Biztonsági projekt a személyes adatok védelméről

TARTALOM

I. CÉL ÉS CÉLKITŰZÉS

Az irányelv rögzíti a személyes adatok kezelésének szabályait. A cél a védelem biztosítása

személyes adatok kézi és automatizált feldolgozás során.

II. ÉRVÉNYESSÉG HATÁLYA

Az irányelv a vállalat minden alkalmazottjára vonatkozik. Mindenki számára kötelező érvényű kötelezettségeket ír elő a személyes adatokat feldolgozó felhatalmazott személyek és a megfelelést felügyelő felelős személyek törvényi rendelkezések a személyes adatok kezelésében. Az irányelv megsértése a munkafegyelem súlyos megsértésének minősül.

III. FOGALMAK MEGHATÁROZÁSA

Személyes adat - azonosított vagy azonosítható természetes személyre vonatkozó adat, amely olyan személy, aki közvetlenül vagy közvetve azonosítható, különösen egy általánosan alkalmazandó

azonosító, vagy egy vagy több olyan jellemző vagy tulajdonság alapján, amelyek a fizikai, fiziológiai, pszichológiai, mentális, gazdasági, kulturális vagy társadalmi identitását azonosítják.

Személyes adatok feldolgozása - a személyes adatokon végzett bármely művelet vagy műveletsorozat végrehajtása pl. az adatok megszerzése, gyűjtése, rögzítése, rendszerezése, feldolgozása, vagy megváltoztatása, visszakeresés, konzultáció, konzultáció, átrendezés, kombináció, áthelyezés, használat, megőrzés, megsemmisítés, továbbítás, rendelkezésre bocsátás, hozzáférhetővé tétel vagy nyilvánosságra hozatal.

Üzemeltető – ParkettWorld Kft., 2045 Törökbálint, Nádasdy Tamás u. 2

Felhatalmazott személy - minden olyan természetes személy, aki személyes adatokkal kerül kapcsolatba a munkaviszonya következtében.

Felelős személy – az információs rendszer üzemeltetője által a felügyelettel megbízott személy írásban felhatalmazást kapott arra, hogy a személyes adatok kezelése során felügyelje a jogszabályi rendelkezések betartását.

Érintett személy – minden természetes személy, akiről személyes adatot kezelnek, alkalmazottak, állásra jelentkezők, ügyfelek

Információs rendszer - bármely szervezett fájl, rendszer vagy adatbázis, amely egy ill.több személyes adatot tartalmaz, amelyeket szisztematikusan dolgozunk fel a cél elérésének szükségletei szerint speciális kritériumok és feltételek segítségével, automatizált, félautomata ill. az automatizált feldolgozási eszközökön kívüli eszközök segítségével, függetlenül attól, hogy központosított, decentralizált, funkcionális vagy földrajzi alapon elosztott rendszerről van-e szó, pl.akták, listák, nyilvántartások, felvételek, vagy dokumentumokat, szerződéseket, nyilvántartásokat, aktákat, igazolásokat, tanulmányokat, értékeléseket, teszteket tartalmazó rendszer.

Automatizált információs rendszer - (a továbbiakban: AIR) a számítástechnikai eszközök összessége, szoftver és alkalmazási berendezések, adatbázis, adatokat tartalmazó adathordozók,telepítő eszközök, az automatizált adatfeldolgozáshoz szükséges műszaki és szoftveres berendezésekhez kapcsolódó dokumentáció.

Felhasználói fiók - a felhasználó azonosítására szolgál az automatizált információs rendszerben, lehetővé teszi a kijelölt felhasználói jogok helyes hozzárendelését a bejelentkezett felhasználóhoz, a következőkből áll fióknév és jelszó.

Jogosult felhasználó – az a munkavállaló, akinek felhasználói fiókot hoztak létre, és hozzárendelték a megfelelőt hozzáférési jogokat, amelyek lehetővé teszik számára munkafeladatainak ellátását.

Munkadokumentumok - minden olyan fájl, amelyet az automatizált információs rendszer felhasználói a cég szükségleteire hoztak létre vagy vettek át.

A személyes adatok megsemmisítése - a személyes adatok megsemmisítése szétválasztással, törléssel vagy az adathordozók fizikai megsemmisítésével, hogy azokról személyes adatok ne legyenek reprodukálhatóak.

Biztonsági intézkedés - gyakorlat, munkafolyamat vagy eszköz, amely csökkenti a kockázatot.

Rendkívüli állapot – olyan esemény, amelynek fennmaradása vagy megismétlődése érdekveszélyt jelenthet az üzemeltető számára.

IV. BIZTONSÁGI INTÉZKEDÉSEK ÉS ALKALMAZÁSUK

A végrehajtott alapvető biztonsági intézkedések a következők:

1 · a helyiségek védelme és a személyek belépésének ellenőrzése,

2 · kötelező azonosítás és hitelesítés az AIR-hez való hozzáféréskor,

3 · biztonsági mentés és vírusvédelem,

4 · a helyiseégek zárása

A biztonsági intézkedések a személyek fizikai belépésének korlátozására és ellenőrzésére, az elektronikus formában tárolt személyes adatokhoz való logikai hozzáférés korlátozására, a védett személyes adatok bizalmas kezelésére és a rendelkezésre állására szolgálnak.

A szervezet minden alkalmazottja köteles:

1 · betartani az épület, a személyes adatok, és a személyes javak védelme érdekében végrehajtott biztonsági intézkedéseket

2 · betartani a belső irányelveket és előírásokat,

3 · az információs rendszerből származó információ kiszivárgása vagy annak gyanúja esetén a felelős személynek jelenteni azt.

V. AZ ENGEDÉLYEZÉS HATÁLYA ÉS A JOGOSULT SZEMÉLYEK ENGEDÉLYEZETT TEVÉKENYSÉGÉNEK LEÍRÁSA

A jogosult személyek közé tartozik:

1 · könyvelő,

2 · igazgató.

Minden olyan személyt, akinek feladata a személyes adatok feldolgozása - felhatalmazott személyek - ki kell oktatni a személyes adatok védelméről szóló 428/2002. sz. törvényből eredő kötelezettségekről. Az oktatásról írásos jegyzőkönyvet kell vezetni.

A személyes adatok a szervezet céljaira kizárólag az érvényben lévő törvények, törvényes előírások és a belső szabályzat alapján lehet felhasználni.

Csak olyan típusú személyes adatok kerülnek feldolgozásra, amelyeknek a kezelése szükséges.

A személyes adatok likvidálását az arra jogosult személy csak a felelős hozzájárulása alapján végezheti.

A munkahely ideiglenes elhagyásakor minden dolgozónak ki kell jelentkeznie a személyes adatokat kezelő programokból, esetleg képernyővédő használata beállított jelszóval, a személyes adatokat tartalmazó írásos dokumentumokat eltenni és elzárni.

V.1. A személyzeti és bérszámfejtési napirend feldolgozásának munkafolyamata

A számvitelért felelős tisztviselő jogosult a munkavállalók és családtagjaik személyes adatainak beszerzésére, manuálisan és elektronikus formában is feldolgozza, betekintést nyerhet, rendszerezheti és felhasználhatja azokat a személyzeti és bérszámfejtési dokumentumok elkészítéséhez, személyes adatokat tartalmazó dokumentumok javítására, módosítására, tárolására.

Hivatalos dokumentumokról másolat csak az érintett személy írásbeli hozzájárulásával készíthető.

A beleegyezésnek tartalmaznia kell, hogy ki adta a beleegyezést, kinek adta a beleegyezést, milyen célból, a személyes adatok listáját, vagy tartalmát, a hozzájárulás érvényességi idejét és a visszavonás feltételeit.

A postai úton érkező álláspályázatok esetében a jelentkező felé írásban kell jelezni, hogy pályázata meddig lesz nyilvántartásba véve, majd törölve. Ugyanakkor a jelentkezőt fel kell kérni, hogy a személyes adataiban bekövetkezett változásokat az említett időpontig küldje el.

Ha a pályázat tárgytalan, a pályázó nem alkalmas, akkor írásban kell értesíteni a jelentkezőt a pályázata és azon feltüntetett személyes adatok törléséről. Hivatalos dokumentumokat, vagy azok másolatát amelyek személyes adatokat tartalmaznak vissza kell juttatni a feladónak.

Más személyre vonatkozó személyes adatok telefonon történő átadása és hozzáférhetővé tétele tilos. A meghatalmazott személyek telefonon megerősíthetik, hogy az adott személy a szervezet alkalmazásában áll-e, további adatok megadása nélkül.

Betegségi igazolást csak az arra képzett személy vehet át.

V.2. Azonosítási és hitelesítési módszer

Minden meghatalmazott személynek az információs rendszerbe való belépéskor névvel és jelszóval kell bejelentkeznie.

A jelszónak legalább 6 karaktert kell tartalmaznia. A jelszót alkotó karakterkombináció nem lehet könnyen megfejthető, hálózati felhasználó nevek, a felhasználók és családtagjainak vezeték és keresztneveinek, születési dátumainak, stb. használata tilos.

Kis- és nagybetűk számokkal és speciális karakterekkel "%, /, #,@, &, $, (, …, való kombinációja ajánlott diakritikus jelek használata nélkül. A jelszavakat rendszeresen 45-60 naponta cserélni kell - a jelszavakat a lejárati idő után nem szabad megismételni.

A jelszó bizalmas kezeléséért a felhasználó felelős. A jelszavak nem lehetnek szabadon elérhetőek, pl. a számítógép mellett, billentyűzet alatt, asztalon stb.

A felhasználó felelős a jelszavának más személy számára történő jogosulatlan felfedéséért, és következésképpen az általa okozott visszaélésszerű használatért és az okozott károkért.

V.3 Az automatizált információs rendszer felhasználóinak kötelezettségei

Az automatizált információs rendszer a szervezet tevékenységével kapcsolatos munkák elvégzésére szolgál, ill. csak erre a célra használható. Az AIR-t nem szabad magáncélra vagy olyan célokra használni amelyek nem kapcsolódnak a szervezet tevékenységéhez.

Az AIR alapvető eszközei, amelyek meghatározott munkák elvégzésére használhatóak a következők:

1 · számítógép, amelyet a jogosult felhasználó használhat,

2 · telepített szoftver,

3 · adatszerver hálózati szolgáltatásai,

4 · számítógépes rendszerek számítási kapacitása vállalati hálózati alkalmazások használatakor.

A felhasználó nem telepíthet maga semmilyen programot, nem használhat és terjeszthet illegális szoftvert, nem másolhat és terjeszthet telepített programokat és operációs rendszereket, azok részeit, kapcsolódó dokumentációkat és használati útmutatókat.

A számítógép és egyéb műszaki berendezések konfigurációjában minden változtatás csak az AIR rendszergazdái végezhetnek el.

A felhasználó semmilyen módon nem kísérelheti meg hozzáférési jogok, vagy kiváltságos állapot megszerzését, amelyet nem az AIR - rendszergazda állított be számára. Ha a felhasználó a program vagy technikai eszköz hibája miatt olyan kiemelt státuszba kerül, amelyet nem kapott, vagy olyan hozzáférési jogokkal rendelkezik amelyek számára nem voltak kiosztva és beállítva, haladéktalanul köteles értesítenie a felelős személyt és az AIR - adminisztrátort. A felhasználó nem végezhet olyan tevékenységet, amely megakadályozza a többi felhasználót az AIR megfelelő használatában.

A felhasználó köteles tiszteletben tartani és fenntartani a számítógépén és a hálózaton lévő könyvtárak szerkezetét, rendet tartani a könyvtárakban, törölni a felesleges fájlokat ezekből a könyvtárakból, nem hozhat létre üres könyvtárakat, kaotikus másolatokat és így tovább.

VI. FELELŐSSÉGI KÖR

VI.1. A meghatalmazott személyek felelőssége

Minden meghatalmazott személy köteles megőrizni a vele kapcsolatba kerülő személyes adatok titkosságát. Nem használhatja fel saját személyes használatra, nem hozhatja azokat nyilvánosságra, és nem teheti hozzáférhetővé senki számára.

A titoktartási kötelezettség a munkaviszony megszűnése után is fennáll.

VI.2 A felelős személy felelőssége

A személyes adatok kezelése során a jogszabályi rendelkezések betartását egy

írásban meghatalmazott, szakmailag képzett felelős személy felügyeli. Szakmai képzés terjedelme

elsősorban a személyes adatok védelméről szóló törvény és a személyes adatokról szóló nemzetközi szerződések tartalmának felel meg. A szakmai képzést végzett személy írásbeli igazolást kap a végzettségről.

A személyes adatok kezelésének megkezdése előtt a felelős személy felméri, hogy azok feldolgozása során fennál-e az érintett személyek jogának és szabadságának megsértésének veszélye.

Az érintett személyek személyes adatainak kezelése előtt észlelt, vagy az adatkezelés során észlelt törvényi előírások megsértéséről a felelős személy az üzemeltetőt haladéktalanul írásban értesíti. Ha az üzemeltető az értesítést követően nem orvosolja haladéktalanul a helyzetet, a felelős személy értesíti a Nemzeti Adatvédelmi és Információszabadság Hatóságot.

A felelős személy biztosítja:

- a szükséges együttműködést a Nemzeti Adatvédelmi és Információszabadság Hatóságával,

- az üzemeltetői alapfeladatok teljesítésének felügyelete

- az adatkezelés megkezdése előtt egyértelműen és konkrétan meghatározza az adatkezelés célját,

- meghatározni az adatkezelés módját, a személyes adatok beszerzése kizárólag meghatározott célból,

- biztosítja, hogy csak olyan személyes adatokat dolgozzanak fel, amelyek terjedelme és tartalma megfelelő és szükségesek az adatkezelés céljának eléréséhez,

- a különböző célokra szükséges személyes adatok gyűjtése külön-külön,

- a különböző célokra gyűjtött személyes adatokat nem szabad összesíteni,

- csak helyes, teljes és naprakész személyes adatokat dolgozzon fel,

- a helytelen és hiányos személyes adatok zárolása, helyesbítése vagy kiegészítése,

- törli a nem helyesbíthető vagy kiegészíthető adatokat,

- biztosítja, hogy a személyes adatok feldolgozása, amely lehetővé teszi az érintettek azonosítását legfeljebb az adatkezelés céljának eléréséhez szükséges ideig történjen,

- törli azokat a személyes adatokat, amelyek feldolgozásának célja megszűnt,

- a személyes adatokat a jó erkölcsnek megfelelően dolgozza fel,

- nem kényszerítheti ki az érintett hozzájárulását azzal fenyegetve, hogy megtagadja a szerződéses kapcsolatot, a szolgáltatások nyújtását vagy termékek átadását,

- a meghatalmazott személyeket a 17. cikk szerint utasítja,

- az érintettek kérelmeinek 30 napon belüli kezelése

- általánosan közérthető formában tájékoztatást adni a személyes adatok kezelésének állásáról

a köv. terjedelemben: az üzemeltető neve, székhelye vagy állandó lakóhelye, jogi formája és azonosító száma; az üzemeltető törvényi meghatalmazottjának és felelős személy vezetékneve; az információs rendszer azonosító jele; az adatkezelés célja, a személyes adatok listája és az érintettek listája; címzettek köre, akik hozzáférnek, vagy hozzá fognak férni az adatokhoz, harmadik felek, akiknek a személyes adatot megkapják vagy fogják kapni; harmadik országok, amelyekbe a személyes adatokat továbbítják; az információs rendszer jogalapja; a közzététel formája, ha a személyes adatok közzétételére sor kerül; a személyes adatok védelmét biztosító intézkedések általános jellemzői és az adatkezelés megkezdésének időpontja,

- általánosan érthető formában pontos tájékoztatást adni arról, hogy a személyes adatokat milyen forrásból szerezték be,

- a személyes adatok általánosan érthető formában történő leírása,

- a helytelen, hiányos vagy elavult személyes adatok javítása,

- a személyes adatok megsemmisítése az adatkezelés céljának teljesülése után; a hivatalos dokumentumok visszaszolgáltatása amennyiben azok a feldolgozás tárgyai voltak

- törvénysértés esetén a személyes adatok megsemmisítése,

- az érintett személy és a Nemzeti Adatvédelmi és Információszabadság Hatóságának azonnali értesítése, hogy a meghatalmazott személy írásos kérvénye alapján amelynek korlátozva voltak a jogai, a helytelen, hiányos és nem aktuális adatai ki lettek javítva, esetleg törölve, és amennyiben a feldolgozás tárgya személyes adatokat tartalmazó hivatalos igazolványok voltak, azok vissza lettek neki adva.

- az érintettek kifogásainak 30 napon belüli ügyintézése az alábbiak esetében

- a személyes adatai direkt marketing célokra kerültek felhasználása az engedélye nélküli

- a személyes adatok direkt marketing célú felhasználása a postai kommunikációban,

- személyes adatok direkt marketing célú szolgáltatása,

- technikai, személyi és szervezési intézkedések végrehajtása és gyakorlati alkalmazásuk felügyelete,

- felügyelet a közvetítő kiválasztása során, valamint írásbeli szerződés vagy közvetítői meghatalmazás elkészítése; ellenőrzi a megállapodás szerinti feltételek betartását,

- a személyes adatok határokon átnyúló áramlásának felügyelete,

- az információs rendszerek bejelentése speciális regisztrációra, változás bejelentéshez és kijelentkezéshez; előírt nyilvántartást vezet a nem regisztrációköteles információs rendszerekről.

A felelős a feldolgozás módjának megfelelő technikai, szervezési és személyi biztonsági intézkedéseket javasol. A felhatalmazott személyekkel együttműködve javasolja a szoftverek és a nyomtatott űrlapok módosítását a vonatkozó törvények és rendeletek változásai alapján, hogy csak azok a típusú személyes adatok kerüljenek feldolgozásra, amelyek feltétlenül szükségesek.

VII. ELLENŐRZŐ TEVÉKENYSÉG

A felelős az érintettek jogai és szabadságai megsértésének észlelése alapján, de évente legalább egy alkalommal a személyes adatok védelmének betartására irányuló vizsgálatot végez az érintett információs rendszerekben.

A felelős személy ellenőrzi:

1 · írásos dokumentumok archiválása – az archiválás feltételeinek megfelelősége,

2 · az AIR rendszergazdával együttműködve a biztonsági mentések működőképességének és teljességének ellenőrzése,

3 · belső szabályzat – a munkafolyamatok pontossága és egyértelműsége a személyes adatok feldolgozásakor.

VIII. VÉSZHELYZETI ELJÁRÁS

Bármely AIR eszköz meghibásodása esetén erről értesíteni kell az AIR rendszergazdát. A meghibásodás elhárításának menetéről az AIS adminisztrátor dönt, a személyes adatok biztonsága érdekében tájékoztatja a felelőst, ha a személyes adatokat tartalmazó műszaki eszközt vagy információhordozót a szervezet telephelyén kívülre szállítanák szervízbeavatkozás céljából, vagy ha a szervízbeavatkozást külső cég végzi.

A tüzek megelőzése érdekében a tűzvédelmi szabályzatnak megfelelő intézkedéseket be kell tartani. Tűz esetén a riasztási és evakuálási irányelvek szerint kell eljárni, amelyek a tűzvédelmi szabályzat részét képezik.

JUDr. Michal Zima

ügyvezető