amely alapján a felhasználó elektronikus hírközlő végberendezésén csak az érintett világos és teljes körű – az adatkezelés céljára is kiterjedő – tájékoztatását követő kifejezett hozzájárulása alapján lehet adatot tárolni, vagy az ott tárolt adathoz hozzáférni.
A felhasználót az adatkezelési tájékoztató útján előzetesen teljes körűen és részletesen tájékoztatni kell a számítógépére felmásolni kívánt adatokról, majd miután ehhez megfelelően dokumentált hozzájárulását adta, tölthető fel a süti az eszközére. A süti elhelyezőjének bizonyítani kell tudnia, hogy a felhasználó a hozzájárulását megadta.
A Hiventures honlapján a sütik kezelését e szabályoknak megfelelően kell kialakítani, és azokat az adatkezelési nyilatkozat megfelelően dokumentált elfogadását követően lehet a felhasználó végberendezésén elhelyezni.

### *13.6. Fénykép-video-, illetve hangfelvétel készítés általános szabályai*

Adott személyekről készített fénykép-, video-, illetve hangfelvétel személyes adatnak minősül, amelynek elkészítéséhez és felhasználásához – törvényi felhatalmazás eseteit kivéve – az érintett személy hozzájárulása szükséges.
A hozzájárulás ráutaló magatartással is megadható, azonban célszerű ehhez írásbeli hozzájárulást kérni.
Nem szükséges a hozzájárulást beszerezni akkor, amikor a felvétel összhatásában örökít meg nyilvánosság előtt lezajlott eseményeket például tömegfelvétel, illetve nyilvános közéleti szereplés esetén, függetlenül attól, hogy a felvételen az érintett felismerhető-e.

### *13.7. Központi e-mail cím kezelése*

A Hiventures központi e-mail fiókjába (info@hiventures.hu) érkező levelek kezelése során személyes adatok is feldolgozásra kerülhetnek (a feladó által esetlegesen megadott személyes adatok, jellemzően név, e-mail cím, telefonszám). A beérkező levelekhez a szenior ügyfélszolgálati menedzser, a titkársági munkatárs, valamint a Marketing Igazgató fér hozzá. Az adatkezelés jogi kötelezettség teljesítésén (GDPR 6. cikk (1) bekezdés c) pontja) alapul, mivel a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény előírja, hogy a cégjegyzék kötelezően tartalmazza valamennyi cég elektronikus kézbesítési címét. A cégeknek a bejelentett elérhetőségen folyamatosan biztosítaniuk kell a részükre elektronikus úton küldött iratok átvételét. A Társaság működéséhez és az ügyfélkapcsolatok fenntartásához szükséges a levelek fogadása és

megválaszolása. A beérkező e-mailek kizárólag az abban foglalt ügy intézésére, megválaszolására használhatók fel.

### *13.8. Panaszok kivizsgálása*

A panaszokról, a közérdekű bejelentésekről, valamint a visszaélések bejelentésével összefüggő szabályokról szóló 2023. évi XXV. törvényben rögzített panasz elektronikus úton a panasz@hiventures.hu e-mail címre nyújtható be. Panasz benyújtására postai úton is van lehetőség a Társaság székhelyére címezve. A panaszt benyújtó természetes személy személyes adatait (neve; elektronikus levélcíme; lakcíme/székhelye; levelezési címe, amennyiben eltér) a Compliance Önálló Osztály munkatársai kezelik a panasz kivizsgálása céljából. Szóbeli panasz esetén – amennyiben a panaszos a panasz kezelésével nem ért egyet – az illetékes szakterület a panaszról jegyzőkönyvet vesz fel, és annak egy másolati példányát a panaszosnak átadja. A panaszt és az arra adott választ 5 évig kell megőrizni.

### *13.9. Cégkapura érkező dokumentumok kezelése*

A Hiventures mint elektronikus kapcsolattartásra kötelezett szervezet Cégkapun fér hozzá a hivatalos levelezéséhez. A Cégkapu kezelésére a Gazdasági és a Hr funkciót ellátó kijelölt munkavállalók, a titkársági munkatárs(ak), valamint a vezérigazgatók jogosultak.

## *14. Munkavállalói (belső) érintettek adatkezelés*

### *14.1 A munkavállalók személyes adatainak kezelése*

A munkavállalók személyes adatai kezelésének részletes szabályait jelen Szabályzat 1. számú melléklete (Adatkezelési tájékoztató munkavállalók részére) tartalmazza.
A munkavállalóktól kizárólag olyan adatok kérhetők és tarthatók nyilván, amelyek munkaviszony létesítéséhez, fenntartásához és/vagy megszüntetéséhez, illetve a Cafeteria és egyéb szociális-jóléti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik.
Amennyiben a munkába lépésre irányuló felvételi eljárást követően munkaviszony létesítésére nem kerülne sor, az érintett adatait haladéktalanul törölni kell annak a szervezeti egység vezetőjének, aki a felvételi eljárás keretében kezelte a kapcsolódó személyes adatokat (pl.: Önéletrajz), kivéve, ha az érintett írásban hozzájárul ahhoz, hogy az adatait a Hiventures továbbra is kezelje. Az így keletkezett személyes adatokat a szervezet kezeli, 1 évig tárolja adatbázisában.
A HR funkció által a személyi és munkaügyi nyilvántartásban kezelt munkavállalói adatkört jelen Szabályzat 1. számú melléklete tartalmazza.
Törvény felhatalmazása, jogi kötelezettség teljesítése alapján vagy az érintett hozzájárulására – az erre feladatkörük meghatározásával kijelölt szervezeti egységei útján – kezelheti továbbá a munkavállalók következő adatait is, így különösen:

a) munkavállalót ért balesetek jegyzőkönyveiben rögzített adatokat.

Az adott szakterületnél már rendelkezésre álló személyes adatok (többszöri, nem frissítés célú) újra kérése tilos, kivéve, ha erről jogszabály külön rendelkezik. Az adatok ismételt megadásának megtagadása miatt a munkavállalót semmiféle hátrány nem érheti. A Hiventures a munkavállaló egyéb személyes adatait kizárólag az érintett – írásbeli – hozzájárulásával, vagy a Hiventures jogszerű érdekeinek érvényesítése céljából kezelheti.
A munkaviszony létesítésére szolgáló eljárás keretében, a munkavállaló közreműködése nélkül, kizárólag a nyilvánosság számára, az érintett által korlátozás nélkül (pl.: internet, sajtó) hozzáférhetővé tett információ ismerhető meg, ideértve az érintett által kifejezetten a munkavállalásának elősegítése érdekében közzétett (pl.: Facebook.com, LinkedIn, szociális háló

útján rögzített) adatot. Harmadik személytől a Hiventures csak a munkavállaló előzetes hozzájárulásával kérheti rá vonatkozó személyes adat szolgáltatását.
Konkrét álláshelyre történő jelentkezés esetében az érintett kifejezett hozzájárulása, illetve jogszabályi előírás hiányában, a munkaviszony létesítésének meghiúsulása esetén, a felvételi eljárás során rögzített személyes adatokat haladéktalanul törölni kell a személyes adatokat kezelő szervezeti egység vezetőjének, kivéve, ha az érintett kifejezetten kéri, hogy az önéletrajzát későbbi pozíciókra való jelentkezés érdekében a Társaság megőrizze.
A munkavállaló adatait a következő személyek ismerhetik meg:

- a feladataik ellátásához elengedhetetlenül szükséges esetben, mértékben és ideig a Hiventures meghatározott szervezeti egységeinek a vezetője, illetve meghatározott – az érintett személyi anyagát kezelő – munkavállaló;
- a feladataik ellátásához elengedhetetlenül szükséges esetben, mértékben és ideig az érintett munkahelyi vezetői (a munkáltatói jogkörgyakorló vezetővel bezárólag) és az általa kijelölt munkatársai;
- konkrét ellenőrzés céljából az ahhoz elengedhetetlenül szükséges esetben, mértékben és ideig az Adatvédelmi Tisztviselő, a Vezérigazgató, valamint a vizsgálati jogkörrel felruházott szervezeti egység munkatársai;
- bíróság, ügyészség, nyomozó hatóság, illetve más eljáró hatóság hivatalos megkeresés alapján az igényelt mértékig;
- más személyek – indokolt esetben – az érintett írásos hozzájárulásával, a hozzájárulás mértékéig.

A munkaviszony megszűnését követően a jogszabályok által előírt megőrzési idők figyelembevételével a munkavállaló adatait törölni kell személyi nyilvántartásból az illetékes szervezetnek, illetve annak a szervezeti egységnek, amelynek a személyzeti nyilvántartásban a munkavállaló adata szerepel kivéve, ha a Hiventures és a munkavállaló között ettől eltérő időtartalmú írásbeli megállapodás jön létre. A törlés az írásbeli megállapodásban nem szereplő munkavállalói adatokra terjed ki.
Nem kell, illetve nem szabad törölni a munkaviszony megszűnését követően sem a munkavállaló azon adatait, amelyek törvény felhatalmazása alapján a továbbiakban is nyilvántarthatók vagy megőrzendők.

### *14.2. Humán Információs rendszer (NEXON)*

A munkavállalótól csak olyan adat közlése, vagy nyilatkozat megtétele kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.
A NEXON rendszerben, valamint a személyügyi dossziéban elhelyezett adatok nyilvántartásának vezetéséhez az érintett munkavállaló saját magára vonatkozóan köteles adatot szolgáltatni. A nyilvántartás pontossága, teljessége, naprakészsége érdekében az érintett munkavállaló az adatkörében beállt változásról köteles öt munkanapon belül, írásban bejelentést tenni.
A munkavállalók humán adataihoz történő belépési-, betekintési- és hozzáférési jogosultságokat munkakörhöz igazítottan, a munkavégzés megfelelő ellátásához szükséges legkisebb mértékű jogosultsági szinten kell meghatározni. Az adatokhoz történő hozzáférést, az azokkal végzett műveleteket – a rendszer lehetőségeihez mérten – részletesen naplózni kell.
A közvetlen munkahelyi vezetők közreműködnek abban, hogy a jogosultságok fentiek szerint meghatározott használatának biztosítása és a hatáskörtúllépés kizárása, ennek ellenőrzése, naprakészsége, a jogosultságok beállításának, módosításának, visszavonásának kezdeményezése biztosított legyen.

### *14.3. Választható béren felüli juttatások (Cafeteria)*

A Társaságnál az arra jogosult munkavállalók által évente igénybe vehető juttatások, melyekre vonatkozó részletes szabályokat a Társaság *Érdekeltségi Rendszeréről, Jóléti és Szociális Juttatásairól szóló Szabályzata* tartalmazza. A cafeteria rendszerben kezelt személyes adatok kizárólag a cafeteria juttatásokkal kapcsolatos adminisztráció és elszámolás teljesítése, valamint a jogszabályban meghatározott adatszolgáltatási kötelezettségek teljesítése érdekében kezelhetőek.

### *14.4. Egészségbiztosítás*

A Társaság munkavállalói számára egészségügyi biztosítás keretében magán orvosi ellátások, diagnosztikai vizsgálatok igénybevétele lehetőségének biztosítása a Társaság szolgáltató partnerén keresztül. Az egészségügyi és személyazonosító adatok kezelése az érintett hozzájárulásán alapul.

### *14.5. Erkölcsi bizonyítványok kezelése*

A Hiventures minden munkakörre vonatkozóan fenntartja magának a jogot, hogy csak olyan munkavállalót alkalmazzon, aki erkölcsileg megfelel az elvárásainak, ezért a Hiventures a munkaviszony létesítését tiszta erkölcsi bizonyítvány meglétéhez kötheti. A tiszta erkölcsi bizonyítvány ellenőrzését a HR munkatárs végzi, az abban szereplő adatokat ő ismerheti meg. Ő ellenőrzi az erkölcsi bizonyítvány:

- érvényességét a munkaviszony létrejöttének idején; illetve
- annak tartalmát.

Egyes méltányolható esetekben azonban a Hiventures Vezérigazgatója, egyedi elbírálás során, dönthet a munkakörre való alkalmasság megítélése mellett akkor is, ha olyan bejegyzés található az erkölcsi bizonyítványban, amely

- az elkövetett cselekmény fajtájától és súlyától függően a betöltendő munkakörben elvártakkal nem összeegyeztethetetlen;
- az érintett a bírósági mentesítési időszakában tart;
- az érintett a törvényi mentesítési idő beálltához közel van;
- egyéb méltányolható indoknál fogva nem veszélyezteti a Hiventures céljait és elveit;
- és nem ütközik a munkakör betöltésére vonatkozó egyéb jogszabályi előírásokba.

Az adatokhoz az itt megjelölteken kívül senki sem férhet hozzá, így a Hiventures más munkavállalója vagy egyéb, a Társasággal más jogviszonyban álló személy azokat semmilyen módon és formában nem ismerheti meg.
A Hiventures nem iktatja be az érintett erkölcsi bizonyítványt fizikailag, azt nem őrzi meg, kizárólag bemutatásra hívja fel az érintettet.
Amennyiben különleges méltánylást igénylő esetben a munkaviszony létesítésével kapcsolatos eljárás során az érintett nem tud erkölcsi bizonyítványt bemutatni, úgy azt 30 (harminc) napos határidőn belül megteheti.

### *14.6. Egészségügyi alkalmassággal kapcsolatos egészségügyi adatok kezelése*

Az egészségügyi alkalmassággal kapcsolatos adatokat a Hiventures nem ismeri meg, és nem kezeli egyetlen érintett adatát sem a célon túlterjeszkedő mértékben. A Hiventures az egészségügyi alkalmasság eldöntése céljából a megbízott üzemorvostól származó alkalmassági eredmény alapján dönt az adott (leendő) dolgozó egészségügyi alkalmasságáról.
A Hiventures csak az egészségügyi alkalmasság tényét bizonyító adatot kezeli.

Amennyiben a munkaszerződés megkötésének folyamata során derül ki, hogy az adott érintett alkalmatlan a munkakör betöltésére és ezért a jogviszony nem jött létre vagy ennek hatására szűnik meg, úgy az adatkezelés határideje és módja is ezzel párhuzamos.

### *14.7. Hozzátartozók adatainak kezelése munkaviszonnyal összefüggésben*

A munkaviszony kapcsán a munkavállaló hozzátartozóinak adatait is kezeli a Hiventures kedvezmények érvényesítése céljából. Az így beszerzett harmadik személy adatai a szükséges adattartamot meg nem haladóan kezelhetők. Ilyen kedvezmény lehet a pótszabadság, családi adókedvezmény igénybevétele, iskolakezdési támogatás vagy akár a baleset esetén értesítendő személy nyilvántartása a gyors kommunikáció elősegítése céljából.
Abban az esetben, ha a munkavállaló harmadik személy adatait adja meg, úgy a harmadik személytől köteles az adatkezeléshez a harmadik személy hozzájárulását megszerezni, amellyel a Hiventures igazolni tudja, hogy a harmadik személy adatainak kezelésére felhatalmazással rendelkezik.
Az adatkezelés célja: munkaviszonnyal összefüggő kedvezmények biztosítása
A kezelt adatok köre: munkavállaló közvetlen hozzátartozójának neve, születési neve, születési helye és ideje, állampolgársága, anyja születési neve, lakóhelyének címe, adóazonosító jele, TAJ száma, elérhetősége.
Az adatkezelés jogalapja: az érintett hozzájárulása és jogi kötelezettség teljesítése.
Az adattárolás határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint

- munkaviszonnyal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a munkaviszony megszűnéséig
- munkaviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig.

Az adatkezelés módja: papíralapon és elektronikusan történhet.

### *14.8. Fénykép-video-, illetve hangfelvétel készítés általános szabályai*

Adott személyekről készített fénykép- video-, illetve hangfelvétel személyes adatnak minősül, amelynek elkészítéséhez és felhasználásához – törvényi felhatalmazás eseteit kivéve – az érintett személy hozzájárulása szükséges.
A hozzájárulás ráutaló magatartással is megadható, azonban célszerű ehhez írásbeli hozzájárulást kérni.
Nem szükséges a hozzájárulást beszerezni akkor, amikor a felvétel összhatásában örökít meg nyilvánosság előtt lezajlott eseményeket például tömegfelvétel, illetve nyilvános közéleti szereplés esetén, függetlenül attól, hogy a felvételen az érintett felismerhető-e.

### *14.9. Gépjárműhasználat*

A Társaság *Gépjárműhasználati Szabályzatában* (a továbbiakban: Szabályzat) meghatározott munkaköri szintekhez tartozó munkavállalók gépjárműhasználatra (személyi használatú, kulcsos, magánhasználat), illetve üzemanyagkártya használatra jogosultak, melynek során a Társaság a Szabályzat mellékleteiként rögzített dokumentumokban meghatározott személyes adatokat kezel.

## *15. A munkavállaló ellenőrzése*

A Mt. 11/A. §-a lehetőséget biztosít arra, hogy a Hiventures a munkavállalót a munkaviszony rendeltetésével közvetlenül összefüggő, feltétlenül szükséges okból ellenőrizze. A végrehajtás

módját egyértelműen, érthetően és pontosan kell meghatározni, beleértve a megfigyelés érdekében alkalmazott eszközökkel kapcsolatos részletszabályokat, a munkavállaló személyes adatai, személyiségi jogai védelmének garanciáit is, betartva a célhoz kötöttség és a tisztességes adatkezelés elvét.
A munkavállaló kizárólag a munkaviszonnyal összefüggő magatartása tekintetében ellenőrizhető, amely nem járhat a személyes adatai, személyiségi jogai, az emberi méltósága megsértésével. A munkavállalót előzetesen tájékoztatni kell azoknak a technikai eszközöknek az alkalmazásáról, amelyek az ellenőrzésére szolgálnak.

### *15.1. Elektronikus megfigyelőrendszer*

Elektronikus megfigyelőrendszer törvény alapján működtethető, valamint a működés jogalapját az adatkezelő jogszerű érdekének igazolása teremti meg.
A Hiventures vonatkozásában a megfigyelés törvényi alapját az Szvtv. biztosítja, egyéb esetekben a munkavégzésre és a személyes adatkezelésekre vonatkozó jogszabályok előírásai irányadók.
Az elektronikus megfigyelő rendszernek felvételt is lehetővé tevő formája a következő esetekben alkalmazható:

- az emberi élet, a testi épség, a személyi szabadság védelme;
- a veszélyes anyagok őrzése;
- az üzleti, bank- és értékpapírtitok védelme; valamint
- a vagyonvédelem érdekében.

A kamera használata során fennálló körülményeknek valószínűsíteniük kell, hogy a jogsértések észlelése, az elkövető tettenérése, illetve e jogsértő cselekmények megelőzése, azok bizonyítása más csekélyebb mértékű módszerrel nem érhető el, továbbá e technikai eszközök alkalmazása elengedhetetlenül szükséges mértékű, és az információs önrendelkezési jog aránytalan korlátozásával nem jár.
Felhasználásnak az minősül, ha a felvételt, valamint más személyes adatot bírósági vagy más hatósági eljárásban bizonyítékként felhasználják.
A kamerát nem lehet kizárólag egy munkavállaló, illetve az általa végzett tevékenység megfigyelése céljából elhelyezni, tilos továbbá öltözőkben, zuhanyzókban, illemhelyiségekben használni.
Az adatkezelőnek minden egyes elektronikus megfigyelő eszköz vonatkozásában pontosan meg kell jelölnie, hogy milyen célból helyezte el az adott területen, milyen területre, berendezésre irányul. A felvételek rögzítése esetén főszabályként azokat három munkanapig lehet megőrizni.
Az elektronikus megfigyelőrendszer alkalmazásához a Hiventures jogszerű érdekeinek érvényesítése miatt kerül sor, azonban előzetesen – igazolható módon – tájékoztatni kell a munkavállalókat a megfigyelőrendszer alkalmazásával együtt járó adatkezelés lényeges körülményeiről, a kamerák látókörében figyelemfelhívó jelzést is el kell helyezni.
Az, akinek jogát vagy jogos érdekét a felvétel, illetve más személyes adatának rögzítése érinti, az adatkezelés tartamán belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje. Bíróság vagy más hatóság megkeresésére a felvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre attól számított harminc napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a felvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.
A felvételt, valamint más személyes adatot csak az arra jogosult személy jogosult megismerni, akinek ez a szerződésből fakadó kötelezettségei érvényesítéséhez szükséges, és a jogsértő cselekmény megelőzése vagy megszakítása érdekében mellőzhetetlen. A felvételt, valamint személyes adatot kezelő, vagy egyéb okból annak megismerésére jogosult személy- és

vagyonvédelmi tevékenységet végző személy nevét, az adatok megismerésének okát és idejét jegyzőkönyvben kell rögzíteni.

### *15.2. Hordozható informatikai eszközök (laptop, táblagép), központi és felhőszolgáltatási tárhely, internet-hozzáférés, elektronikus levelezés, mobiltelefon*

A Hiventures a munkavállalók részére a munkakörök ellátásához, kizárólag munkavégzés céljára hordozható informatikai eszközt, központi és felhőszolgáltatási tárhelyet, internet-hozzáférést, elektronikus postafiókot biztosíthat. Az informatikai biztonság szintjének fenntartása érdekében ezen eszközök és szolgáltatások használatával kapcsolatos forgalmi adatokat a Hiventures az Mt. 11/A. § alapján naplózza és szükséges mértékben ellenőrzi.
Az ellenőrzésre szolgáló technikai eszközök és biztonsági rendszerek alkalmazásáról a munkavállalókat minden részletre kiterjedően tájékoztatni kell.
Az informatikai eszközök és szolgáltatások rendeltetésszerű használatára fel kell hívni a munkavállalók figyelmét, beleértve azt is, hogy az informatikai eszköz használata önmagában megteremti annak jogalapját, hogy az abban rögzített adatokat a munkáltató, a jogszabályi előírásoknak és jelen szabályzatnak megfelelően felhasználja, és az informatikai eszköz használatát ellenőrizze.
Az előírások megsértése esetén, indokolt esetben tájékoztatni kell a munkáltatói jogokat gyakorló vezetőt, aki a Compliance Önálló Osztály kollégájával és az illetékes rendszergazda bevonásával külön eseti ellenőrzést rendelhet el. Amennyiben az informatikai biztonság veszélyeztetése is felmerül, akkor indokolt az Informatikai Biztonsági Felelős bevonása. A vizsgálat során biztosítani kell a munkavállaló jelenlétének lehetőségét. Az ellenőrzés tényét, helyét, indokát, eredményét, valamint a résztvevők nevét jegyzőkönyvben kell rögzíteni.
A Hiventures rendszereinek biztonsága érdekében a munkavállalók kötelesek megismerni és betartani a mindenkor hatályos Informatikai és Biztonsági Szabályzatában (a továbbiakban: IBSz) leírtakat.

#### *15.2.1. Elektronikus levelezés*

Az elektronikus levelet azonos szintű védelemben kell részesíteni, mint a hagyományos, postai úton továbbított küldeményt. A munkáltató megbízásából, a munkavállaló által hivatalos ügyekben írt és fogadott elektronikus dokumentum tartalmát a munkáltató jogosult megismerni, ugyanakkor biztosítani kell a levelezésben érintett harmadik személy azon jogát is, hogy az adatkezelés részleteiről tájékoztatást kapjon.
A Hiventures által biztosított elektronikus levelező rendszer használata során, a személyes adatok védelme érdekében, az alábbi szabályokat kell betartani:

- a levelező rendszer hivatalos célra használható;
- több e-mail címzett esetén az üzenet továbbítójának meg kell vizsgálni, hogy a küldemény valamennyi címzettjét rejtett módon (titkos másolat mezőben) adja meg a spam küldemények csökkentése érdekében;
- amennyiben a címzettek között a Hiventures levelezőrendszerén kívüli címzett is szerepel, vizsgálni kell az előző pontban leírt módszer alkalmazásának szükségességét;
- a nagyobb mennyiségű személyes adatot tartalmazó küldemény továbbítása kizárólag technikai védelemmel (illetéktelen megnyitás ellen jelszóval védett Office dokumentumban, RMS védelemmel, jelszóval védett tömörített állományban stb.) engedélyezett;
- A személyes adatot tartalmazó elektronikus leveket a következő záradékkal kell ellátni: „A jelen levélben kézbesített információ kizárólag a címzettnek szól, és bizalmas üzleti, illetve személyes adatokat tartalmazhat. Amennyiben nem Érintett a levél címzettje, a

levélben található információ felhasználása, vagy bármilyen módon történő közzététele, másolása vagy megosztása tilos. Amennyiben jelen levelet tévedésből kapta meg, kérem lépjen kapcsolatba a levél feladójával és az üzenetet haladéktalanul törölje a számítógépéről. A levél feladójának e-mail címe kifejezetten vállalati felhasználásra szolgál, a biztonsági szervezet – vezetői ellenőrzés céljából – betekinthet tartalmába, kérem erre a címre magánjellegű küldeményt, reklámanyagot ne küldjön!".

A munkavállaló által használt e-mail postafiók ellenőrzése:

- a munkavállalót az ellenőrzést megelőzően tájékoztatni kell az ellenőrzés részleteiről;
- a munkáltató korlátozhatja az e-mail postafiók használatát;
- meghatározhatók azok a címek, ahonnan e-mail fogadható, illetőleg amelyekre küldhető;
- korlátozható a küldött/fogadott levél mellékletének terjedelme.

A levelezésre használt hordozható informatikai eszközök adattartalmára vonatkozóan a felhasználót a 3. számú mellékletben található dokumentum felhasználásával nyilatkoztatni kell.

A kizárólag munkavégzés céljából biztosított e-mail postafiók esetén a munkáltatónak joga van a postafiókban lévő e-mailek fejlécének megtekintése után – ahol szerepel a küldő és a fogadó személye, e-mail címe, a levél megnevezése, a küldés időpontja, a levél mérete – a konkrét levél kiadását kérni a munkavállalótól.

A munkavállaló a levél átadását csak a harmadik személy jogát sértő levéltitokra történő hivatkozással tagadhatja meg. Abban az esetben, ha az e-mail postafiókot kizárólag hivatalos használatra adták át számára és az abban található magánjellegű levelet a munkavállaló írta, vele szemben munkajogi szankciókat alkalmazhat a munkáltatói jogkörgyakorló.

Amennyiben egy munkavállaló tartós távolléte alatt, vagy munkaviszonyának megszűnését követően – kitöltött 3. számú melléklet hiányában – a személyhez rendelt e-mail postafiók ellenőrzése szükséges vagy indokolt, az érintett munkavállaló által a levelező rendszerben a postafiókjához hozzáféréssel rendelkező másik munkavállaló – ha ilyen személy nincs, vagy nem tartózkodik a munkahelyen, akkor a munkáltató felkérésére a rendszer üzemeltetéséért felelős informatikus – jegyzőkönyv felvétele mellett betekinthet az e-mail postafiókba.

Amelyik levélről egyértelműen megállapítható, hogy hivatalos tárgyú, átadható a munkáltatónak.

A távollévő érintettet, az információs érintett rendelkezési jog maradéktalan érvényesülése érdekében tájékoztatni kell arról, hogy más személy az e-mail postafiókja tartalmát megismerte.

### *15.2.2. Mobiltelefon*

A Társaság által a munkavállalók rendelkezésére bocsátott mobiltelefon a hívások és az sms-ek vonatkozásában használható magáncélra is, azonban a használatnak *A céges mobiltelefonok használatáról szóló 5/2022. (10.27.) számú vezérigazgatói utasításban* (a továbbiakban: Utasítás) meghatározott keretösszeget meghaladó költségét a munkavállaló köteles viselni. A költségviselés szabálya irányadó abban az esetben is, amikor a szolgálati E-SIM/SIM-kártyát a munkavállaló saját tulajdonában lévő készülékében – mely megfelel a mindenkor hatályos IBSz-ben és az Utasításban rögzített informatikai biztonsági követelményeknek – használja.

Az ellenőrzés során a Hiventures a következő szabályokat alkalmazza:

- Ellenőrzésre kizárólag a Társaság jogos gazdasági érdekével összefüggésben kerülhet sor.
- Az ellenőrzést kizárólag a Gazdasági funkciót ellátó munkavállalója végezheti (az egyes eszközök ellenőrzéséhez szakmai segítséget vehet igénybe, pl.: informatikus).
- Az ellenőrzés során a fokozatosság elvére való tekintettel az ellenőrzést végző az ellenőrzött eszközt birtokló munkavállaló jelenlétében (illetve amennyiben ez lehetetlen vagy

ellentétes az ellenőrzés céljával, úgy a munkavállaló jelenlétén kívül) megbizonyosodik arról, hogy a munkavállaló a rendelkezésére bocsátott eszközt rendeltetésszerűen használta.
- A használat ellenőrzése nem terjedhet ki arra, hogy a munkavállalók magáncélból kit és mikor hívtak fel.
- Amennyiben titoktartási kötelezettség vagy üzleti titok megsértése, vagy a Hiventures részéről polgári jogi, munkajogi vagy büntetőjogi igényt megalapozó okból kerül sor az ellenőrzés lefolytatására, úgy a potenciálisan privát tartalmat (és így potenciális személyes adatot, akár különleges adatot) tartalmazó adatokat, dokumentumokat, beszélgetéseket, levelezéseket a munkavállalónak lehetősége van az ellenőrzést végző előtt felfedni, ezzel alátámasztva a rendelkezésére bocsátott eszköz rendeltetésszerű használatát.
- Amennyiben a munkavállaló felfedi a kétes elem tartalmát és megállapítást nyer, hogy rendeltetészerűen használta az eszközt, úgy a Hiventures biztosítja részére a további eszközhasználatot.
- Amennyiben a munkavállaló megtagadja a kétes elem tartalmának felfedését, vagy felfedi ugyan, de a vizsgálat során megállapítást nyer, hogy a munkavállaló a rendelkezésére bocsátott eszközt nem rendeltetésszerűen használta, úgy az eszköz használati joga megvonásra kerülhet, illetve további munkajogi következmények kerülhetnek alkalmazásra.

Az eszközök nem előírásszerű használata esetén a használati jog megvonásra kerülhet.

A fenti informatikai és infokommunikációs eszközök előzőekben bemutatott ellenőrzésén túl a Társaság – különösen az alábbi indokolt esetekben – további ellenőrzést folytathat le, az adott ellenőrzéssel érintett munkavállaló tájékoztatása mellett:

- a munkavállaló munkaköre gyakorlása során tudomására jutott védendő információt arra illetéktelen személlyel, vagy szervezettel megosztja;
- a munkavállaló munkáltatója felé fennálló együttműködési kötelezettségét megszegve jár el;
- amennyiben az érintett munkavállaló nyilatkozatának beszerzése lehetetlen és azt a közeli hozzátartozója írásban, indokai megjelölésével kéri, továbbá alappal feltehető, hogy az adatok kiadása az érintett munkavállaló létfontosságú érdekei védelméhez szükséges, valamint az adatok kiadását az Adatvédelmi Tisztviselő véleményének kikérését követően indokoltnak, az információs önrendelkezési jog korlátozásával arányosnak tartja.

### *15.3. Beléptetőkártya*

A Társaság által használt beléptető rendszer alapján lehetőség van a munkavállalók céges beléptetőkártyája adatainak (munkavállaló neve, melyik szervezetben dolgozik, beléptetőkártya azonosító száma, randomizált egyedi azonító, beléptetőkártya RFID azonosító száma, ki, melyik ajtót használhatja) ellenőrzésére, melyre jelenleg nem kerül sor. A céges beléptetőkártya és a munkaidő-nyilvántartás nem kerül összekapcsolásra.

## *16. Jelentési és tájékoztatási kötelezettség*

Az a munkavállaló, akinek tudomására jut, hogy a Hiventures vagy annak adatfeldolgozója által kezelt személyes adat jogosulatlan személy tudomására jutott, vagy jogsértő módon került továbbításra, köteles erről az Adatvédelmi Tisztviselőt tájékoztatni. Az Adatvédelmi Tisztviselő intézkedik az eset körülményeinek feltárásáról és az adatkezelő szerv vezetőjén keresztül gondoskodik az érintett haladéktalan tájékoztatásáról.

### *17. A személyes adatokat tartalmazó iratok kezelése*

A személyes adatokat tartalmazó iratok, adathordozók kizárólag zárt borítékban (vagy egyéb, ezzel egyenértékű megoldással, pl. jelszóval védett adathordozó, e-mail) továbbíthatók a címzett részére, és azokon fel kell tüntetni, hogy az „Zártan kezelendő!"

### *18. A személyes adatok védelme adatfeldolgozó igénybevétele esetén*

A Hiventures a munkaviszonyból származó kötelezettség teljesítése céljából a munkavállaló személyes adatait adatfeldolgozó számára átadhatja, amelyről a munkavállalót előzetesen tájékoztatni szükséges.
A munkavállalót már a belépéskor tájékoztatni kell adatainak külső szolgáltatóhoz történő továbbításáról. Ezt közérthetően és olyan módon kell megfogalmazni, hogy abból a munkavállaló számára világos legyen, hogy mely személyi kör jogosult az adataihoz hozzáférni.
A szolgáltató számára szerződésben kell meghatározni, hogy az adatok védelme érdekében milyen intézkedéseket kell megtennie, illetve a védendő adatok megőrzésére, valamint annak megszegése jogkövetkezményeire vonatkozó előírásokat is meg kell fogalmazni, tekintve, hogy az adatfeldolgozó által okozott, a munkavállalót ért kárért a munkáltató köteles helytállni.

### *19. A távolról végzett munka/távmunka*

Amennyiben a munkafeladatok ellátása távolról végzett munka útján valósul meg (pl.: VPN kapcsolaton keresztül), és az a Hiventures által biztosított eszköz igénybevételével történik, a Hiventures betekinthet az eszközön az érintett által tárolt, a munkaviszonnyal összefüggő adatokba. Amennyiben a távmunkához a Hiventures kizárólag munkavégzés céljára biztosítja az eszközt, a felhasználásával összefüggő tilalom, vagy korlátozás betartásának ellenőrzése céljából a Hiventures a teljes adattartalmat ellenőrizheti.

### *20. Üres asztal és tiszta képernyő*

A személyes adatok megfelelő kezelése érdekében a Hiventures valamennyi munkavállalója köteles a papír alapú dokumentumok és a digitális adathordozók fizikai hozzáférés védelméről gondoskodni, amelynek betartását a munkahelyi vezető alkalomszerűen ellenőrizheti. Az „Üres asztal, tiszta képernyő" szabály részleteit a Társaság *Informatikai Biztonsági Szabályzata* tartalmazza.
A személyes adatok feldolgozására szolgáló alkalmazásokat úgy kell kialakítani, hogy a monitoron történő megjelenítés során figyelmeztető jelzés utaljon a tartalom zárt kezelést igénylő jellegére (pl.: figyelmeztető felirattal vagy figyelemfelkeltő szín, effektus használatával). A jelenleg használt alkalmazások korrekciója során gondoskodni kell az előzőkben írtak szerinti megoldás megvalósításáról.

### *21. A munkahelyre érkező magánjellegű küldemények kezelése*

Magánjellegű levelezés folytatása a Társaságnál nem engedélyezett. Amennyiben ennek ellenére postai, vagy futár útján ilyen névre szóló küldemény érkezik, annak felbontása nem csak az érintett személyes adatai védelméhez, hanem a levéltitokhoz való jogának sérelmével is járhat, ezért azt más nem bonthatja fel, a címzettnek át kell adni, vagy a feladójának vissza kell küldeni.
Amennyiben kétség merül fel a levél hivatalos, vagy magánjellegét illetően, a címzett számára lehetőséget kell biztosítani a küldemény felbontására.

Ha egy levélről a felbontást követően derül ki, annak magánjellege, a borítékot vissza kell zárni és a jogos címzettnek átadni a Titkárság funkció értesítésével együtt.

### *22. Egyéb feladatok és felelősség*

Az érintett munkavállalókat felvételkor, illetve munkakörük megváltozása esetén, a munkakörük jellegéhez igazodóan, a kellő mértékig, dokumentált módon tájékoztatni szükséges az adatvédelem kérdéseiről, amelyért a munkáltatói jogkör gyakorlója a felelős.

### *23. Adatvédelmi szabályok megtartásának ellenőrzése*

Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint jelen Szabályzat rendelkezései érvényesülésének ellenőrzésére jogosultak:

a) a Hiventures Vezérigazgatója,
b) az Adatvédelmi Tisztviselő,
c) a Belső Ellenőr,
d) a jogszabályban erre felhatalmazott személy (pl.: a Hatóság tisztviselői),
e) a Hiventures által megbízott személy (pl.: külső auditor).

Az ellenőrzésnek különösen az alábbiakra kell kiterjednie:

a) adatvédelmi és adatbiztonsági szabályzat,
b) adatkezelési tájékoztató és adatvédelmi nyilatkozat,
c) az adatvédelmi nyilvántartásba történő bejelentés,
d) feliratok, piktogramok megléte,
e) a munkavállalók betekintési- és hozzáférési jogosultságának naprakészsége,
f) a fizikai biztonsági előírások érvényesülése,
g) a jelszavak időszakonkénti cseréje,
h) az adattovábbítási nyilvántartás vezetése,
i) adathordozók meglétének szúrópróbaszerű ellenőrzése,
j) a selejtezés, megsemmisítés végrehajtására, dokumentálása,
k) a jelen szabályzat rendelkezéseinek betartása.

### *24. Az Adatvédelmi incidens észlelése és jelentése*

Az adatvédelmi incidenseket a következő három klasszikus adatbiztonsági kritériumon keresztül kategorizálhatók:

- „Bizalmas jelleg sérülése”, ami a személyes adatok jogosulatlan vagy véletlen közzétételének vagy az ezekhez való hozzáférésnek felel meg;
- „Integritás sérülése” alatt a személyes adatok felhatalmazás nélküli vagy véletlenül bekövetkező módosítását értjük;
- „Rendelkezésre állás sérülése”, mely a személyes adatok véletlen vagy jogosulatlan megsemmisítésének vagy a személyes adatok elvesztésének felel meg.

Az adatvédelmi incidenst a tudomásra jutást követően indokolatlan késedelem nélkül, de legkésőbb 72 (hetvenkettő) órán belül be kell jelenteni a Hatóság részére, annak mindenkori nyomtatványa alapján (https://www.naih.hu/index.php/adatvedelmi-incidensbejelento-rendszer) kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.
Ha a bejelentés nem történik meg a megadott időintervallumban, a Társaság köteles ennek okát igazolni a hatóság felé, mely során mellékelni kell a késedelem igazolására szolgáló indokokat is.

A Társaság általi tudomásszerzésnek minősül, ha a Társaság észszerű bizonyossággal rendelkezik arról, hogy a bekövetkezett biztonsági esemény adatvédelmi incidensnek minősül.

Az a munkavállaló, aki a Hiventures által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz a biztonság olyan sérülését észleli, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést észlel, az köteles az **adatvedelem@hiventures.hu** kialakított elektronikus e-mail címen haladéktalanul, de legkésőbb 4 (négy) órán belül megtenni a bejelentést, megadva a nevét, telefonszámát és/vagy e-mail címét, a szervezeti egységét, dátum és pontos idő megadásával mikor észlelte az incidenst, az incidens tárgyát, valamint azt, hogy az incidens milyen eszközt, alkalmazást, rendszert érint.
A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

### *25. Az adatvédelmi incidens kezelése*

A bejelentett adatvédelmi incidens az Adatvédelmi Tisztviselőhöz kerül bejelentésre.
Az Adatvédelmi Tisztviselő összehívja az IT funkciót és a Compliance Önálló Osztály incidens kezelésére kijelölt kollégáit (a továbbiakban: csoport), és megvizsgálják a bejelentést.
Amennyiben a vizsgálat megállapítja, hogy az incidens nagy kockázatot jelent az érintett személyek jogaira és szabadságaira, akkor az Adatvédelmi Tisztviselő megkezdi a hatósági bejelentést a jelen Szabályzat 24. pontjában nevezett nyomtatványon.
Az incidens bejelentés szakaszosan is megtehető. A Hatósággal a kapcsolattartást az Adatvédelmi Tisztviselő tartja.
A bejelentés után az Adatvédelmi Tisztviselő és a csoport megkezdik a GDPR szerinti kockázatokkal arányos enyhítési feladatokat. Ennek alapján amennyiben az érintettek bevonása a kár enyhítése, illetve további elkerülése érdekében szükséges, úgy értesíteni kell az érintetteket is.
Az Adatvédelmi Tisztviselő az incidens kezelési folyamatot végig figyelemmel kíséri, és tanácsaival segíti a csoport munkáját.
Amennyiben az incidens nagy kockázatot jelent az érintettek jogaira és szabadságaira az adatvédelmi tisztviselő jelenti az esetet a vezérigazgatónak.
Az incidensekről a Hiventures nyilvántartást vezet.

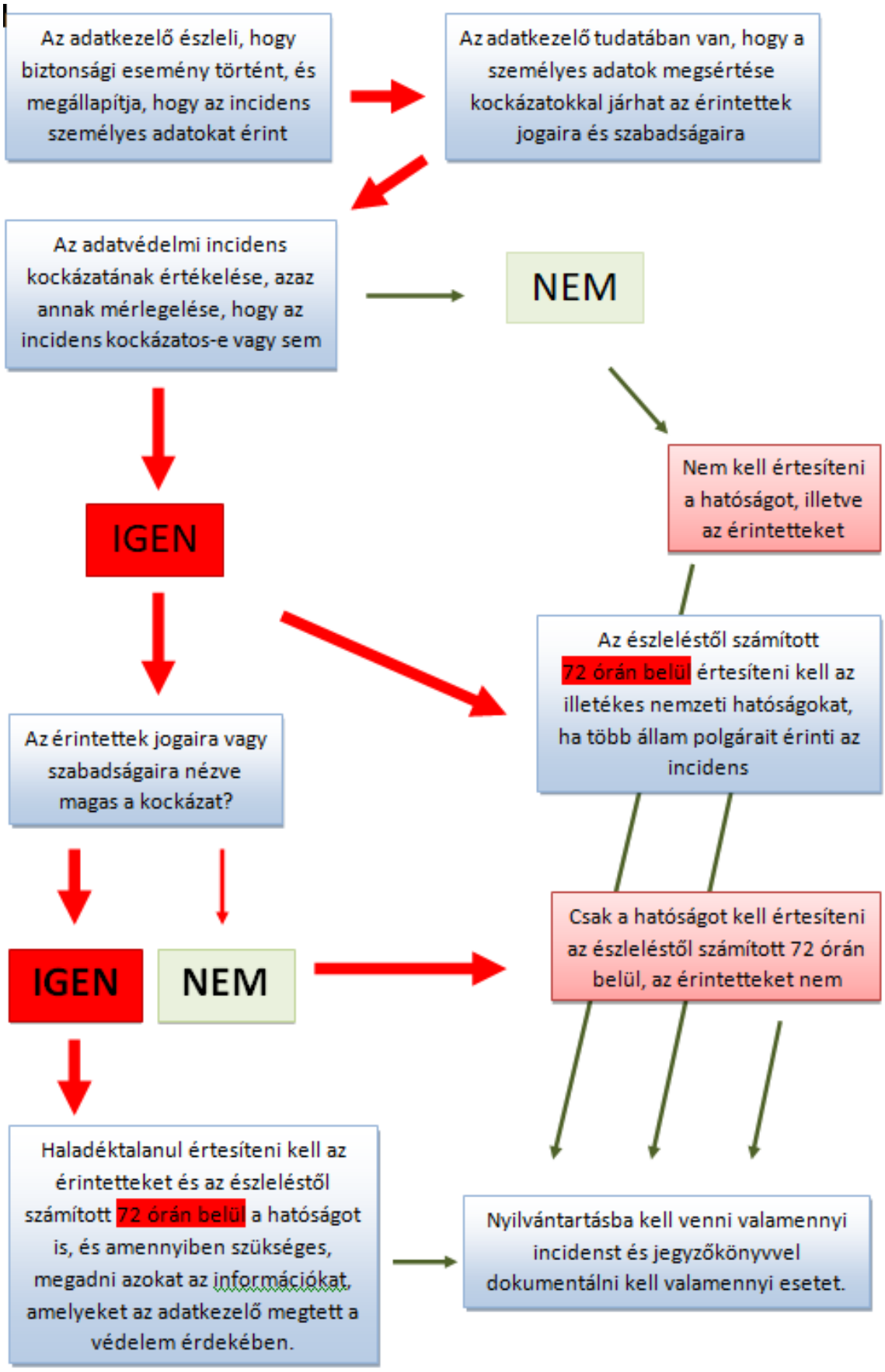
### *26. Az adatvédelmi incidens nyilvántartása*

Az adatvédelmi incidenseket nyilvántartásban rögzíteni kell a következő adatokkal:

a) az érintett személyes adatok körét,
b) az adatvédelmi incidenssel érintettek körét és számát,
c) az adatvédelmi incidens időpontját,
d) az adatvédelmi incidens körülményeit, hatásait,
e) az adatvédelmi incidens elhárítására megtett intézkedéseket,
f) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 (öt) évig, különleges adatokat érintő incidens esetében 20 (húsz) évig köteles a Hiventures megőrizni.

Az adatvédelmi incidenskezelés folyamatának sematikus ábrája:



## *27. Adatvédelmi hatásvizsgálat*

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. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

Az alábbi esetekben kötelező a hatásvizsgálat elvégzése:

- Ha egy természetes személy biometrikus adatainak kezelése módszeres megfigyelésre irányul.
- Ha kiszolgáltatott helyzetben lévő érintettekkel – különös tekintettel a gyermekekre, munkavállalókra, idős, mentális betegségben szenvedőkre – kapcsolatos biometrikus adat kezelése történik.
- Ha az adatkezelés egy természetes személy genetikai adatainak egyéb különleges adatokhoz vagy fokozottan személyes jellegű adatokhoz történő hozzákapcsolásával jár.
- Ha egy természetes személy genetikai adatai kezelésének célja a természetes személy értékelése vagy pontozása.
- Pontozás. Az adatkezelés célja, hogy az érintett bizonyos tulajdonságait felmérje, és annak eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére.
- Hitelképesség értékelése. Az adatkezelés célja, hogy az érintett hitelképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.
- Fizetőképesség értékelése. Az adatkezelés célja, hogy az érintett fizetőképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.
- Harmadik személytől gyűjtött adatok további felhasználása. Az adatkezelés célja, hogy a harmadik személytől begyűjtött személyes adatokat felhasználják az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál.
- Diákok, hallgatók személyes adatainak értékelésre való felhasználása. Az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép- vagy felsőfokú.
- Profilozás. Az adatkezelés célja személyes adatok nagy számú, illetve módszeres értékelése révén végzett profilozás, különösen, ha az az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján történik.
- Csalás elleni fellépés. Az adatkezelés célja hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázis felhasználása ügyfelek szűrésére.
- Okosmérők. Az adatkezelés célja közműszolgáltatók által telepített „okosmérők” alkalmazása (fogyasztási szokások nyomon követése).
- Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal. Az adatkezelés célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala, amely adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti.
- Módszeres megfigyelés. Érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok

felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera).
- Helymeghatározási adatok kezelése, ha az módszeres megfigyelésre vagy profilalkotásra utal.
- Munkavállaló munkájának megfigyelése. Munkavállalók munkájának megfigyelése. Az adatkezelés célja a munkavállaló munkájának megfigyelése során a munkavállaló személyes adatainak nagy számú és módszeres feldolgozása, illetve értékelése. Például GPS megfigyelő autóban történő elhelyezése, kamerás megfigyelés lopás vagy csalás elleni fellépés céljából.
- Különleges adatok nagy számban való kezelése. A GDPR (91) preambulumbekezdése alapján a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik.
- Nagyszámú személyes adatok kezelése bűnüldözési célból.
- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelése: pl. gyermekek, idősek, mentális betegségben szenvedők esetében.
- Gyermekek személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy marketing céljából, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában.
- Új technológiai megoldások használata az adatkezelés során. Ideértve az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelése (pl.: okos televízió, okos háztartási eszközök, okos játékok stb.), és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik.
- Egészségügyi adatokra vonatkozó adatkezelések. Nagy számban kezelt adatok tekintetében a kórházak, egészségügyi ellátó intézmények, magán-egészségügyi szolgáltatók vagy nagyszámú páciensi körrel rendelkező természetgyógyászok által kezelt különleges adatok vonatkozásában. Ideértve a nagyobb sportlétesítmények, edzőtermek által a tagoktól felvett egészségügyi adatok kezelése.
- Amikor több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni, amelyben különleges adatokat is kezelnek.
- Az adatkezelés célja a különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása.

A hatásvizsgálat legalább az alábbiakra terjed ki:

- a tervezett adatkezelési műveletek leírása és az adatkezelési célok egyértelmű, pontos meghatározása;
- a tervezett adatkezelési célok figyelembevételével annak megállapítása, hogy a tervezett adatkezelés szükséges-e, és az adatkezeléssel járó kockázat arányban áll-e az adatkezeléssel elérhető előnyökkel;
- az adatkezeléssel járó kockázatok feltárása és értékelése;
- a feltárt kockázatok kezelését célzó intézkedések.

A Társaság indokolt esetben az üzleti érdekeinek, a közérdek védelmének, illetve a tervezett adatkezelési műveletek biztonságának sérelme nélkül kikéri az érintettek véleményét a tervezett adatkezelésről. A hatásvizsgálat lefolytatásához szükséges ellenőrző kérdések a 4. számú mellékletben találhatók.

Amennyiben a hatásvizsgálat alapján az adatkezelés a Társaság által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal járna, a személyes adatok kezelését megelőzően a Társaság konzultál a Hatósággal. A konzultáció alapján a Hatóság tanácsokat adhat a tervezett adatkezeléshez, de akár meg is tilthatja azt a Társaság részére.

## *28. Érdekmérlegelési teszt elvégzése*

Amennyiben az adatkezelés jogalapját a GDPR 6. cikk (1) bekezdés f) pontja jelenti (az adatkezelés az adatkezelő vagy egy harmadik fél *jogos érdekeinek érvényesítéséhez* szükséges), az adatkezelési folyamat akkor és annyiban jogszerű, amennyiben az adatkezelés a Társaság vagy egy harmadik fél jogos érdekének érvényesítéséhez szükséges, kivéve, ha ezen érdekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

A jogos érdek, mint adatkezelési jogalap azonosításához az alábbi lépésekből álló tesztet kell elvégezni az adatgazdának:

1. a Társaság vagy a harmadik fél jogos – jogszabállyal összhangban álló – érdekének azonosítása;
2. az érintett alapvető jogainak, szabadságainak, valamint a – nem feltétlenül jogos –, a Társaság vagy a harmadik fél jogos érdekével szemben álló érdekének azonosítása;
3. a Társaság vagy a harmadik fél jogos érdeke és az érintett érdeke, alapvető jogai és szabadságai közötti mérlegelés elvégzése az alábbi szempontok alapján:
   - az érintettre nézve arányos-e a korlátozás;
   - a Társaság vagy a harmadik fél jogos érdeke nem érvényesíthető-e más módon, mint az érintett érdekének, alapvető jogainak és szabadságainak korlátozásával;
   - a kezelt adatok relevánsak-e;
   - az érintett jogai (előzetes tájékoztatás, tiltakozás) érvényesülnek-e az adatkezelése során;
   - a személyes adatok védelmét biztosító garanciális intézkedések (például adatbiztonsági kontrollok bevezetése, adatvédelmi hatásvizsgálat elvégzése) bevezetésre kerülnek-e.
4. az érdekmérlegelési teszt dokumentálása az elszámoltathatóság érdekében.

Az adatgazda tájékoztatást, szakmai tanácsot kérhet az Adatvédelmi Tisztviselőtől az érdekmérlegelési teszt elvégzése során.

## *29. Záró rendelkezések*

Jelen Szabályzat az aláírás napján lép hatályba, ezzel egyidejűleg hatályát veszti a 2020. február 13. napján hatályba lépett Adatvédelmi és Adatbiztonsági Szabályzat.

Budapest, 2025. október 13.

Hradszki László
Vezérigazgató

Mellékletek:

1. számú melléklet: Adatkezelési tájékoztató munkavállalók részére
2. számú melléklet: Nyilatkozat a Hiventures Zrt. Adatvédelmi és Adatbiztonsági Szabályzatának megismeréséről és tudomásul vételéről
3. számú melléklet: Nyilatkozat az informatikai eszközök adattartalmáról az eszköz visszaszolgáltatásakor
4. számú melléklet: Ellenőrző kérdések az adatvédelmi hatásvizsgálat elvégzéséhez
5. számú melléklet: Adattovábbítási nyilvántartás sablon
6. számú mellékelt: Adatvédelmi incidens nyilvántartás sablon