HOPI HOLDING	**A HOPI HOLDING a.s. belső irányelvei a személyes adatok feldolgozására és védelmére**	1/25 oldal. Verzió: Azonosító:

Ez a belső irányelv a HOPI HOLDING a.s. és a HOPI Csoporthoz tartozó társaságok számára készült, és arról tájékoztat, hogy mi, mint személyes adatok kezelője, hogyan gyűjtjük, kezeljük, használjuk és védjük a munkavállalók személyes adatait a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló (EU) 2016/679 európai uniós és tanácsi rendeletnek („GDPR") megfelelően.

A dokumentum érvényessége és hatálya: 2023. 01. 11-től határozatlan időre

	Kidolgozta:	Ellenőrizte:	Jóváhagyta a QM részéről	Jóváhagyta a HOPI CZ részéről
Beosztás:	Belső ellenőr	Jogi szolgálat		
Vezetéknév és utónév:	Knotek, Karel	Judr. Šmatlák, Jiří		
Dátum:	2023. 08. 01.	2023. 09. 01.		

Oldal	Javítás/Csere	Dátum	Vezetéknév és utónév

Tartalom

I. ÁLTALÁNOS RÉSZ

a) **A GDPR 4. cikkének 7. pontja értelmében adatkezelő az a jogalany, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.**

b) **A személyes adatok kezelője a HOPI HOLDING a.s. társaság** (a továbbiakban: „**adatkezelő**"), valamint a **HOPI-csoporthoz tartozó következő társaságok**: HOPI s.r.o. (Cégazonosító: 453 56 700), HOPI Foods s.r.o. (Cégazonosító 280 16 572), HOPI Energy s.r.o. (Cégazonosító 280 17 005), HOPI CEE FISH HUB s.r.o. (Cégazonosító 066 17 883), HOPI GLOBAL Solution s.r.o. (Cégazonosító 140 12 316), HOPI FARMS s.r.o. (Cégazonosító 084 76 471), HOPI Real Estate s.r.o. (Cégazonosító 084 60 434), HOPI Activity Delta s.r.o. (Cégazonosító 090 73 647), HOPI CZ Fleet Services s.r.o. (Cégazonosító 090 73 591), HOPI CHEF TECH FOOD a.s. (Cégazonosító 098 55 009), HOPI Properties s.r.o. (Cégazonosító 099 86 626), HOPI GLOBAL Solution Czechia s.r.o. (Cégazonosító 177 32 662), FineDine s.r.o. (Cégazonosító 087 75 486), HOLLANDIA Karlovy Vary, s.r.o. (Cégazonosító 405 22 962) a PERFECT CANTEEN s.r.o. (Cégazonosító 090 50 329), PERFECT CATERING s.r.o. (Cégazonosító 27427358), EAT PERFECT s.r.o. (Cégazonosító 09073469), Farma Otročín s.r.o. (Cégazonosító 001 16 262), FARMA MALONTY s.r.o. (Cégazonosító 600 71 222), Družstvo ČESKÉ BIOMLÉKO (Cégazonosító 293 62 148), Milchhof Joghurt GmbH (HRB 235289), AD FineDine GmbH (HRB 516819), HOPI SK s.r.o. (Cégazonosító 35785 632), HOPI SK Activity s.r.o. (Cégazonosító 54 312 868), HOPI GLOBAL Solution Hungary Kft. (Cg.13-09-217427), HOPI Hungária Logisztikai Kft. (Cg. 13-09-108397), HOPI GLOBAL SOLUTION ROMANIA S.R.L. (J35/3085/2022), HOPI RO LOGISTICS S.R.L. (J35/277/2013), HOPI GLOBAL Solution Poland sp.z.o.o. (0000999128), HOPI PL POLAND sp.z.o.o. (0000427499), az Ústí nad Labem-i Regionális Bíróságon vezetett cégnyilvántartásba bejegyezve, betétszám: B2165, adószám: 287 36 931**.**

c) Az **adatkezelő** a székhely címén érhető el: Pražská 673, 431 51 Klášterec nad Ohří, iroda: Pražská 673, 431 51 Klášterec nad Ohří, vagy telefonon: +420 474 375, fax: +420 474 375 095, e-mail: hopi@hopi.cz

d) Ez a belső szabályzat azoknak a személyes adatoknak a feldolgozását és védelmét szabályozza, amelyeket a munkáltató, mint **adatkezelő**, a munkavállalóiról és az álláspályázatokra jelentkezőkről kezel.

e) Ez a belső szabályzat elsősorban a személyes adatok kezelésének célját, a személyes adatok kezelésének eszközeit és módját, valamint a személyes adatok védelmét biztosító technikai és szervezési intézkedések dokumentálását szolgálja.

II. FOGALOMMEGHATÁROZÁSOK

a) **GDPR**: „general data protection regulation", azaz az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: angol rövidítéssel „**GDPR**" vagy „**Rendelet**"). A GDPR rendelet a személyes adatok védelmének általános jogi keretét jelenti, amely az EU egész területén – és bizonyos esetekben ezen a területen kívül is – érvényes és

hatályos. A GDPR fő célja, hogy biztosítsa az érintettek jogainak átfogó védelmét személyes és egyéb adataik jogosulatlan kezelésével szemben, egyensúlyt teremtsen az adatkezelők, az adatfeldolgozók és az adatok érintettjei jogos érdekei közötti egyensúly megteremtése, az egységes jogérvényesítési rendszer és egységes szankcionálási mechanizmus létrehozása ezen a területen.

b) **Személyes adat**: az azonosított vagy azonosítható természetes személyre (a továbbiakban: „**érintett**") vonatkozó bármely információ; azonosítható természetes személy az a természetes személy, aki közvetlenül vagy közvetve azonosítható, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, hálózati azonosító vagy az adott természetes személy fizikai, fiziológiai, genetikai, mentális, gazdasági, kulturális vagy szociális identitásának egy vagy több konkrét eleme alapján. Mindezeket az adatokat a GDPR-nak megfelelően kell kezelni. Személyes adat tehát egy vagy több olyan adat lehet, amelyek együttesen lehetővé teszik egy adott személy azonosítását. Személyes adatnak minősül minden, ami egy adott személlyel kapcsolatban kerül rögzítésre.

c) Mik a személyes adatok:

A leggyakoribb általános személyes adatok:

- Vezetéknév és utónév
- Állandó lakcím, kézbesítési cím
- Nem, életkor
- Születési idő és hely
- Személyi azonosító szám
- Családi állapot
- Egészségügyi helyzet
- Fényképfelvétel, videofelvétel, hangfelvétel
- E-mail cím (különösen, ha az tartalmazza a nevet és/vagy a cégnevet)
- Személyes és munkahelyi telefonszám
- IP-cím
- Különféle, állam által kiadott azonosító adatok: személyazonosító szám, adószám, személyazonosító igazolvány száma, vezetői engedély száma, útlevélszám és továbbiak...
- Iskolai végzettség
- Munkaviszonyból származó jövedelem (bér, fizetés), nyugdíjból származó jövedelem
- Gyermekek vagy házastárs, élettárs személyes adatai

A leggyakoribb érzékeny személyes adatok: A GDPR általánosságban tiltja az érzékeny személyes adatok feldolgozását, kivéve a rendeletben kifejezetten felsorolt eseteket.

- Faji vagy etnikai származásra (nemzetiség) vonatkozó adatok, állampolgárságra vonatkozó adatok
- Politikai vélemények, politikai párthoz vagy mozgalomhoz való tartozás, 1989 előtti tagság a kommunista pártban (az Alkotmánybíróság szerint).
- Vallási meggyőződés
- Filozófiai hitvallás

- Szakszervezeti tagság
- Egészségi állapot – testi vagy lelki egészségre, egészségügyi szolgáltatások nyújtására vonatkozó adatok
- Szexuális irányultság
- Büntetőjogi vétségek
- Jogerős bírósági ítéletek

Genetikai adatok

- DNS, RNS
- Vércsoport
- A vér RH faktora stb.

Biometrikus adatok

- Arcmás
- Ujjlenyomat
- Az írisz képe
- A retina képe
- Aláírás, hang stb.

Sajátosságok . A számlaszám csak cégek, azaz jogi személyek esetében nem minősül személyes adatnak. Az egyéni vállalkozóhoz tartozó számlaszámok személyes adatnak minősülnek, mivel azok egy konkrét természetes személyhez kapcsolódnak.

A névjegykártyákon általában megadott adatok, mint például a név, e-mail cím vagy telefonszám, személyes adatoknak minősülnek, és a GDPR hatálya alá tartoznak. Kézi feldolgozás esetén azonban a GDPR csak azokra a személyes adatokra vonatkozik, amelyeket egy nyilvántartás tartalmaz (pl. egy belső informatikai rendszerben), vagy amelyeket egy ilyen nyilvántartásba kell felvenni. Ebben az értelemben a GDPR nem vonatkozik azokra a helyzetekre, amikor például egy munkavállaló letesz néhány névjegykártyát az asztalára, és nem dolgozik tovább velük semmilyen nyilvántartásban. Az uralkodó szakértői vélemény szerint pusztán a névjegykártya önkéntes átadása egy másik személynek (munkavállalónak) a névjegykártya személyes névjegyzékbe való felvételéhez való hozzájárulásként értelmezhető.

A gyakorlatban azt is meg kell határozni, hogy egy **nyilvános szerződésben** milyen személyes adatok tarthatók meg, és melyeket szükséges anonimizálni („kifeketíteni”). A szerződések közzétételével összefüggésben bizonyos esetekben természetes személyeket azonosító személyes adatok jelenhetnek meg. Ilyen helyzetek lehetnek például: • A vezeték- és keresztnév, a számlaszám és az aláírás kombinációja személyes adat lehet • Az egyéni vállalkozó székhelye a vezeték- és utónévvel kombinálva személyes adat, ha a székhely egybeesik a természetes személy lakóhelyével • A vállalkozást vezető természetes személlyel kötött szerződés fejlécének szövege jellemzően tartalmazza a vezetéknevet, az utónevet, a vállalkozás székhelyét (amely gyakran megegyezik az állandó lakcímmel), a cégnyilvántartási számot és a számlaszámot, míg a szerződés szkennelt változata tartalmazza a természetes személy aláírását is • Jogi személy ügyvezetője aláírásának és a számlaszámnak a kombinációja.

d) **A személyes adatok feldolgozása** A személyes adatok kezelését olyan kidolgozott, nem esetleges tevékenységnek kell tekinteni, amelyet az adatkezelő a személyes adatokkal meghatározott célból és bizonyos szempontból szisztematikusan végez. A személyes adatok kezelése alatt az adatok kezelésének teljes szokásos ciklusa értendő, azaz az adatok gyűjtése, rendezése, adathordozón való tárolása, visszakeresése és felhasználása, majd archiválása és megsemmisítése, valamint minden egyes művelet vagy korlátozott műveletsorozat, például az adatok adatbázisban való keresése és közzététele. A személyes adatoknak a GDPR-rendszer szerinti feldolgozása akkor is alkalmazandó, ha a feldolgozás automatizált módon, azaz információs és kommunikációs technológiák segítségével történik.

e) **Milyen személyes adatokat kezelünk?** Tevékenységeink részeként kezeljük az Ön személyes adatait. Az áttekinthetőség kedvéért ezeket több kategóriába soroltuk és az alábbiakban kivonatosan ismertetjük:

- Azonosító adatok, mint például vezetéknév, utónév, személyi igazolvány száma, születési dátum, titulus stb.
- Kapcsolattartási adatok, mint például cím, e-mail cím, telefon stb;
- Családi állapotra és családtagokra vonatkozó adatok, mint például házastárs, élettárs vagy gyermekek;
- Képzettségre vonatkozó adatok, például iskolai végzettség;
- Foglalkoztatási adatok, például munkáltató, jelenlegi pozíció stb;
- Gazdasági és pénzügyi adatok, mint például munkabér vagy egyéb díjazás, törvényes járulékok és adók, bankszámlaszám stb.
- A szerződésben megadott információk;
- A vonatkozó jogszabályoknak megfelelően az ellenőrzési vagy auditálási tevékenységek során szerzett egyéb adatok;
- Hang-, video- és fényképfelvételek, mindezek kizárólag bizonyos indokolt esetekben, a munkáltató jogos érdekei miatt feltétlenül szükséges mértékben
- Egészségügyi adatok, kizárólag a vonatkozó jogszabályokkal összhangban;
- Büntetőjogi vonatkozású adatok, például a hatósági erkölcsi bizonyítvány
- Egyéb olyan konkrét adatok, amelyeket Ön szolgáltat nekünk, akár panasza, petíciója, tiltakozása, javaslata, kérdése vagy például információkérése részeként.

f) **A munkavállalók személyes adatai, amelyeket adatkezelői minőségünkben a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló (EU) 2016/679 rendelet („GDPR") értelmében a munkaszerződés megkötésével és az azt követő jogi kötelezettségekkel összefüggésben gyűjtünk, kezelünk, használunk és védünk, a következők:**

<u>Általános munkavállalók</u>:

- vezetéknév, utónév, titulus
- születési vezetéknév és az összes korábbi vezetéknév
- nem
- születési dátum
- születési hely

- személyi azonosító szám
- személyes állapot (családi állapot)
- állampolgárság
- állandó lakcím
- levelezési cím
- kapcsolattartási e-mail cím
- kapcsolattartási telefon
- a foglalkoztatással kapcsolatos dokumentumok (bérjegyzék, nyugdíjbiztosítási nyilvántartási lap, adóköteles jövedelemigazolás stb.) küldésére szolgáló e-mail cím
- hivatalos dokumentumok fogadására szolgáló fiók azonosítója
- sürgősségi kapcsolat (kihez forduljunk, ha valami történik)
- egészségbiztosítás
- egészségbiztosítói azonosítószám
- társadalombiztosítási szám
- portré jellegű fénykép
- a gyermek/gyermekek (eltartottak) vezeték- és utóneve
- a gyermek/gyermekek másik szülőjének vezeték- és utóneve
- a gyermek/gyermekek másik szülőjének munkáltatója
- a gyermek/gyermekek másik szülőjének családi állapota
- határozatok – eltartottak I. (gyermek/gyermekek felügyeleti joga, örökbefogadás)
- eltartottakat érintő határozatok II. (tartásdíj, eltartási kötelezettség stb.)
- munkavégzéssel kapcsolatos tevékenységet tiltó ítéletek/határozatok
- a közigazgatási hatóságok határozatai a külföldiek ügyrendjével kapcsolatos ügyekben (munka és tartózkodás)
- a közigazgatási hatóságok határozatai a munkavállaló vagyoni helyzetét érintő ügyekben (végrehajtási utasítások, fizetésképtelenség stb.)
- a közigazgatási hatóság határozatai a személyi állapottal kapcsolatos ügyekben (megváltozott munkaképesség, rokkantság, özvegyi nyugdíj)
- a foglalkozás-egészségügyi szolgáltató közigazgatási határozatai (a munkaképességre vonatkozó orvosi szakvélemények, az élelmiszeripari dolgozó egészségügyi bizonyítványa)
- munkaviszony igazolása az előző munkáltatótól (előmeneteli kimutatás)
- az előző munkáltatótól származó adóköteles jövedelemre vonatkozó igazolás
- a gyermek másik szülőjének munkáltatójától származó igazolás
- a gyermek/gyermekek születési anyakönyvi kivonata
- az éves adóelszámoláshoz szükséges dokumentumok (jelzálogszerződések, nyugdíjbiztosítás, véradói igazolás stb.)
- igazolás a legmagasabb befejezett iskolai végzettségről (szakmunkás bizonyítvány, bizonyítvány, oklevél stb.)
- a 2006-ig elvégzett általános és középfokú oktatás részletei (a végzés éve, az oktatás típusa, a tanulmányok területe)

- a 2006 óta az általános és középiskolákban, főiskolákon és egyetemeken elvégzett tanulmányokra vonatkozó adatok korlátlanul (végzés éve, az oktatás típusa, az iskola székhelye, az iskola neve, a szakterület megnevezése)
- az eltartottak igazoló dokumentumai (tanulmányok igazolása stb.)
- igazoló dokumentumok a munkavállalás akadályoztatásának igazolására - átmeneti munkaképtelenség, beteg családtag gondozása (az egészségügyi intézmény neve, az orvos neve, a szabadság időtartama stb.)
- egyéb igazoló dokumentumok a munkavégzés akadályoztatásának igazolására (bírósági és egyéb hatósági igazolások, a katonai közigazgatás által kiadott katonai kiképzési tervek stb.)
- bankszámlaszám
- munkahelyi balesetek dokumentációja

<u>Külföldi állampolgárok esetében ezen felül</u>:

- az úti okmányban szereplő adatok (útlevél száma, ki és mikor állította ki, érvényesség – fénymásolatot készítünk)
- a munkavállalási engedélyben szereplő adatok (okmányszám, ki és mikor állította ki, érvényesség – fénymásolatot készítünk)
- a tartózkodási engedélyben szereplő adatok (okmányszám, ki és mikor állította ki, érvényesség – fénymásolatot készítünk)
- az uniós polgárok személyi igazolványának adatai (az okmány száma, ki és mikor állította ki, érvényesség – fénymásolatot készítünk).
- egészségbiztosítási kártya
- igazolás a lakhatásról (szállás biztosítása, bérleti szerződés stb.)

Személyes adatok, amelyek jellemzően az információs és kommunikációs technológiákhoz és az ezeket a technológiákat használó alkalmazásokhoz kapcsolódnak, és amelyek a szervezet által kezelt **kiberbiztonsági és adatvédelmi kérdések körébe tartoznak**. Mint az közismert, a hálózati adatok és a hitelesítő adatok azon adatok, amelyek lehetővé teszik a hálózaton lévő számítógépes rendszerek alapvető működését.

- azonosítószám
- földrajzi helymeghatározási adatok
- hálózati azonosítók/IP-cím, cookie-azonosító
- személyes vagy munkahelyi e-mail
- hitelesítési/azonosító adatok
- a fizikai, fiziológiai, kulturális vagy társadalmi identitás elemei
- a fizikai, fiziológiai, kulturális vagy társadalmi identitás elemei

g) **A személyes adatok kezelője az a szervezet, amely számára az adatkezelést külön jogszabály előírja.** Minden munkáltató a munkavállalói személyes adatainak adatkezelője a foglalkoztatási jogszabályokban meghatározott célok tekintetében. A személyes adatok kezelője a jogi normától

függetlenül minden olyan szervezet is, amely maga dönt a személyes adatok kezeléséről, vagyis meghatározza az adatkezelés célját és módját. Jogosult továbbá szerződés, felhatalmazás, megbízás vagy jogi szabályozás alapján a személyes adatokat egy másik adatkezelő részére kezelni. A GDPR értelmében az adatkezelőknek intézkedéseket kell bevezetniük az adatgyűjtési, -felhasználási és -megőrzési követelményeknek való megfelelés érdekében. Biztosítaniuk kell továbbá, hogy az emberek hozzáférjenek az adataikhoz, és hogy az adatfeldolgozók teljesítsék az adatok biztonságos és jogszerű feldolgozására vonatkozó szerződéses kötelezettségeiket.

h) Az **adatfeldolgozó** szerződés, megbízás, felhatalmazás vagy jogszabályi rendelkezés alapján jogosult arra is, hogy személyes adatokat egy másik adatkezelő számára kezeljen. Az adatfeldolgozó esetében ez mindig egy külső, saját jogi személyiséggel rendelkező szervezet, pl. egy biztonsági ügynökség, amely az adatkezelő zárt láncú kamerarendszerét használja a telephelyek őrzésére, egy munka- vagy munkaerő-közvetítő ügynökség stb. A vállalaton belül azonban a belső könyvelési vagy HR osztály nem adatfeldolgozó. Így egy szervezet egyszerre lehet a személyes adatok adatkezelője vagy adatfeldolgozója különböző adatkezelések tekintetében.

i) Az érintett kizárólag az a természetes személy, akire a személyes adatok vonatkoznak, és aki a munkáltatóval munkaviszonyban vagy hasonló jogviszonyban áll.

j) A **személyes adatok kezelésének köre** a személyes adatok kezelésének módját, a tárolás időtartamát, az adatkezelés eszközeit, a címzettek kategóriáinak meghatározását, az adatkezelés okait és a személyes adatok kezelését leíró egyéb adatokat jelenti.

   A személyes adatok kezelése körének meghatározása magában foglalja az adatkezelés jogalapjának (**jogcímének**) meghatározását is, valamint az érintettől szerzett személyes adatok esetében azt, hogy a személyes adatok gyűjtése **jogszabályok által előírt** vagy **szerződéses** követelmény-e.

k) A Cseh Köztársaságban a magánélet és a személyes adatok védelmét felügyelő központi közigazgatási hatóság az **Úřad pro ochranu osobních údajů** (Személyes Adatok Védelmével Foglalkozó Hivatal, a továbbiakban: „**Hivatal**"). A Hivatal tevékenységét a személyes adatok kezeléséről szóló 110/2019 sz. törvény határozza meg.

l) Az **adatvédelmi tisztviselő** („Data Protection Officer" vagy DPO) az adott adatkezelő vagy adatfeldolgozó személyes adatok védelmével kapcsolatos koordinátorként vagy segítőjeként működik, és egyúttal egyfajta kapcsolattartóként is működik a felügyeleti hatóságokkal (a Cseh Köztársaságban az Úřad pro ochranu osobních údajů hivatallal) való kapcsolattartás során. Az adatvédelmi tisztviselő a **munkavállaló kapcsolattartója** abban az esetben, ha a munkavállalónak aggályai merülnek fel az adatvédelmi megfeleléssel és a GDPR-nak való meg nem feleléssel kapcsolatban.

m) Az **automatizált adatfeldolgozás** úgy értelmezhető, hogy az adatfeldolgozást információs rendszerek, azaz logikailag automatizált szoftverek végzik. Leegyszerűsítve tehát az automatizált adatfeldolgozás a számítástechnika segítségével történő automatizálást jelenti.

n) Az **álnevesítés** az általános rendelet meghatározása szerint a személyes adatok olyan módon történő kezelése, hogy azok további információk felhasználása nélkül nem feleltethetők meg egy adott érintettnek. Ezeknek a kiegészítő információknak elvileg el kell különülniük a természetes

személyre vonatkozó többi információtól, és technikailag és szervezeti szempontból biztonságosnak kell lenniük. Az **álnevesítés** kétirányú, vagyis a létrehozott fájlból vissza lehet generálni az eredeti fájlt.

o) Az **anonimizált adatok** olyan adatok, amelyek még közvetve sem teszik lehetővé egy adott személy azonosítását, és ezért semmilyen módon nem kapcsolódnak az adott személyhez. Ezáltal szabadabban kezelhetőbbek, mivel nem vonatkoznak rájuk az **adatvédelmi törvény** szigorú szabályai.

p) **Hozzájárulás a személyes adatok kezeléséhez.** Az érintett hozzájárulásának olyan szabadon megadott, konkrét, tájékoztatáson alapuló és egyértelmű akaratnyilvánításnak kell lennie, amellyel az érintett nyilatkozat vagy más nyilvánvaló megerősítés útján hozzájárulását adja személyes adatainak kezeléséhez. Az embereknek joguk van visszavonni a beleegyezésüket, és erről a jogukról tájékoztatni kell őket. A hozzájárulást olyan személynek kell kifejeznie, aki megfelel az adott állam jogszabályai szerinti korhatárnak, ellenkező esetben hozzájárulását a szülőnek vagy törvényes gyámnak hitelesítenie kell.

A személyes adatok kezeléséhez adott **hozzájárulás** a következő módon történhet:

- **Írásbeli hozzájárulás a személyes adatok kezeléséhez**. A személyes adatok kezeléséhez való hozzájárulást külön nyomtatványon kell feldolgozni; az nem lehet része például egy munkaszerződésnek. A hozzájárulás szövegének tartalmaznia kell egy arra vonatkozó nyilatkozatot, hogy ez egy olyan hozzájárulás, amelyet az érintett személynek nem kötelező megadni, ugyanakkor a hozzájárulást bármikor visszavonhatja. Ellenkező esetben a hozzájárulás érvénytelen, és annak kezelése a GDPR-t megsértve jogellenesnek minősül.

- **Elektronikus hozzájárulás a személyes adatok kezeléséhez.** Ha a hozzájárulás megadása a weboldalon található űrlap formájában történik, a hozzájárulást egyértelműen ki kell fejezni, azaz a bejelölő négyzet nem lehet előre bejelölve. A felhasználónak kell azt bejelölnie. A felhasználó jogosult kell, hogy legyen arra, hogy a hozzájárulását bármikor visszavonhassa, ugyanolyan egyszerűen, mint ahogy azt megadta. Az általánosan elfogadott lehetőség a „Jelölje be a beleegyezés jelölőnégyzetét, és adja meg az e-mail címét” szöveg. Azonban minden elküldött e-mailben lehetőséget kell biztosítani arra, hogy a felhasználó egyszerűen leiratkozhasson az üzenetekről. A személyes adatok kezeléséhez az interneten keresztül történő hozzájárulás akkor lehetséges, ha az a GDPR-nak megfelelően visszamenőlegesen bizonyítható és ellenőrizhető.

q) **A munkavállaló hozzájárulása a személyes adatainak kezeléséhez** csak abban az esetben kerül alkalmazásra, ha a munkáltató a személyes adatok kezelését nem tudja más jogcím alá rendelni. A GDPR 6. cikke szerint a hozzájárulás csak az egyik jogcím a személyes adatok kezelésére.

A személyes adatok kezeléséhez való hozzájárulás a munkaviszonyban csak minimálisan van jelen. A munkavállaló hozzájárulása az adatok kezeléséhez csak akkor lehetséges, ha nincs más jogcím. A hozzájárulás szükséges a kiválasztási eljárás lefolytatását követő további

adatfeldolgozás esetén azon jelöltek esetében, akiket nem választottak ki, de akiknek személyes adatait a munkáltató meg kívánja őrizni az esetleges jövőbeli állásajánlatok tekintetében.

r) **A munkavállaló tájékoztatása a személyes adatok kezeléséről**. A munkáltató a személyes adatokat elsősorban a szükséges személyzeti és bérszámfejtési adminisztráció céljából kezeli a munkavállaló hozzájárulása nélkül. Az adatok kötelezően megadandó voltát a munkavállaló részéről a szerződés teljesítése, a jogi kötelezettségek teljesítése vagy a munkáltató jogos érdeke biztosítja.

Ebben az esetben a munkáltató csak arra köteles, hogy tájékoztassa a munkavállalót személyes adatainak kezeléséről. Az esetek túlnyomó többségében a munkavállalók személyes adatainak kezelése nem a munkavállaló hozzájárulásán, hanem egyéb jogalapon nyugszik. A szerződés szükségessége az egyik olyan jogcím, ahol a személyes adatok kezelésének a szolgáltatás működéséhez szükségesnek kell lennie, és azt az érintettekkel kötött szerződésben kell meghatározni.

III. A BELSŐ SZABÁLYOZÁS HATÁLYA

Ez a belső szabályzat a munkáltató minden olyan munkavállalójára vonatkozik, aki bármilyen módon kezeli azokat a személyes adatokat, amelyeknek a munkáltató az adatkezelője vagy adatfeldolgozója. A HOPI HOLDING a.s. valamennyi egységére és munkahelyére, valamint a HOPI HOLDING a.s. valamennyi leányvállalatára és munkavállalójára vonatkozik azokban az országokban, ahol a vállalat működik. A jelen dokumentumtól való eltéréseket (eltérő jogszabályok, eltérő ügyfélkövetelmények stb.) országonként kell kezelni

IV. A DOKUMENTUM TULAJDONOSA

A dokumentum tulajdonosa, valamint a dokumentum rendszeres frissítéséért és felülvizsgálatáért felelős személy a HOPI adatvédelmi tisztviselője, akit kinevezési utasítással bíznak meg.

V. A SZEMÉLYES ADATOK KEZELÉSÉRE VONATKOZÓ POLITIKA

A munkáltató a személyes adatok kezelése során az alábbi alapelveknek tesz eleget:

1. Jogszerűség, méltányosság és átláthatóság

1.1. A személyes adatok munkáltató általi kezelésére csak a GDPR-ban vagy adott esetben más jogszabályokban meghatározott előírások alapján kerülhet sor, és azt a jogszabályokkal összhangban kell végezni. Az egyes adatkezelési tevékenységek konkrét jogalapjait e belső szabályzat X. fejezete tartalmazza.

1.2. A munkáltató a személyes adatok kezelése során köteles nyitott és átlátható módon eljárni, különösen annak tekintetében, hogy milyen módon kezeli a személyes adatokat. A személyes adatok kezelése során a munkáltató köteles az érintettek észszerű elvárásainak megfelelően eljárni az adatkezelés módját illetően,

és nem kezelheti a személyes adatokat olyan módon, amely indokolatlanul hátrányos hatást gyakorolhat az érintettekre.

2. Legalább egy jogalap igazolása, amely alapján a személyes adatok kezelése indokolt

3. Célhoz kötöttség

3.1. A munkáltató csak meghatározott, egyértelmű és jogszerű célból kezelhet személyes adatokat. Az adatkezelés konkrét módja és mértéke nem lehet aránytalan a célhoz képest.

3.2. A célt kellő egyértelműséggel kell meghatározni ahhoz, hogy nyilvánvalóvá váljon, milyen feldolgozási tevékenységeket végeznek a cél elérése érdekében. A célnak egyértelműnek kell lennie, és az érintett érintettet tájékoztatni kell a célról.

4. Az adatok minimalizálása

4.1. A munkáltató csak az adatkezelés célja szempontjából releváns személyes adatokat gyűjtheti és kezelheti, és csak a cél eléréséhez szükséges mértékben. A munkáltatónak minden egyes tervezett adatkezelési művelet esetében gondosan mérlegelnie kell, hogy a művelet szükséges-e az adatkezelés céljának teljesítéséhez, és hogy csak releváns és arányos személyes adatokat használ-e fel.

5. Pontosság

5.1. A munkáltató által kezelt személyes adatoknak pontosnak, tényszerűnek és szükség esetén naprakésznek kell lenniük. Ha az adatok nem pontosak, a munkáltatónak minden észszerű lépést meg kell tennie a pontatlan adatok kijavítása vagy megsemmisítése érdekében.

6. Korlátozott tárolás

6.1. A munkáltató csak addig őrizheti meg a személyes adatokat, amíg azok a személyes adatok kezelésének céljához szükségesek. A megőrzési időtartamot relatív módon is meg lehet határozni, azaz egy konkrét kiváltó eseményhez (pl. egy adott szolgáltatás nyújtásának megszűnése, a munkaviszony megszűnését követő elévülési idő lejárta stb.) viszonyítva. Ezen időszak után az érintett személyes adatokat meg kell semmisíteni vagy anonimizálni kell.

7. Integritás és bizalmas kezelés

7.1. A munkáltatónak a személyes adatokat oly módon kell kezelnie, hogy biztosítsa azok megfelelő védelmét a jogosulatlan vagy jogellenes adatkezelés, valamint a véletlen elvesztés, megsemmisülés vagy sérülés ellen. E célból a munkáltató és munkavállalói kötelesek betartani a jelen szabályzatban meghatározott valamennyi szabályt és eljárást.

A munkáltató felelős a fenti irányelvek betartásáért. A személyes adatokat olyan módon kell kezelni, amely biztosítja a megfelelő biztonságot, beleértve a megfelelő technikai vagy szervezési intézkedésekkel történő védelmet a jogosulatlan vagy jogellenes adatkezelés, valamint a véletlen elvesztés, megsemmisülés vagy sérülés ellen.

VI. A SZEMÉLYES ADATOK KEZELÉSÉNEK CÉLJA

a) A munkavállalóival kapcsolatban kezelt személyes adatokat, mint például a vezetéknév és utónév, személyazonosító szám, állandó lakóhely, személyi igazolvány vagy tartózkodási engedély száma, állampolgárság, kiskorú gyermekek száma és egyéb, a jogszabályokból eredő adatok, a munkáltató a természetes személyek foglalkoztatásával kapcsolatos kötelezettségi teljesítése érdekében kezeli, különösen a beteg-, nyugdíj- és egészségbiztosítás, valamint a bért és jövedelmet terhelő adók területén.

b) A munkavállalóival kapcsolatban feldolgozott személyes adatokat, azaz a végzettségre és képzettségre vonatkozó információkat a munkáltató egyrészt a munkavállalóval kötött szerződésből eredő kötelezettségek teljesítése céljából (különösen a munkavállaló olyan munkára való beosztásának kötelezettsége, amelyre a munkavállaló képzettséggel vagy képesítéssel rendelkezik), másrészt a munkáltató szerződéses partnereivel kötött olyan szerződések teljesítése céljából kezeli, amelyekben a munkáltató kötelezettséget vállal arra, hogy képzett személyek (munkavállalók) révén tevékenységeket végez vagy szolgáltatásokat nyújt.

c) A munkára jelentkező természetes személyekkel kapcsolatban kezelt személyes adatokat a munkáltató a megfelelő jelölt kiválasztása céljából kezeli a szerződés megkötésére irányuló intézkedések (kiválasztási eljárás) végrehajtása keretében, amely a munkára jelentkező személy pályázata alapján történik.

VII. A SZEMÉLYES ADATOK KEZELÉSÉNEK ESZKÖZEI ÉS MÓDSZEREI

a) A munkáltató a személyes adatokat a kiválasztási eljárás keretében az állásra pályázók által küldött önéletrajzok, valamint a munkaviszony kezdetekor a munkavállalók által kitöltött, személyes adatokat tartalmazó kérdőívek útján szerzi meg.

b) A személyes adatokat a munkáltató, azaz az **adatkezelő kezeli**, aki egyben az **adatfeldolgozó** is.

c) A munkáltató a személyes adatokat a következők formájában kezeli:

- a munkáltató által a munkavállalóival vagy az állásra pályázókkal kapcsolatban vezetett személyi akták és az állásra pályázókról szóló aktákban található dokumentumok formájában,

- elektronikusan egy olyan adatbázisban, amelyet a munkáltató a munkavállalóival vagy álláskeresőivel kapcsolatban vezet.

d) A munkavállalóknak joguk van hozzáférni az személyes adataikhoz, amelyet a munkáltató a munkavállalóival kapcsolatban kezel.

VIII. A SZEMÉLYES ADATOK BIZTONSÁGÁT SZOLGÁLÓ TECHNIKAI ÉS SZERVEZETI INTÉZKEDÉSEK

a) A **papíron tárolt személyes adatokra a következő szabályok vonatkoznak**:

1. A munkáltató célja, hogy korlátozza a személyes adatokat tartalmazó dokumentumok meglétét, ezért a személyes adatokat tartalmazó dokumentumok kinyomtatása csak szükség esetén engedélyezett.
2. A munkáltató munkavállalóinak a személyes adatokat tartalmazó dokumentumok kezelése során különösen a következő szabályokat kell betartania:

   2.1. A személyes adatokat tartalmazó dokumentumokat tilos az íróasztalon, az irodában vagy más helyen hagyni, mint ahol dolgoznak velük, kivéve, ha személyesen jelen vannak az adott helyen, hogy biztosítsák, hogy azokhoz illetéktelenek ne férjenek hozzá;

   2.2. Távollétük idején, különösen munkaidő után vagy amikor munkahelyükön kívül tartózkodnak, az iratokat zárható tárolóhelyeken, pl. íróasztalfiókokban, irattartó szekrényekben, szekrényekben stb. helyezik el, és ezeket a tárolóhelyeket bezárják. A tárolóhelyek kulcsait nem hagyhatják szabadon hozzáférhető helyen a tárolóhelyiségek helyiségeiben vagy máshol, ahol azokhoz illetéktelen személyek könnyen hozzáférhetnek;

   2.3. A személyes adatokat tartalmazó dokumentumok nem vihetők ki a munkahelyen kívülre, kivéve, ha az a munkaköri feladatok megfelelő ellátásához feltétlenül szükséges. Ha a személyes adatokat tartalmazó dokumentumokat a munkahelyen kívülre viszik, gondoskodni kell a jogosulatlan hozzáférés, elvesztés vagy megsemmisülés megakadályozásáról;

   2.4. A személyes adatokat tartalmazó dokumentumokat csak akkor lehet harmadik félnek (hatóságoknak, üzleti partnereknek, külső szolgáltatóknak) átadni, ha ez a jogi kötelezettségek teljesítéséhez vagy a munkáltató, illetve a személyes adatokkal érintett munkavállaló jogos érdekei miatt feltétlenül szükséges;

   2.5. Amennyiben a személyes adatokat tartalmazó dokumentumokat postai úton küldik, azokat lehetőleg annak a konkrét természetes személynek a saját kezéhez kell elküldeni, akinek azokat át kell vennie, amennyiben ez a személy ismert vagy azonosítható. A postai küldeményeket mindig úgy kell feladni, hogy a munkáltató visszaigazolást kapjon a célállomásra történő kézbesítésről.

   2.6. A személyes adatokat tartalmazó dokumentumok faxon nem küldhetők el. Ez a tilalom nem vonatkozik arra az esetre, ha a vonatkozó dokumentumokban szereplő személyes adatok kizárólag nyilvánosan hozzáférhető személyes adatok;

   2.7. Ha a munkavállalónak már nincs szüksége a személyes adatokat tartalmazó dokumentumokra a feladatai ellátásához, a munkavállalónak meg kell semmisítenie ezeket a dokumentumokat, vagy gondoskodnia kell azok megfelelő archiválásáról.

b) Az elektronikus formában tárolt személyes adatok védelmét hozzáférési jogok, vírusvédelem, biztonsági mentések és biztonsági irányelvek biztosítják.

c) A személyes adatokkal kapcsolatos számítástechnikai eszközök használatára **a következő szabályok vonatkoznak**:

1. A munkáltató munkavállalói (a továbbiakban: „felhasználók") a számítástechnikai eszközöket csak a munkájukkal kapcsolatos tevékenységekre és csak a hozzáférési jogosultságuk keretein belül használhatják. A felhasználók a számítástechnikai eszközök használata során kötelesek a rendszergazda és az általa felhatalmazott személyek utasításait követni;
2. A hozzáférési jogokat és engedélyeket a rendszergazda osztja ki a felhasználóknak. A felhasználó semmilyen módon nem jogosult olyan hozzáférési jogokat szerezni, amelyeket nem rendeltek hozzá. Ha a felhasználó olyan hozzáférési jogokat szerez, amelyek nem őt illetik meg, haladéktalanul értesítenie kell az illetékes rendszergazdát, és nem használhatja ezeket a jogokat;
3. A felhasználó köteles kizárólag a saját személyazonosságát használni. A felhasználó nem használhat olyan erőforrásokat, amelyekbe egy másik felhasználó személyazonosságával van bejelentkezve, és nem kísérelheti meg semmilyen módon megszerezni vagy felhasználni egy másik felhasználó személyazonosságát, kivéve, ha ez a munkáltató érdekében feltétlenül szükséges az ügyfelektől érkező szállítások és megrendelések feldolgozásához, és egyidejűleg ezeken az erőforrásokon keresztül csak nyilvánosan hozzáférhető személyes adatok feldolgozására kerül sor;
4. A jelszóval történő személyazonosság-ellenőrzés esetén a felhasználónak az adatkezelő által meghatározott szabályoknak megfelelő jelszót kell használnia, azt a visszaélések megelőzése érdekében titokban kell tartania, és a visszaélések megelőzése érdekében rendszeresen meg kell változtatnia;
5. Az információs rendszerekhez való hozzáférést biztosító jelszavak nem tárolhatók a számítógépen nem biztonságos (szabadon olvasható) formában, és nem lehetnek könnyen hozzáférhetőek a munkavállaló munkahelyén (hirdetőtáblán, lezáratlan fiókban, a billentyűzeten, monitoron stb. lévő papírlapon feltüntetve). A bejelentkezési adatokat nem szabad olyan helyzetekben megadni, ahol azokat más személyek megfigyelhetik.
6. A munkáltató munkavállalói csak a szokásos felhasználói tevékenységhez használhatják a számítógépes eszközöket. A felhasználók számára tilos minden technikai manipuláció, például az adathálózathoz való első csatlakozás, a számítógépes eszközök beállítása, szoftverek telepítése stb. A számítógépes eszközök technikai kezelésére kizárólag a rendszergazda vagy az általa megbízott személy jogosult;
7. A felhasználó köteles haladéktalanul értesíteni a rendszergazdát a számítógépes eszközök bármilyen meghibásodásáról. A számítástechnikai eszközök minden javítását a rendszergazda vagy az általa felhatalmazott személy végzi;
8. A rendszergazda engedélye nélkül tilos bármilyen technikai berendezést közvetlenül vagy közvetve az adathálózathoz csatlakoztatni;
9. Tilos olyan külső és hordozható lemezmeghajtókat csatlakoztatni a munkahelyi számítógépekhez (asztali PC, laptop), amelyek tartalma nem függ össze a munkaköri feladatokkal; az ilyen eszközökre történő írást a rendszergazdának kell jóváhagynia és engedélyeznie;

10. A felhasználók csak olyan programokat használhatnak, amelyeket számukra megfelelően átadtak, vagy amelyek használatát a számukra megfelelően átadott számítástechnikai eszközökön keresztül (pl. szerverprogramok és információs rendszerek) és a licencfeltételeknek megfelelően teszik lehetővé;
11. A felhasználó a rendszergazda megfelelő hozzájárulása nélkül nem avatkozhat be a számítástechnikai erőforrások és az adathálózat szoftverébe és műszaki berendezésébe;
12. A felhasználó nem akadályozhatja az adathálózat működését és teljesítményét, és nem használhat olyan szolgáltatásokat vagy szoftvereket, amelyek veszélyeztetik a hálózat működését vagy túlzott terhelést jelentenek, nem módosíthatja a szoftvert és nem manipulálhatja az adatokat;
13. Tilos olyan külső és hordozható lemezmeghajtókat csatlakoztatni a munkahelyi számítógépekhez (asztali PC, laptop), amelyek tartalma nem függ össze a munkaköri feladatokkal; az ilyen eszközökre történő írást a rendszergazdának kell jóváhagynia és engedélyeznie;
14. A felhasználó köteles betartani a számítógépes vírusok megelőzésére vonatkozó szokásos szabályokat (tilos megnyitni, elmenteni vagy futtatni a kéretlen vagy gyanús fájlokat, linkeket vagy e-mail mellékleteket stb.) Ha a felhasználó vírusfertőzésre gyanakszik, azonnal értesítenie kell a rendszergazdát;
15. Szigorúan tilos az adatokat a rendszergazda által jóváhagyottaktól eltérő internetes tárhelyeken (felhőkön) tárolni;
16. A munkahely elhagyásakor a felhasználó köteles a számítógépet (asztali számítógép, laptop) és az azon keresztül elérhető adatokat (a számítógép lezárásával) biztosítani a visszaélések ellen;
17. A felhasználó köteles a munkája során birtokába kerülő adatokat, különösen a személyes adatokat bizalmasan kezelni, és azokat más személyekkel nem közölni. Az adatokhoz, különösen a személyes adatokhoz való jogosulatlan hozzáférést, azok elvesztését vagy sérülését haladéktalanul jelenteni kell a rendszergazdának és a személyes adatok védelméért felelős tisztviselőnek.

d) Ha a munkavállalók a munkaköri feladataik ellátása során – például az e-mailek kezelésére – olyan mobileszközöket, például okostelefonokat és táblagépeket használnak, amelyek információs rendszerekhez, szerverekhez vagy a munkáltató hálózatához kapcsolódnak, akkor a következő szabályokat kell betartaniuk, függetlenül attól, hogy az eszköz a sajátjuk vagy a munkáltató által biztosított eszköz:
    1. A mobileszközöket úgy kell alkalmazni, hogy minden egyes eszközre legalább egy vírusirtó rendszer legyen telepítve, és a munkavállalók tartsák be a munkáltató információs rendszereihez e mobileszközökön keresztül történő hozzáféréssel kapcsolatos biztonsági szabályzatokat és általános biztonsági irányelveket;
    2. A mobileszközhöz való hozzáférést jelszóval kell védeni.
    3. Ha az eszközt nyilvános helyen használják, a felhasználónak gondoskodnia kell arról, hogy az eszközhöz illetéktelen személyek ne férjenek hozzá, illetve ne tudják azt lehallgatni;
    4. A mobil eszközt mindig megfelelően biztosítani kell az elvesztés vagy lopás ellen, figyelembe véve az adott helyzetet (különösen a felhasználó nem hagyhatja a készüléket a járműben vagy olyan helyen, ahol illetéktelen személyek hozzáférhetnek);

5. Minden személyes adatokat tartalmazó adatot törölni kell a mobileszközről, ha azok tárolása az eszközön már nem szükséges;
6. A felhasználónak haladéktalanul jelentenie kell a mobileszköz elvesztését, ellopását vagy a biztonság bármilyen más megsértését a rendszergazdának és a személyes adatok biztonságáért felelős tisztviselőnek.

e) Kiberbiztonság – A munkáltató a személyes adatokat elektronikus formában, információs rendszerek és webes alkalmazások segítségével kezeli. Felhasználónak csak azok a munkavállalók minősülnek, akik felhasználónévvel és jelszóval jelentkeznek be a környezetbe és az információs rendszerekbe. A munkáltató a magas kockázatot jelentő személyes adatokat titkosítja, álnevesíti vagy a kezelt adatok kockázati szintjének megfelelő egyéb technikai intézkedésekkel védi.

f) Az elektronikus formában tárolt személyes adatokat biztonságos tárolóhelyen kell tárolni. A biztonságot frissített vírusirtó program, további biztonsági javítások vagy biztonsági irányelvek, valamint tűzfal és más, a szervereket védő rendszerek, valamint a számítógépes hálózat védelme az internetről érkező támadások elleni védelem formájában valósítják meg. Ezzel egyidejűleg adatmentés is történik.

g) Az elektronikus kommunikáció biztonságos e-mail szerveren, adattároló fiókon keresztül és szükség esetén garantált elektronikus aláírással történik, amely a munkáltató és a kiválasztott munkavállalók számára elérhető.

h) A munkáltató által kezelt személyes adatokhoz való hozzáférés a munkáltatóval fennálló munkaviszonyukból adódó feladataik miatt jogosult munkavállalókra, valamint azokra a munkavállalókra korlátozódik, akiknek a Munka Törvénykönyve alapján joguk van a munkakörüknek és munkaköri feladataiknak megfelelően betekinteni a munkavállalók személyes aktáiba. Az alábbi pozíciókban dolgozó munkavállalókról van szó:

   - a HOPI személyzeti osztályának (HR) munkatársai
   - a rendszerek- és alkalmazások rendszergazdája (IT)
   - a HOPI bérszámfejtője
   - épületbiztonsági személyzet
   - a HOPI biztonsági vezetője
   - a disztribúció adminisztrációs személyzete

i) A személyes adatokhoz hozzáféréssel rendelkező munkavállalók kötelesek az ilyen adatok tartalmát bizalmasan kezelni, még munkaviszonyuk megszűnése után is.

j) A személyes adatok biztonságával foglalkozó munkavállalók kötelesek titokban tartani a személyes adatok védelmét biztosító biztonsági intézkedéseket, még munkaviszonyuk megszűnése után is.

k) Minden olyan munkavállalót, akit a személyes adatok vagy a biztonsági intézkedések bizalmas kezelése kötelez, a munkáltatónak egyénileg tájékoztatnia kell erről a kötelezettségéről, és az adatvédelem jogi hátteréről is oktatást kell biztosítania (lásd **Titoktartási és információvédelmi, valamint az adatokkal való visszaélés tilalmáról szóló megállapodás**, amelyet minden alkalmazott a munkaviszonya részeként ír alá).

l) A személyes adatok kezelésének elsődleges elemzése. E belső rendelet hatálybalépését megelőzően és az intézkedések megfelelő kialakítása érdekében a munkáltató elvégezte a személyes adatok kezelése jelenlegi helyzetének elemzését.

m) Kockázatelemzés – A munkáltató elvégezte a személyes adatok védelme és kezelése terén fennálló releváns kockázatok elemzését.

n) A személyes adatokhoz való hozzáférés korlátozása a munkáltató szervezeti struktúráján belüli hatáskörök meghatározásával, ahol az adatokhoz való hozzáférés általában osztályonként és munkakörönként differenciált. A jogszabályban előírt szervek minden adathoz és információhoz hozzáférnek.

o) Bizonyos címtárakhoz és alkalmazásokhoz (programokhoz) való hozzáférés korlátozása korlátozott számú jogosult személyre.

p) A munkavállaló csak olyan adatfeldolgozónak adhat át személyes adatokat, aki megfelelő garanciákat nyújt a szükséges technikai és szervezési intézkedések végrehajtására.

q) Az a munkavállaló, akinek személyes adatokat kell átadnia egy adatfeldolgozónak adatkezelés céljából, köteles ellenőrizni, hogy a munkáltató rendelkezik-e írásos szerződéssel az adatfeldolgozóval a személyes adatok kezelésére, és szükség esetén kezdeményezni egy ilyen szerződés megkötését.

r) A személyes adatok továbbítására a következő szabályok vonatkoznak:

1. Amikor személyes adatok továbbítására kerül sor harmadik félnek e-mailben történő kommunikáció útján, a munkáltatónak mindig mérlegelnie kell a természetes személyek jogait és szabadságait érintő valószínűsíthető kockázatokat, amelyeket a személyes adatok továbbításának ez a módja jelent, és e kockázatok fényében megfelelő biztonsági intézkedéseket kell hoznia.

    1.1. Elektronikus formában tárolt személyes adatok csak titkosított formában továbbíthatók harmadik félnek e-mailben, feltéve, hogy az adatok dekódolásához szükséges kulcsot csak olyan módon lehet a címzettnek továbbítani, hogy az e-mailes kommunikáció biztonságának megsértése esetén a kulcshoz a behatoló ne férhessen hozzá (pl. közönséges postai úton, telefonon, SMS-ben stb.); ez a szabály nem vonatkozik arra az esetre, ha kizárólag nyilvánosan hozzáférhető személyes adatokat továbbítanak.

    1.2. Amennyiben a személyes adatok továbbítása virtuális tárhelyre (cloud) történő feltöltéssel történik, az adatkezelőnek először meg kell győződnie

arról, hogy egy megbízható szervezet által üzemeltetett, kellően biztonságos adattárolóhelyről van-e szó, és hogy az adattovábbítás titkosított.

2. A személyes adatok papíralapú továbbítására az e belső irányelv VIII. cikkének a) pontjában meghatározott szabályokat kell alkalmazni.

s) A munkáltató évente teszteli, elemzi és értékeli a személyes adatok kezelésének biztonságát biztosító technikai és szervezeti intézkedések hatékonyságát.

t) A személyes adatokhoz hozzáféréssel rendelkező munkavállalók munkavégzési vagy szervezeti szabályzatának és munkaköri leírásának részét képezi egy titoktartási és adatvédelmi záradék, és hasonló tartalmú záradékot kell beépíteni az adatfeldolgozókkal kötött szerződésekbe. Szükség esetén a személyes adatok védelméről és a titoktartásról külön megállapodást kötnek ilyen értelemben.

IX. A MUNKAVÁLLALÓK SZEMÉLYES ADATOK VÉDELMÉVEL KAPCSOLATOS KÉPZÉSE

a) **Alapképzés**
Az adatvédelmi tisztviselő gondoskodik arról, hogy a munkáltató minden olyan munkavállalója, aki a munkaviszonya keretében személyes adatokat kezel, a HOPI Holdinghoz való csatlakozása előtt vagy közvetlenül azt követően megismerje a jelen belső irányelv tartalmát, valamint a személyes adatoknak a vállalaton belüli feldolgozására vonatkozó valamennyi szabályt és eljárást.

b) **Rendszeres képzés**
Az elszámoltathatóság elvére tekintettel az adatvédelmi tisztviselő gondoskodik a személyes adatok védelméről szóló időszakos képzés megszervezéséről, amelyet évente legalább egyszer meg kell tartani, és amelyen a munkáltató minden olyan munkavállalója részt vesz, aki munkaviszonya keretében személyes adatokat kezel.

X. AZ ADATVÉDELMI INCIDENSEK JELENTÉSÉRE ÉS BEJELENTÉSÉRE VONATKOZÓ ELJÁRÁS

a) A személyes adatok megsértése olyan esemény, amely a továbbított, tárolt vagy más módon feldolgozott személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását vagy jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi (a továbbiakban: „adatvédelmi incidens”).

b) Az adatvédelmi incidens bekövetkezhet mind a munkáltató vállalatán kívüli (pl. kibertámadások, ipari kémkedés), mind a munkáltató vállalatán belüli (pl. adatoknak a munkavállaló által harmadik fél számára történő jogosulatlan átadása), szándékos vagy gondatlan (pl. nem megfelelően védett adatok véletlen megsemmisítése) tevékenység révén.

c) Az adatvédelmi tisztviselő legkésőbb 72 órával azután, hogy az adatvédelmi incidenst a szervezetben először észlelték, értesíti a Hatóságot az adatvédelmi incidensről/adatszivárgásról.

d) Az adatvédelmi tisztviselő dokumentálja a jogsértéseket, azok hatásait és a meghozott korrekciós intézkedéseket. Ha az elektronikusan feldolgozott személyes adatok biztonságára vonatkozó jogsértés történik, a felelős munkavállaló 24 órán belül tájékoztatja az információs rendszereket kezelő személyt, hogy a behatolót azonosítsa, és 48 órán belül korrekciós intézkedéseket javasoljon. Az adatvédelmi incidensek kezelése során a munkáltató együttműködik a hálózati rendszergazdával, valamint a személyes adatok feldolgozásával és védelmével kapcsolatos biztonsági, technikai és szervezési intézkedések végrehajtásáért és ellenőrzéséért felelős személlyel.

e) Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintett jogaira és szabadságaira nézve, az érintettet az arra jogosult munkavállalónak indokolatlan késedelem nélkül értesítenie kell.

XI. A SZEMÉLYES ADATOK TÁROLÁSA ÉS MEGSEMMISÍTÉSE

a) A kiválasztási eljárás befejezésével összefüggésben a munkáltató megsemmisíti azon álláspályázók személyes adatait, amelyek kezelésének szükségessége megszűnt.

b) A munkaviszony megszűnésével összefüggésben a munkáltató megsemmisíti azon munkavállalók személyes adatait, amelyek kezelésének szükségessége megszűnt.

c) A munkáltató a munkaviszony megszűnését követően is köteles az előírt ideig archiválni a különleges jogszabályok által előírt megőrzendő dokumentumokat, különösen az adózás, a nyugdíj-, a beteg- és az egészségbiztosítás területén.

d) A munkáltató a munkaviszony megszűnését követően is köteles a szükséges ideig megőrizni azokat az iratokat, amelyek a munkáltatói jogok védelméhez szükségesek.

e) A személyes adatokat olyan formában kell megőrizni, amely lehetővé teszi az érintett azonosítását, legfeljebb annyi ideig, amennyi az adatkezelés céljainak eléréséhez szükséges; ezt követően az adatkezelő köteles a személyes adatokat megsemmisíteni. Pl. adott ideig, a szerződés időtartamára, a kiválasztási eljárás lezárásáig. Az adatokat nem lehet korlátlan ideig tárolni.

XII. A SZEMÉLYES ADATOK KEZELÉSÉNEK JOGALAPJA

a) Bármely személyes adat az alábbi, a **Rendeletből** eredő jogcímek alapján kezelhető, mégpedig:

- amennyiben a **Rendelet** kifejezetten megengedi (**öt jogcím**, ahol az adatkezelés megengedett); vagy
- az érintett hozzájárul az adatkezeléshez (**hatodik jogcím**).

b) A GDPR szerinti személyes adatok kezelésének egyik alapelve az adatkezelés jogszerűségének elve. Ez azt jelenti, hogy bármely személyes adatot a munkáltató csak akkor kezelhet, ha az ilyen adatkezelés a rendeletben meghatározott hat jogcím valamelyikének tulajdonítható:

1. **Szerződés**
   (az adatkezelés a szerződés teljesítéséhez szükséges, az érintett hozzájárulása nem szükséges)
2. **Jogi kötelezettség**
   (az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, az érintett hozzájárulása nem szükséges)
3. **Létfontosságú érdekek védelme**
   (az érintett hozzájárulása nem szükséges)
4. **Közérdek**
   (az érintett hozzájárulása nem szükséges)
5. **Jogos érdek**
   Az adatkezelés az adatkezelő vagy egy 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. Az érintett hozzájárulása nem szükséges.
6. **Az érintett hozzájárulása**
   A személyes adatok kezeléséhez való hozzájárulást ezért kizárólag akkor kell alkalmazni, ha a GDPR 6. cikke (1) bekezdésének b)-f) pontjában meghatározott más jogcím nem rendelhető a kezeléshez.

Személyes adatok nem kezelhetők jogalap nélkül.

Jogalap nélkül a személyes adatok nem továbbíthatók senkinek, az alábbiakat kivéve:

- Cseh Társadalombiztosítási Igazgatóság, Cseh Rendőrség, adóhivatal
- Támogatásnyújtó – szerződés, jogos érdek

XIII. SZERZŐDÉS

A személyes adatok kezeléséhez való hozzájárulásnak a következő feltételeknek kell megfelelnie.

- A hozzájárulás szövegének tömörnek és érthetőnek kell lennie.
- El kell különülnie a szöveg többi részétől.
- Ha az adatkezelésnek több célja van, a hozzájárulást minden egyes célra külön-külön meg kell adni.

- A 6. cikk (1) bekezdésének a) pontja megerősíti, hogy az érintett hozzájárulását „**egy vagy több konkrét célra**” kell megadni, és az érintettnek mindegyik cél tekintetében választási lehetősége van.
- A 6. cikk (1) bekezdésének a) pontja szerint a szabadon adott hozzájárulás másik jellemzője a **többszintűség**. Amennyiben egy szolgáltatás **több célú** adatkezelési műveletet foglal magában, az érintettnek választania kell, hogy mely célokat fogadja el, és nem kényszeríthető arra, hogy az adatkezelési célok teljes csomagjához hozzájáruljon.
- Szükség esetén lehetőség van a **hozzájárulás iránti kérelmek többszintűségét** biztosítani. Ha az adatkezelő több különböző célra kér hozzájárulást, akkor minden egyes célra külön választási lehetőséget kell biztosítania.
- Összefoglalva, az "egyediség" követelményének való megfelelés érdekében az adatkezelőnek célmeghatározást kell alkalmaznia a nem szándékolt funkciók kiterjesztése elleni biztosítékként oly módon, hogy a hozzájárulási kérelemben nem általános hozzájárulást kér, hanem egyetlen dokumentumban határozza meg az adatkezelési kérelem konkrét céljait.
- Az érintettnek aktív lépéseket kell tennie a hozzájárulás megadása érdekében.
- Az érintett nem köteles megadni a hozzájárulást, és nem büntethető a hozzájárulás megtagadása miatt.
- A hozzájárulás visszavonásának ugyanolyan egyszerűnek kell lennie, mint annak megadásának.
- Az adatkezelőnek képesnek kell lennie bizonyítani, hogy az érintett megadta a hozzájárulását.
- Az adatkezelő nem hallgathatja el az érintett előtt, hogy milyen célból kezeli a személyes adatokat.

XIV. A MUNKÁLTATÓ JOGOS ÉRDEKE

A munkavállaló személyes adatainak a munkáltató általi kezelése az adatkezelő (munkáltató) jogainak és védett (jogos) érdekeinek védelme érdekében szükséges. A munkavállaló személyes adatai kezelésének oka azonban nem állhat ellentétben az érintett (a munkavállaló) magánéletének védelméhez való jogával. A társaság érdekének érvényesülnie kell (az eljárás indokoltságát jogi indokokkal kell alátámasztani - pl. a Munka Törvénykönyve 103. § (2) bekezdése).

- A munkáltató a munkavállaló fényképét a munkavállaló hozzájárulása nélkül is kezelheti a vállalat belső biztonsági rendszerében a jogosultsággal bíró személyek azonosítása céljából.
- A szervezet biztonsági politikájára tekintettel a munkáltató megköveteli, hogy a munkavállalóról fénykép készüljön, és amikor a munkáltató telephelyén tartózkodik, a fényképes igazolványt jól látható helyen viselje (ezt a fényképet a munkáltató intranetjén is közzéteszik).
- A munkáltató a munkavállaló hozzájárulása nélkül is kezelhet munkával kapcsolatos személyes adatokat.

- Az adatkezelő jogos érdekének gyakorlása keretében a HOPI holding telephelyén található kamerarendszer videófelvételeinek megszerzése és rövid távú tárolása (a megőrzési idő egy hónap), nyomós okokból, különösen az adatkezelő tulajdonjogának ellenőrzése, a személyes egészségvédelem és az élelmiszer-védelem, valamint a telephely működésének általános biztonsága céljából.
- A munkáltató a szervezet biztonsági politikájára tekintettel kamerarendszert használ, a telephelyen elhelyezett kamerákkal, amelyek a munkavállalókról is felvételeket készítenek. Ez is az adatkezelő jogos érdeke alapján tehető meg, ugyanakkor az adatkezelőnek el kell végeznie egy arányossági vizsgálatot (más néven kiegyensúlyozottsági vizsgálatot), amelyben összehasonlítja, hogy az adatkezeléssel elérni kívánt cél (azaz a kamerarendszer által nyújtott biztonság) és a választott eszköz arányos-e az adatkezelés konkrét céljával vagy az érintettek jogaival és szabadságaival. Az adatkezelőnek képesnek kell lennie arra, hogy a fentieket ellenőrzés esetén igazolni tudja.
- Következésképpen a Munka Törvénykönyve 316. szakaszának (1) bekezdése a munkáltatónak jogot ad arra, hogy észszerűen ellenőrizze, hogy a munkavállalók a munka- és termelési eszközöket a rájuk bízott feladatok elvégzéséhez használják-e.
- A munkáltató a vállalati járműveiben GPS nyomkövető készülékeket használ, amelyek kikapcsolhatók. Ha a jármű helyének rögzítésére munkaidőben kerül sor, a személyes adatok feldolgozása az adatkezelő jogos érdekén alapul.
- A munkavállalók érzékeny személyes adatait ezután a GDPR 9. cikke (2) bekezdésének b) pontja szerinti jogalap alapján kezelik, amely lehetővé teszi az érzékeny személyes adatok kezelését, ha az szükséges az adatkezelő vagy az érintettek munkajogi, társadalombiztosítási és szociális védelemmel kapcsolatos kötelezettségeinek teljesítéséhez és különleges jogainak gyakorlásához. Ilyen eset például az, ha a munkáltató az általános egészségbiztosítási törvény vonatkozó rendelkezései alapján személyes adatokat továbbít egy egészségbiztosítónak. Ezen túlmenően a munkavállalók érzékeny személyes adatai a GDPR 9. cikke (2) bekezdésének h) pontja szerinti jogalap alapján is kezelhetők, amely ebben az összefüggésben lehetővé teszi az érzékeny személyes adatok kezelését, ha erre megelőző vagy foglalkozás-egészségügyi célokból vagy a munkavállaló munkaképességének felméréséhez van szükség.
- Mivel a munkavállaló egyben érintett is, a munkáltatónak eleget kell tennie a munkavállalóval szembeni tájékoztatási kötelezettségének is – azaz tájékoztatnia kell arról, hogy milyen személyes adatokat kezel róla, és milyen mértékben, milyen jogalapon, mennyi ideig tárolja a személyes adatokat, kivel osztja meg a személyes adatokat, és tájékoztatnia kell a jogairól is, beleértve a felügyeleti hatóságnál – a személyes adatok védelméért felelős hivatalnál – történő panasztétel jogát is.

XV. A MUNKAVÁLLALÓ JOGAI

A munkavállalónak joga van az alábbiakra:

a) **a személyes adataihoz** és **a következő információkhoz való hozzáférés** (**a GDPR 15. cikke szerint**)

- az adatkezelés célja
- az érintett személyes adatok kategóriái
- a címzettek vagy a címzettek kategóriái, akikkel a személyes adatokat közölték vagy közölni fogják
- a személyes adatok tárolásának tervezett időtartama
- az adatkezelőtől a személyes adatok helyesbítését vagy törlését kérő jog fennállása
- a feldolgozás elleni tiltakozás
- a felügyeleti hatóságnál történő panasztétel joga
- a személyes adatok forrására vonatkozó minden rendelkezésre álló információ, kivéve, ha azt az érintettől szerezték be
- az automatizált döntéshozatal keretében az alkalmazott eljárásra vonatkozó érdemi információk megszerzéséhez
- a feldolgozott személyes adatok másolatának átadásához való jog

b) a személyes adatok helyesbítéséhez való jog (a GDPR 16. cikke alapján)

- az adatkezelőnek indokolatlan késedelem nélkül helyesbítenie kell a pontatlan személyes adatokat

c) a törléshez való jog („a személyes adatok tárolásának megszüntetéséhez való jog", a GDPR 17. cikke szerint)

- a személyes adatokra már nincs szükség azokhoz a célokhoz, amelyek érdekében azokat kezelték
- a hozzájárulás visszavonásához való jog, amely alapján az adatokat kezelték, és az adatkezelésnek nincs további jogalapja
- az érintett tiltakozik az adatkezelés ellen
- a személyes adatokat jogellenesen dolgozták fel
- a törléshez való jog nem kizárólagos, csak az esetek korlátozott körében gyakorolható, nem alkalmazható például az adatkezelő szakmai és jogi kötelezettségeinek teljesítése során, és ha az adatkezelés szükséges

d) az adatkezelés korlátozásához való jog (a GDPR 18. cikke szerint)

- az érintett tagadja a személyes adatok pontosságát
- az adatkezelés jogellenes
- az adatkezelőnek már nincs szüksége a személyes adatokra az adatkezelés céljából
- az érintett tiltakozik az adatkezelés ellen
- a személyes adatok feldolgozásának korlátozása a tiltakozás időtartamára

e) a személyes adatok helyesbítésére vagy törlésére, illetve az adatkezelés korlátozására vonatkozó **értesítési kötelezettség** (**a GDPR 19. cikke szerint**)

f) az adatkezelő által kezelt **adatok hordozhatóságához való jog** (**a GDPR 20. cikke szerint**)

g) a személyes adatok kezelése elleni **tiltakozás** (**a GDPR 21. cikke szerint**)
   - az érintett tiltakozhat az adatkezelés ellen, ha egyéni helyzet vagy közvetlen üzletszerzés miatt jogos érdeke fűződik hozzá. Az adatkezelőnek bizonyítania kell, hogy e tevékenységeket jogos okból végzi

h) **az automatizált döntés felülvizsgálatához való jog** (**a GDPR 22. cikke alapján**)
   - az érintettnek joga van ahhoz, hogy a döntést ne kizárólag automatizált gép hozza meg, kérheti emberi döntés meghozatalát

i) **a hatékony jogvédelemre való jog**, az érintett bírósághoz fordulhat az adatkezelővel folytatott jogvita esetén

XVI. PANASZBENYÚJTÁSI JOG

Ha az érintett úgy véli, hogy megsértették a személyes adatok kezelésére vonatkozó jogszabályokból eredő kötelezettségeket, joga van panaszt tenni a felügyeleti hatóságnál, amely a Személyes adatok védelmével foglalkozó hivatal, székhelye: Pplk. Sochor 27, 170 00 Praha 7 - Holešovice, tel. 234 665 111, weboldal: https://www.uoou.cz/, http://www.uoou.cz/vagy a bírósághoz fordulhat, illetve kapcsolatba léphet velünk adatvédelmi tisztviselőnkön, Karel Knotek úron keresztül a gdpr@hopi.cz e-mail címen vagy a +420 604 295 011-es telefonszámon.

XVII. A MUNKAVÁLLALÓK KÖTELEZETTSÉGEI A SZEMÉLYES ADATOK KEZELÉSE SORÁN

a) Minden munkavállaló köteles biztosítani, hogy a személyes adatok ne kerüljenek illetéktelen címzettek tudomására, és köteles bizalmasan kezelni minden olyan érintett személyes adatait, akivel munkája során kapcsolatba kerül.

b) Minden munkavállalónak haladéktalanul, de legkésőbb 24 órával azután, hogy tudomást szerzett a személyes adatok megsértéséről, jelentenie kell azt felettesének vagy az adatvédelmi tisztviselőnek.

c) A munkavállaló a munkáltató utasítására az érintettek személyes adatait csak jogszerűen, tisztességesen, átlátható módon, az érintett által megadott cél érdekében, a szükséges legkisebb mértékben, pontosan, az adatkezelés céljához szükségesnél nem hosszabb ideig, valamint a személyes adatok megfelelő biztonságát, beleértve azok védelmét is, biztosító módon kezeli.

d) A munkavállaló köteles megőrizni a munkáltató számítógépes rendszereihez való hozzáférési adatainak és jelszavainak titkosságát. A munkavállaló köteles a személyes adatokat tartalmazó irathordozókat (dokumentumokat) megfelelően biztosítani a jogosulatlan hozzáférés, sérülés, visszaélés vagy elvesztés ellen, amikor nem dolgozik velük. A munkavállaló köteles kijelentkezni

a számítógépes rendszerből (lezárni azt), amikor távol van a munkáltató számítógépétől, amelyen dolgozik, és köteles a rábízott technológiát illetéktelen hozzáférés ellen biztosítani.

e) Amennyiben a személyes adatok kezelése az érintett hozzájárulásán alapul, a hozzájárulást írásban kell megadni, és azt papíron vagy elektronikus formában kell tárolni annak érdekében, hogy igazolható legyen. A hozzájárulást elkészítő munkavállalónak a jelen belső irányelvhez csatolt hozzájárulást kell alapértelmezett mintaként használnia, és minden esetben tájékoztatnia kell az érintettet arról, hogy a hozzájárulás visszavonható a munkáltató hivatalos postázási e-mail címére vagy postai címére küldött kérelemmel.

f) Amennyiben a munkavállaló 18 év alatti érintett személyes adatait kezeli olyan esetekben, amikor az adatkezelést nem jogszabályi kötelezettség írja elő, azt a törvényes képviselő – az érintett szülője – hozzájárulásával és jóváhagyásával köteles megtenni. A munkavállalónak észszerű erőfeszítéseket kell tennie annak ellenőrzésére, hogy a hozzájárulást valóban a szülő adta-e meg.

g) Tilos a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személy egyedi azonosítására szolgáló biometrikus adatok, továbbá a természetes személy egészségi állapotára, szexuális életére vagy szexuális irányultságára vonatkozó adatok kezelése, kivéve, ha a személyzeti ügyek kezelése vagy az alkalmazandó jog által előírt feladatok ellátásához szükséges feladatok elvégzése érdekében törvényben meghatározott kivételek állnak fenn.
h) Az adatminimalizálás elve tekintetében fontos szem előtt tartani a szervezet azon kötelezettségét, hogy nem kezelhet olyan személyes adatokat, amelyekre nincs szüksége, vagy amelyek nem megfelelőek a célnak megfelelő formában.
i) A személyazonosító igazolványokról szóló 328/1999. sz. törvény a 15a. szakasz rendelkezéseiben korlátozza a személyazonosító igazolványok kezelését. Ez a rendelkezés kimondja, hogy a személyazonosító igazolványról tilos bármilyen módon másolatot készíteni annak a polgárnak az igazolható hozzájárulása nélkül, akinek a személyazonosító igazolványt kiállították, kivéve, ha külön törvény vagy olyan nemzetközi szerződés, amelyhez a Cseh Köztársaságot köti, másként rendelkezik.
j) Az álláshelyekre sikertelenül pályázók személyes adatainak kezelése (ez magában foglalja az önéletrajzban, a kísérőlevélben és esetleg a szóbeli kiválasztási forduló egyes feljegyzéseiben szereplő információkat) a munkáltató mint adatkezelő jogos érdeke alapján történik (azaz a GDPR 6. cikke (1) bekezdésének f) pontja szerint). Azt azonban, hogy az ilyen adatokat mennyi ideig őrzik meg a szervezetben, belső szervezeti szabályzatban kell szabályozni. Ugyanakkor az adatkezelőnek tájékoztatási kötelezettsége is van az álláspályázókkal szemben (akik szintén érintettek).

XVIII. A GDPR-NEK VALÓ MEGFELELÉS BELSŐ ELLENŐRZÉSI FOLYAMATAI

Az elsődleges ellenőrzési folyamat az összes tevékenység ISO 9001 szerinti éves belső ellenőrzésének elvégzése. Az audit magában foglalja a következőket:

- A belső szabályzatok érvényességének megerősítése és a szabályzatok felülvizsgálata
- A személyes adatokat kezelő kiválasztott felhasználók munkájának szúrópróbaszerű ellenőrzése az egyes ellenőrzött helyszíneken az ellenőrzési lista kérdései keretében
- Az informatikai folyamatok felülvizsgálata a személyes adatok GDPR-nak megfelelő védelme biztosításának érdekében
- A személyes adatok kezelésére használt alkalmazások ellenőrzése

XIX. A KAPCSOLÓDÓ ADATVÉDELMI DOKUMENTÁCIÓ

- A HOPI HOLDING a.s. belső irányelvei Kiberbiztonság
- IKT magatartási kódex
- A munkavállalók tájékoztatása a személyes adatok kezeléséről
- Az álláshelyekre pályázók tájékoztatása a személyes adatok kezeléséről
- A GDPR bemutatása az e-learning platformon
- Megállapodás a titoktartásról, az információk védelméről és a visszaélés tilalmáról
- Tájékoztatás a személyes adatok kezeléséről a telephelyre látogatók számára
- A munkavállaló hozzájárulása a személyes adatok kezeléséhez a HOPI intranetes információs portálon
- A munkavállaló hozzájárulása a személyes adatok kezeléséhez a HOPI LinkedIn szakmai hálózaton történő bemutatkozásával összefüggésben