

90...../2017. számú ügyvezetői utasítás/Order of the Managing Director No. 90...../2017.

1. A Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Korlátolt Felelősségű Társaság (a továbbiakban: Társaság) adatvédelemre és adatbiztonságra vonatkozó szabályzatát jelen ügyvezetői utasítás 1. számú mellékleteként magyar nyelven, 2. számú mellékleteként angol nyelven kiadom./ I hereby publish the Bylaw on data protection and data security of Széchenyi Programme Office Consulting And Service Nonprofit Limited Liability Company in Hungarian version as Annex no. 1. and in English version as Annex no. 2. of the present Managing Director's order.
2. Jelen ügyvezetői utasítás 2017. 11. 17. napján lép hatályba./The present managing director's order shall enter into force on 17. 11. 2017.
3. Jelen ügyvezetői utasítás hatályba lépésével egyidejűleg a 28/2017. számú ügyvezetői utasítással kiadott Adatvédelmi Szabályzat hatályát veszti./When the present managing director's order enters into force, the Bylaws on data protection and data security by managing director's order no. 28/2017 cease to have effect.

Budapest, 2017. 11. 17. / 17. 11. 2017.

Széchenyi Programiroda  
Tanácsadó és Szolgáltató Nonprofit  
Korlátolt Felelősségű Társaság  
Adószám: 18080313-2-41  
Tel.: 327-08-30, fax: 327-08-33  
1053 Budapest, Szép utca 2. IV. emelet  
1.

Schultz Gábor/Gabor Schultz  
ügyvezető/managing director








1. számú melléklet a 90/2017. számú ügyvezetői utasításhoz

## ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

CÉGNÉV:	SZÉCHENYI PROGRAMIRODA NONPROFIT KFT.
SZÉKHELY:	1053 Budapest, Szép utca 2. IV. emelet
ADÓSZÁM:	18080313-2-41
CÉGJEGYZÉKSZÁM:	01-09-916-308
a továbbiakban:	Társaság

Jelen Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) tartalmazza a Társaság belső adatkezelési folyamatai nyilvántartásának szabályait és az érintettek jogainak biztosítását szolgáló garanciális szabályokat.

A Szabályzat a Társaság valamennyi munkavállalója és szervezeti egysége számára kötelező érvényű.

Készítette: dr. Vigh Péter	Ellenőrizte: dr. Kongorác László	Jóváhagyta: Hajasné dr. Kurka Csilla
		
A munka törvénykönyvéről szóló 2012. évi I. törvény 17. § (2) bekezdése alapján a munkáltatói szabályzatot közzé kell tekinteni, ha azt a helyben szokásos és általában ismert módon közzé teszik.		

## Tartalom

I. Bevezető .....	3
II. A szabályzat célja és hatálya.....	3
III. A szabályozás során felhasznált jogszabályok és rövidítései.....	3
IV. Értelmező rendelkezések.....	3
V. Az adatkezelés általános szabályai.....	5
VI. A Társaság adatvédelmi rendszere.....	6
VII. Felelősségi körök.....	6
VIII. Adatbiztonsági szabályok .....	7
IX. Az érintettek jogainak érvényesítése.....	8
X. A Társaságnál megvalósuló adatkezelések.....	9
1. A Monitoring Rendszer (MR) használatával összefüggő adatkezelés .....	9
2. Hírlevél szolgáltatással összefüggő adatkezelés .....	10
3. Személyügyi adatkezelés .....	10
3.1. Munkavállalók munkaviszonnyal összefüggő adatkezelése .....	10
3.2. Munkavállalók ellenőrzésével összefüggő adatkezelés .....	11
3.3. Munkára jelentkezők adatkezelése.....	12
1. sz. melléklet.....	14
<b>Titoktartási nyilatkozat</b> .....	14
2. sz. melléklet.....	15
<b>Adatvédelmi tájékoztató és nyilatkozat</b> .....	15
3. sz. melléklet.....	16
<b>Tájékoztató elektronikus rendszerek használatával összefüggő adatkezelésről</b> .....	16
4. sz. melléklet.....	17
<b>Válaszlevél bepörlő önéletrajzokra</b> .....	17



## I. Bevezető

A Társaság a belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából jelen Szabályzatot alkotja. Jelen rendelkezéseket a Társaság többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és bármely más, jelen Szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadóak.

## II. A szabályzat célja és hatálya

1. A Társaság a Szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 15. §-ában meghatározott tájékoztatáshoz való jog megvalósulását.

2. Jelen Szabályzat célja, hogy az érintettek megfelelő tájékoztatást kaphassanak a Társaság által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevééről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

3. A Szabályzattal a Társaság biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, és azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

4. A Szabályzat tárgyi hatálya kiterjed a Társaság valamennyi szervezeti egységénél folytatott valamennyi folyamatra, amely során az Infotv. 3. § 2. pontjában meghatározott személyes adat kezelése megvalósul.

5. A Társaság a Szabályzatban nevesített adatkezelések mellett adott programhoz, illetve projekthez kapcsolódóan - az ott meghatározottak szerint - további adatkezelést folytathat, melynek program- vagy projektspecifikus részletei a Társaság, illetve az adott projekt vagy program honlapján kerülnek közzétételre. A Szabályzat rendelkezései ezen további adatkezelésekre is irányadóak.

## III. A szabályozás során felhasznált jogszabályok és rövidítéseik

Infotv. az információs önrendelkezési jogról és az információszabadságról szóló 2011. CXII. törvény

Mt. a munka törvénykönyvéről szóló 2012. évi I. törvény

Szja tv. személyi jövedelemadóról szóló 1995. évi CXVII. törvény

## IV. Értelmező rendelkezések

A jelen Szabályzat fogalmi rendszere megfelel az Infotv. 3. §-ban meghatározott értelmező fogalommagyarázatoknak, így különösen:

1. Érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

**2. Személyes adat:** bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet;

**3. Különleges adat:**

- a) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviselői szervezeti tagságra,
- b) az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat;

**4. Bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

**5. Hozzájárulás:** az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

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

**7. Adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely a személyes adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;

**8. Adatkezelés:** az alkalmazott eljárástól függetlenül a személyes adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérynymat, DNS-minta, íriszkép) rögzítése is;

**9. Adattovábbítás:** ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik; - Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

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

**11. Adatzárolás:** az adatok továbbításának, megismerésének, nyilvánosságra hozatalának, átalakításának, megváltoztatásának, megsemmisítésének, törlésének, összekapcsolásának vagy összehangolásának és felhasználásának véglegesen vagy meghatározott időre történő lehetetlenné tétele;

**12. Adatmegsemmisítés:** az adatok vagy az azokat tartalmazó adathordozó teljes fizikai megsemmisítése;

**13.** 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 adaton végzik;

**14.** Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi;

**15.** Adatállomány: az egy nyilvántartó rendszerben kezelt adatok összessége;

**16.** Hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság;

**17.** Személyesadat-nyilvántartó rendszer (nyilvántartó rendszer): személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórótt állománya, amely meghatározott ismérvek alapján hozzáférhető;

Amennyiben a mindenkori hatályos adatvédelmi jogszabály (jelen Szabályzat megalkotásakor az Infotv.) fogalommagyarázatai eltérnek jelen Szabályzat fogalommagyarázataitól, akkor a jogszabály által meghatározott fogalmak az irányadóak.

## **V. Az adatkezelés általános szabályai**

A Társaság eljárásai során csak és kizárólag a hatályos jogszabályok rendelkezéseinek megfelelően végez adatkezelést, így különösen:

**1.** A Társaságnál személyes adat kezelésére csak jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség. A Társaság által kezelt személyes adatok magáncélra való felhasználása tilos.

**2.** Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének, amelynek értelmében

- a Társaság személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges minimális mértékben és ideig,
- az adatkezelésnek minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatok törlésre kerülnek.

**3.** A Társaság személyes adatot csak az érintett előzetes – különleges adat esetén írásbeli – hozzájárulása vagy törvény, illetve törvényi felhatalmazás alapján kezel.

**4.** A Társaság az adat felvétele előtt minden esetben közli az érintettel az adatkezelés célját, valamint az adatkezelés jogalapját.

**5.** A Társaság szervezeti egységeinél adatkezelést végző munkavállalók és eseti jelleggel a Társaság megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottjai kötelesek a megismert személyes adatokat üzleti titokként megőrizni. A személyes adatokat kezelő és azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek Titoktartási nyilatkozatot tenni (1. sz. melléklet). A Társaság adatkezelést végző munkavállalója fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a feladat- és hatáskörének gyakorlása során tudomására jutott személyes adatok jogszerű kezeléséért, a Társaság nyilvántartásaihoz rendelkezésére álló hozzáférési jogosultságok jogszerű gyakorlásáért.

6. Amennyiben a Szabályzat hatálya alatt álló személy tudomást szerez arról, hogy a Társaság által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

## VI. A Társaság adatvédelmi rendszere

1. A Társaság ügyvezetője a Társaság sajátosságainak figyelembe vételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személyt.

2. A Társaság adatvédelmi rendszerének felügyeletét az ügyvezető látja el az általa kijelölt belső adatvédelmi felelős útján. A Társaságbelső adatvédelmi felelőse a Humánerőforrás és Hálózatfejlesztési Osztály (a továbbiakban: HR) vezetője.

## VII. Felelősségi körök

### 1. Az ügyvezető az adatvédelemmel kapcsolatosan:

a) felelős az érintettek Infotv.-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;

b) felelős a Társaság által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;

c) felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;

d) felügyeli a belső adatvédelmi felelős tevékenységét;

e) vizsgálatot rendelhet el;

f) kiadja a Társaság adatvédelemmel, adatbiztonsággal kapcsolatos belső szabályait.

### 2. A belső adatvédelmi felelős az adatvédelemmel kapcsolatosan:

a) segítséget nyújt az érintett jogainak biztosításában;

b) kezdeményezi a Hatóságnál az Infotv.-ben meghatározott nyilvántartásba vételi eljárás lefolytatását;

c) minden év január 31. napjáig jelentést készít az ügyvezető részére a Társaság adatvédelmi feladatainak végrehajtásáról;

d) jogosult jelen Szabályzat betartását az egyes szervezeti egységeknél ellenőrizni;

e) vezeti az adattovábbítási nyilvántartást;

f) figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen Szabályzat módosítását;



g) közreműködik a Hatóságtól érkezett megkeresések megválaszolásában és a Hatóság által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;

h) általános állásfoglalás megadása céljából megkeresést fogalmaz meg a Hatóság felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg,

i) ellátja az ügyvezető által részére megállapított eseti feladatokat.

3. A Szabályzatban előírtak betartásáért a feladatkörében minden érintett önálló szervezeti egység vezetője felelős.

4. A Társaság munkavállalói munkájuk során kötelesek gondoskodni arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

## VIII. Adatbiztonsági szabályok

### 1. A papír alapon kezelt személyes adatok biztonsága érdekében a Társaság az alábbi intézkedéseket alkalmazza:

a) az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;

b) a dokumentumokat jól zárható, száraz, tűzvédelmi berendezéssel ellátott helyiségben helyezi el;

c) a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;

d) a Társaság adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;

e) a Társaság adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;

f) amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza a Társaság.

### 2. A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a Társaság, összhangban az Informatikai Biztonsági Szabályzat előírásaival, az alábbi intézkedéseket és garanciális elemeket alkalmazza:

a) az adatkezelés során használt személyi számítógépek és laptopok a Társaság tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír;

b) a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal, legalább felhasználói névvel és jelszóval lehet hozzáférni, a jelszavak cseréjéről a Társaság - a mindenkori Információbiztonsági szabályzat rendelkezéseivel összhangban - rendszeresen gondoskodik;

c) az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;

d) a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és kizárólag az arra kijelölt személyek férhetnek hozzá;

e) amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető; erről az adatkezelés szempontjából feladat- és hatáskörrel rendelkező legalacsonyabb szintű szervezeti egység vezetője (a továbbiakban: szervezeti egység vezető) köteles gondoskodni;

f) a hálózaton tárolt adatok biztonsága érdekében a szerveren folyamatos tükrözéssel kerül el a Társaság az adatvesztést;

g) a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez, a mentés a központi szerver teljes adatállományára vonatkozik és mágneses adathordozóra történik;

h) a lementett adatokat tároló mágneses adathordozó az erre a célra kialakított páncéldobozban tűzbiztos helyen és módon tárolt;

i) a személyes adatokat kezelő hálózaton a vírusvédelemről a Társaság folyamatosan gondoskodik;

j) a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

## **IX. Az érintettek jogainak érvényesítése**

1. Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését vagy zárolását.
2. A Társaság a beérkezett kérelmet, illetve tiltakozást köteles a beérkezéstől számított három napon belül áttenni az adatkezelés szempontjából feladat- és hatáskörrel rendelkező szervezeti egység vezetőjéhez.
3. A szervezeti egység vezetője az érintett személyes adatának kezelésével összefüggő kérelmének 2. pont szerinti áttételétől számított 3 napon belül közérthető formában választ készít elő, amelyet véleményezés céljából haladéktalanul megküld a belső adatvédelmi felelősnek.
4. A belső adatvédelmi felelős az előkészített választ haladéktalanul megvizsgálja és az általa jóváhagyott választervezetet – aláírás és az érintett részére történő megküldés céljából - azonnal továbbítja az ügyvezetőnek.
5. Az ügyvezető, mint az adatkezelő képviselője az érintett személyes adatának kezelésével összefüggő kérelmére a Társasághoz történő beérkezésétől számított legkésőbb 25 – tiltakozási jog gyakorlása esetén 15 – napon belül írásban tájékoztatja az érintettet.
6. A tájékoztatás kiterjed az Infotv. 15. § (1) bekezdésében meghatározott információkra, amennyiben az érintett tájékoztatása törvény alapján nem tagadható meg.
7. A tájékoztatás főszabály szerint ingyenes, költségtérítést a Társaság csak az Infotv.-ben meghatározott esetben számít fel.
8. A Társaság kérelmet csak az Infotv.-ben meghatározott okokból utasíthat el, erre csak indokolással, az Infotv.-ben meghatározott tájékoztatással, írásban kerülhet sor.
9. A valóságnak nem megfelelő adatot az adatot kezelő szervezeti egység vezetője – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, az Infotv. 17. § (2) bekezdésében meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törlése iránt.

10. Az érintett személyes adata kezelése elleni tiltakozásának elbírálása időtartamára – de legfeljebb 5 napra – az adatkezelést az adatkezelést végző szervezeti egység vezetője felfüggeszti, a tiltakozás megalapozottságát megvizsgálja a döntést előkészíti, melyet véleményezés céljából megküld a belső adatvédelmi felelősnek. A döntésről jelen fejezet 5. pontjában meghatározott határidők figyelembevételével a kérelmezőt az Infotv. 21. § (2) bekezdésében foglaltak szerint az adatkezelőt képviselő ügyvezető tájékoztatja.

11. Amennyiben a tiltakozás indokolt, az adatot kezelő szervezeti egység vezetője az Infotv.-ben meghatározottak szerint jár el.

12. Amennyiben az érintett jogainak gyakorlása során az ügy megítélése nem egyértelmű, az adatot kezelő szervezeti egység vezetője az ügy iratainak és az ügyre vonatkozó álláspontjának megküldésével állásfoglalást kérhet a belső adatvédelmi felelőstől, aki azt három napon belül teljesíti.

13. A Társaság az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat megtéríti. Az adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Ugyanígy nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

14. Az érintett a jogainak megsértése esetén az Infotv. alapján az illetékes bírósághoz, illetőleg a Hatósághoz fordulhat:

név: Nemzeti Adatvédelmi és Információszabadság Hatóság

székhely: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

honlap: [www.naih.hu](http://www.naih.hu)

## X. A Társaságnál megvalósuló adatkezelések

Az adatkezelés helye: 1053 Budapest, Szép utca 2.

### 1. A Monitoring Rendszer (MR) használatával összefüggő adatkezelés

A Társaság „A pályázók és kedvezményezettek kapacitásainak támogatása, segítése a projektek tervezése és végrehajtása során” című KÖFOP-3.3.3-15-2016-00001 azonosítószámú projekt (a továbbiakban: Projekt) megvalósítása során használt MR-ben személyes adatokat kezel.

Adatkezelés célja: a pályázati anyagok érdemi elbírálása, a visszatájékoztatás, Projekt végrehajtáshoz kapcsolódó feladatok szabályszerű ellátása, a Társaság Projekttel kapcsolatos jogi kötelezettségének teljesítése

Adatkezelés jogalapja: az érintett hozzájárulása {Infotv. 5. § (1) bek. a) pont}

Adatkezelés időtartama: a kezelt adatokat az érintett hozzájárulásának visszavonásáig, de legkésőbb a Projekt pénzügyi befejezését követő 5 évig szerveren megőrzik.

Kezelt adatok köre: név, cím, telefonszám, e-mail cím

Adatkezelés módja: elektronikus

## 2. Hírlevél szolgáltatással összefüggő adatkezelés

A Társaság a [www.szpi.hu](http://www.szpi.hu) honlapon (a továbbiakban: Honlap) történő hírlevél feliratkozással összefüggésben személyes adatokat kezel.

Adatkezelés célja: a Honlap szolgáltatásai igénybevételének biztosítása (tájékoztató jellegű hírlevél küldése). Az internetes kapcsolat fenntartása során a Honlap látogatója által használt böngészőprogrammal, domain névvel (URL), a látogatás időpontjával, valamint a megtekintett oldalakkal kapcsolatosan automatikusan képződnek technikai adatok a Társaság számítógépes rendszerében. Az Társaság ezeket kizárólag a Honlappal kapcsolatos elemzésre és statisztikai információk gyűjtésére használja fel.

Kezelt adatok köre: név, e-mail cím

Adatkezelés jogalapja: az érintett hozzájárulása {Infotv. 5. § (1) bek. a) pont}

Adatkezelés időtartama: az adatokat az érintett hozzájárulásának visszavonásáig, de legkésőbb a Projekt (KÖFOP-3.3.3-15-2016-00001) pénzügyi befejezését követő 5 évig szerveren megőrzik

Adatkezelés módja: elektronikus

## 3. Személyügyi adatkezelés

### 3.1. Munkavállalók munkaviszonnal összefüggő adatkezelése

Az adatok csak az Mt. szerinti adatkörben - különös tekintettel az Mt. 10-11 §-ában foglaltakra - kezelhetők.

Adatkezelés célja: munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása

Kezelt adatok köre a munkavállalók kapcsán:

viselt neve, születési neve, születési helye és ideje, fényképe, állampolgársága, törzsszáma, anyja születési neve, lakóhelyének címe, tartózkodási helye (amennyiben eltérő a lakóhelytől), magán-nyugdíjpénztári tagság ténye, belépés ideje (év, hó, nap), adóazonosító jele, társadalombiztosítási azonosító jele (TAJ szám), nyugdíjas törzsszám (nyugdíjas munkavállaló esetén), folyószámla száma, bank neve, munkaviszony kezdő napja, biztosítási jogviszony típusa, heti munkaórák száma, telefonszáma, családi állapota, végzettséget igazoló okmány másolati példánya, munka-alkalmassági egészségügyi igazolás, munkaköre, orvosi alkalmasság ténye, erkölcsi bizonyítvány eredeti példánya, az Mt. 120. § alapján járó pótszabadság igénybevételével kapcsolatos igazoló okmány fénymásolata; pótszabadság, ill. családi adókedvezmény igénybe vétele céljából munkavállaló 16. életévét be nem töltött hozzátartozójának születési helye és ideje, lakcíme, anyja neve, társadalombiztosítási azonosító jele (TAJ szám), adóazonosító jele; korábbi munkahely kilépő dokumentumai két évre visszamenőleg, főálláson kívüli munkavégzés esetén jogviszony jellege, foglalkoztató neve és székhelye, a főálláson kívüli munkahelyen teljesített átlagos munkaidő, elvégzendő tevékenység, gazdasági társaságban való részvétel ténye, részvétel minősége, kezdete, gazdasági társaság tevékenysége

Adatkezelés jogalapja: törvényi felhatalmazás [Mt. 10. § (1) és (3)] és az érintett hozzájárulása [Infotv. 5 § (1) a) és 6. § (6)];

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

Adatkezelés módja: elektronikus és papíralapú

A munkaviszony kapcsán beszerzett harmadik személy adatai a szükséges adattartamot meg nem haladóan vehetők fel és kezelhetők. (Pl. pótszabadság, családi adókedvezmény)

Munkavállalók adatkezelésére vonatkozóan adatvédelmi tájékoztató készül, melynek célja a munkavállalók előzetes tájékoztatása az adatkezelésről. (2. sz. melléklet) A tájékoztató – jelen Szabályzat hatálybalépését követően haladéktalanul – aláírásra kerül a munkavállalók által. Új munkavállaló a munkaviszony létesítésével egyidejűleg köteles az adatvédelmi tájékoztató aláírására.

A személyügyi terület adatkezelésének jogalapja esetenként más jogszabály is lehet. Az adatkezelés időtartama az adott területre vonatkozó jogszabályok által meghatározott. (Pl. Szja tv., Mt.)

A személyügyi adatkezelések körében a nem közvetlenül a munkaviszonyból eredtetett adatkezelések során minden esetben be kell szerezni az érintett kifejezett hozzájárulását, az adatkezelés céljának és várható időtartamának megjelölésével.

### **3.2. Munkavállalók ellenőrzésével összefüggő adatkezelés**

#### **3.2.1. Adatkezelés elektronikus rendszerek használatával összefüggésben**

A munkáltató ellenőrizheti a munkavállalókat a munkaviszonyból eredő kötelezettségek teljesítése céljából a munkaviszonnyal összefüggő magatartásuk körében. Az ellenőrzésre a Mt. [11. § (1)-(2)] ad jogalapot.

A Társaság a munkavállalóknak indokolt esetben, munkavégzés céljára biztosít számítógépet, e-mail címet és internet-hozzáférést. A használat szabályairól és az ellenőrzés lehetőségéről a munkavállalókat a Társaság előzetesen írásban tájékoztatja. Az írásbeli tájékoztatás jelen Szabályzat 3. számú melléklete alapján történik, melyet a Társaság megismertet a munkavállalókkal.

Mivel a Társaság tulajdonát képező személyi számítógépeket és laptopokat, céges e-mail címeket a Társaság munkavégzés céljából biztosítja, így amennyiben a munkavállaló ezen eszközökön magáncélú személyes adatait (pl.: családi fotók, telefonkönyvek, saját adatbázisok stb.) tárolja, úgy a Társaság a számítógép ellenőrzése során ezeket az adatokat is megismerheti. Ezen adatkezelés ellen kifogással nem élhet a munkavállaló, mert a nem munkavégzés céljából történő, de a Társasági eszközön való személyes adatok tárolása – ráutaló magatartással - az adatkezeléshez történő Infotv. 5. § (1) a) bekezdése szerinti érintetti hozzájárulásnak minősülnek. Erről (illetve az archiválás és a rendszergazdai tevékenység tényéről) a munkavállalókat az eszközök használata előtt írásban tájékoztatja a Társaság.

Mindazon e-mail címek, amelyekben a Társaság neve kiterjesztésként benne foglaltatik (...@.....hu), valamint, amelyek alapvető rendeltetése a Munkáltató működésével összefüggő tevékenységek ellátása (pl.: .....@vati.hu), a Társaság tulajdonát képezik. Ezen címeken a Társaság munkavállalói által folytatott levelezés munkacélú levelezésnek minősül. Az ilyen címeken folytatott levelezésbe a Társaság az Mt. 11. § (1) bekezdése alapján jogosult betekinteni. A Társaság jogosult a fent nevezett címeken folytatott levelezések meghatározott időközönkénti biztonsági mentésére, az elektronikus levelező rendszer folyamatosságának és stabilitásának érdekében adatbiztonsági okokból saját eszközein bármilyen állomány törlésére. Amennyiben a munkavállaló a fenti céges e-mail címén található leveleiben magáncélú személyes adatait, kifejezett utalás nélkül, tárolja, úgy a Társaság az e-mail cím ellenőrzése során ezeket az adatokat is megismerheti. Ezen adatkezelés ellen kifogással nem élhet a munkavállaló,

mert a nem munkavégzés céljából történő, de a társasági e-mail címen való személyes adatok tárolása – ráutaló magatartással - az adatkezeléshez történő Infotv. 5. § (1) a) bekezdése szerinti érintetti hozzájárulásnak minősülnek. A munkáltató jogosult ellenőrizni a munkahelyi postafiókot és internet használatot. Mindemellett főszabály szerint a magáncélú levelek tartalmát a munkáltató munkaviszonyból fakadó jogosultság érvényesítése során sem jogosult megismerni.

### **3.2.2. Biometrikus azonosító rendszer alkalmazásával kapcsolatos adatkezelés**

A Társaság a 1053 Budapest, Szép utca 2. szám alatti épületben az általa bérelt területeken (2., 3., 4. és 7.emeleteken)biometrikus azonosító rendszert (a továbbiakban: blokkoló rendszer) működtet a munkavállalók azonosítása, valamint a jelenlét nyilvántartása érdekében.

A blokkoló rendszer használatára az adott emelet irodáiban állandó jelleggel dolgozó munkavállalók kötelesek érkezéskor (a munkaidő kezdetekor), valamint távozáskor (a munkaidő lejártával).

A blokkoló rendszer alkalmazásának indokoltsága:

A munkáltató az európai uniós, egyéb nemzetközi, illetve hazai költségvetési források elérésével kapcsolatos programok kezelése (mint közfeladatot ellátó segítő funkció) körében olyan üzleti és gazdasági adatokat kezel, amelynek legmagasabb szintű védelme mind a pályázók üzleti érdeke, mind a forrást biztosító szervezetek által is védett nemzetgazdasági érdekek miatt elengedhetetlen a blokkoló rendszer alkalmazása, illetve másodsorban a munkavállalók munkaidőben történő rendelkezésre állásának ellenőrzése. Más, kevésbé intenzív módszerek (mint pl. jelenléti ív vagy mágneskártya) nem biztosítják, hogy a bevitt adatok valóban abban az időpontban és attól a nyilvántartásban szereplő személytől származnak, akihez a rendszer köti.

A Társaság a blokkoló rendszer alkalmazása során kiemelt figyelmet fordít a munkavállalók személyiségi jogainak tiszteletben tartására.

Adatkezelés célja: a munkavállalók Mt. 11. § (1) bekezdése szerinti ellenőrzése.

Kezelt adatok köre: az ellenőrzés során rögzített személyes adatok (ujjlenyomat barázdáinak pontjai).

Adatkezelés jogalapja: Mt. 11. § (1) bekezdése és Infotv. 5. § (1) bekezdés a) pontja.

Adattárolás határideje: kizárólag a munkaviszony fennállása alatt, a munkaviszony megszűnésével az adatok törlésre kerülnek.

Adatkezelés módja: elektronikus

### **3.2.3. Elektronikus megfigyelőrendszer alkalmazásával kapcsolatos adatkezelés**

A Társaságnál alkalmazott elektronikus megfigyelőrendszerek használatával összefüggő adatkezelés szabályait a 7/2017. számú ügyvezetői utasítással 2017. március 7. napján hatályba lépett Elektronikus megfigyelőrendszer szabályzat tartalmazza.

### **3.3. Munkára jelentkezők adatkezelése**

A Társaság a munkára jelentkezés céljából érkezett személyes adatot tartalmazó önéletrajzok (továbbiakban: CV) esetén nem tesz különbséget azok érkezésének módja között: azonos elbírálás alá esik a papíralapon és az elektronikus módon beküldött CV.

A postai úton érkező CV-k esetében, amennyiben a jelentkező a munkaerő-toborzás során meghirdetett címre, az elvárt jelöléssel küldi meg, úgy ebben az esetben a Társaság garantálja a jelen pont szerinti adatkezelést.

Amennyiben azonban nem a meghirdetetteknek megfelelő módon érkezik a papíralapú CV, úgy az iratkezelési szabályok szerint a címzettnek minősülő személy köteles arról gondoskodni, hogy a CV a HR vezetőjéhez kerüljön. Ha ez nem történik meg, úgy a Társaság az iratkezelésre vonatkozó általános szabályokat alkalmazza, függetlenül a levél tartalmától.

Nem meghirdetett álláshelyre való jelentkezés (a továbbiakban: berepülő önéletrajz) esetén a Társaság válaszlevelet küld a jelentkezőnek, amelyben tájékoztatja az adatkezelés tényéről, jogalapjáról és az adatkezelés elleni tiltakozás formáiról. A „válaszlevél berepülő önéletrajzokra” a Szabályzat 4. sz. mellékletét képezi.

### 3.3.1 A munkaerő-toborzásra vonatkozó különös szabályok

A Társaság a CV-ket főszabály szerint a későbbi felhasználás céljából tárolja – igaz ez abban az esetben is, ha a CV konkrét meghirdetett pozíció betöltése céljából érkezett. A CV-t és az azon szereplő személyes adatokat a Társaság a jelen Szabályzat alapján és az abban foglaltak szerint kezeli. A Társaság a CV megküldését hozzájárulásnak tekinti az abban foglalt személyes adatok kezelésére vonatkozóan. Amennyiben az érintett nem kívánja, hogy a későbbiekben Társaságunk jelen Szabályzatban foglaltak szerint kezelje adatait, úgy ezt vagy a CV megküldésével egyidejűleg kell jeleznie, vagy a későbbiek során visszavonni a CV beküldésével megadott hozzájárulását.

A CV alapján kiválasztott érintett adatainak további kezelése (úgy, mint: alkalmasság eldöntése) már a munkaviszony létesítése céljából történik, így az azzal kapcsolatos adatkezelést a 3.1. pont taglalja.

Adatkezelés célja: a megüresedő álláshelyek betöltésére megfelelő leendő munkavállaló kiválasztása, a jelentkezők személyes adatainak kezelése

Kezelt adatok köre: név, születési dátum, anyja neve, lakcím, képzési adatok, fénykép, az érintett által megadott egyéb adatok

Adatkezelés jogalapja: az Infotv. 5 § (1) bekezdés a) pont szerinti hozzájárulás

Adattárolás határideje: az adatfelvételtől számított 1 évig

Adattárolás módja: papíralapon és elektronikusan

### Titoktartási nyilatkozat

Jelen nyilatkozatunkban rögzítjük, hogy a Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Korlátolt Felelősség Társaság (a továbbiakban: Társaság) által ..... (anyja neve: ....., születési hely és idő: ....., .....) előtt az eddigiekben feltárt és a jövőben feltárandó bizonyos információk, így különösen üzleti titok, ügyfelek adatai és egyéb tulajdonosi információk, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) hatálya alá tartozó személyes adatok (összefoglalóan: információk) bizalmas jellegűek.

..... a nyilatkozat aláírásával elfogadja, hogy az információk egyetlen részét vagy töredékét sem teszi közzé, nem bocsátja rendelkezésre, vagy nem tárja fel más módon semmilyen harmadik fél előtt a Társaság ügyvezetőjének, illetőleg a jogosult erre felhatalmazó előzetes írásbeli beleegyezése nélkül, kivéve, ha ezek az információk bizonyító erejű dokumentumokként nyilvánosságra bocsáthatók. Az ilyen információk nem tekintendők nyilvánosságra bocsáthatónak pusztán azért, mert ezekből további általános információkat lehet szerezni, vagy mert begyűjthetők egy vagy több forrásból is, vagy ha abból adódóan kerültek nyilvánosságra, mert megszegték a jelen nyilatkozatot, vagy harmadik személlyel vagy jogi személlyel kötött hasonló nyilatkozatokat.

Nyilatkozattevő kijelenti, hogy minden ésszerű elővigyázatossági intézkedést megtesz annak érdekében, hogy szóban, írásos anyagban, vagy elektronikus adattároló eszközön vagy más módon feltárt információkat megfelelő védelemmel lásson el bármely harmadik fél előtti jogosulatlan feltárással szemben, így különösen betartja a Társaság Adatvédelmi és Adatbiztonsági Szabályzatának irányadó rendelkezéseit. Nyilatkozattevő kijelenti, hogy saját, illetve illetéktelen harmadik személy részére egyetlen anyagról sem készít másolatot és az ilyen anyagok valamennyi másolatát kérésre azonnal visszaszolgáltatja.

Nyilatkozattevő elfogadja továbbá, hogy valamennyi ilyen információ tulajdonosa a Társaság, mindezen információk bizalmas jellegűek, értékesek és nélkülözhetetlenek. Nyilatkozattevő kijelenti, hogy az ilyen információkat megőrzi, azokat saját vagy harmadik fél javára fel nem használja.

Jelen nyilatkozat aláírása a nyilatkozattevőt nem ruházza fel semmiféle jogosultsággal vagy egyéb joggal.

Jelen titoktartási nyilatkozaton megadott, az Infotv. hatálya alá tartozó személyes adatot a Társaság az Adatvédelmi és Adatbiztonsági Szabályzata alapján kezeli.

....., 20.....

.....  
Nyilatkozattevő

.....  
Társaság képviseletében



### Adatvédelmi tájékoztató és nyilatkozat

A Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Korlátolt Felelősség Társaság (a továbbiakban: Társaság), mint munkáltató a munkavállalók személyes adatait kizárólag a munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) szerinti adatkörben - különös tekintettel a Mt. 10-11 §-ára –a munkaviszonnyal összefüggésben kezeli.

A munkaviszony kapcsán beszerzett harmadik személy adatai a szükséges adattartamot meg nem haladóan vehetők fel és kezelhetők. (Pl. pótszabadság, családi adókedvezmény)

Az adatkezelés célja: munkaviszony létesítése, teljesítése vagy megszüntetése, az ezekkel kapcsolatos jogosultságok elismerése és kötelezettségek tanúsítása.

Az adatkezelés jogalapja: törvényi felhatalmazás [Mt. 10. § (1) és (3)] és az érintett hozzájárulása [az információs önrendelkezési jogról és az információszabadságról szóló 2011. CXII. törvény (Infotv.) 5 § (1) a)].

Az adattárolás határideje: az adatkezelés céljának megvalósulásáig, főszabály szerint a munkaviszonnyal kapcsolatos jogosultságokkal és kötelezettségekkel kapcsolatosan a munkaviszony megszűnéséig, munkaviszonyból fakadó jogosultságokkal kapcsolatosan a nyugdíjfolyósításról szóló jogszabályokban meghatározott határideig.

Az adatkezelés módja: elektronikus és papíralapú.

Jogérvényesítési lehetőségek: a munkavállaló az Infotv. 14-19.§-ban, valamint a Társaság Adatvédelmi és Adatbiztonsági Szabályzatában foglaltak szerint tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – azok törlését vagy zárolását.

Alulírott ..... (születési hely, idő: ....., ....., anyja neve: ..... ) kijelentem, hogy a fenti tájékoztatást tudomásul vettem. Az Infotv. 5. § (1) bekezdés a) pontja szerint hozzájárulásomat adom, hogy a Társaság, mint munkáltató az Infotv. 3. § 2. pontja szerinti személyes adataimat<sup>1</sup> kezelje. A hozzájárulás kiterjed továbbá arra, hogy a Társaság az alábbi személyes adataimat:

- név, anyja neve, születési hely, születési idő, személyazonosító igazolvány száma, lakcím, önéletrajzi adatok, céges e-mail címem,

a tevékenysége folytatásához szükséges körben harmadik személy részére továbbítsa.

Kelt: .....

.....  
(név)

<sup>1</sup>személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés;

## Tájékoztató elektronikus rendszerek használatával összefüggő adatkezelésről

Tisztelt Munkavállaló!

Munkaviszonyával összefüggésben tájékoztatjuk Önt, hogy a Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Korlátolt Felelősség Társaság (a továbbiakban: Munkáltató) a munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) 11. § (1)-(2) bekezdésének rendelkezései alapján jogosult a munkavállalókat a munkaviszonyból eredő kötelezettségek teljesítése céljából a munkaviszonnyal összefüggő magatartásuk körében ellenőrizni.

A Munkáltató a munkavállalók számára munkavégzési célból számítógépet, e-mail címet és internet-hozzáférést biztosíthat. A használat részletes szabályait a Munkáltató belső szabályzatai és eljárásrendjei tartalmazzák.

Figyelemmel arra, hogy a Munkáltató a tulajdonát képező személyi számítógépeket és laptopokat, céges e-mail címeket kizárólag munkavégzés céljából biztosítja, így amennyiben a munkavállaló ezen eszközökön magáncélú személyes adatait (pl.: családi fotók, telefonkönyvek, saját adatbázisok stb.) tárolja, úgy a Munkáltató a számítógép ellenőrzése során ezeket az adatokat is megismerheti. Ezen adatkezelés ellen a munkavállaló kifogással nem élhet, tekintettel arra, hogy a nem munkavégzés céljából történő, de a Munkáltató tulajdonát képező eszközön való személyes adatok tárolása az adatkezeléshez történő 2011. évi CXII. törvény (Info tv.) 5. § (1) bekezdés a) pont szerinti hozzájárulásnak minősül.

Mindazon e-mail címek, amelyekben a Munkáltató neve kiterjesztésként benne foglaltatik (.....@szechenyiprogramiroda.hu, ...@szpi.hu), valamint, amelyek alapvető rendeltetése a Munkáltató működésével összefüggő tevékenységek ellátása (pl.: .....@vati.hu), a Munkáltató tulajdonát képezik. Ezek a címeken folytatott levelezés munkacélú levelezésnek minősül, melybe a Munkáltató az Mt. 11. § (1) bekezdése alapján jogosult betekinteni. A Munkáltató jogosult továbbá a fent nevezett címeken folytatott levelezések meghatározott időközönkénti biztonsági mentésére, az elektronikus levelező rendszer folyamatosságának és stabilitásának érdekében adatbiztonsági okokból saját eszközein bármilyen állomány törlésére. Amennyiben a munkavállaló a fenti céges e-mail címén található leveleiben magáncélú személyes adatait, kifejezett utalás nélkül, tárolja, úgy a Munkáltató az e-mail cím ellenőrzése során ezeket az adatokat is megismerheti. Ezen adatkezelés ellen kifogással nem élhet a munkavállaló, tekintettel arra, hogy a nem munkavégzés céljából történő, de a munkáltatói e-mail címen való személyes adatok tárolása az adatkezeléshez történő Info tv. 5. § (1) bekezdés a) pont szerinti hozzájárulásnak minősül.

A Munkáltató jogosult ellenőrizni a munkavállalók részére munkavégzés céljából biztosított eszközöket, a munkahelyi postafiókot és internet használatot. Mindemellett főszabály szerint a magáncélú levelek tartalmát a Munkáltató munkaviszonyból fakadó jogosultság érvényesítése során sem jogosult megismerni.

Budapest, .....

Schultz Gábor  
 ügyvezető  
 Széchenyi Programiroda Nonprofit Kft.

Átvettem és tudomásul vettem Budapesten, 201... .. hó ... napján:

Munkavállaló

## Válaszlevél berepülő önéletrajzokra

**Tisztelt .....!**

Köszönjük, hogy önéletrajzát elküldte a Széchenyi Programiroda Nonprofit Kft. (a továbbiakban: Társaság) számára.

Sajnálattal tájékoztatjuk, hogy az Ön végzettségének és tapasztalatainak megfelelő munkakör betöltésére a Társaságnál jelenleg nincs folyamatban kiválasztási eljárás.

A jövőt tekintve azonban bízunk benne, hogy az Ön képzettségének és tapasztalatainak megfelelő pozíciót tudunk ajánlani. Erre való tekintettel, illetve a Társaság Adatvédelmi és Adatbiztonsági Szabályzata alapján önéletrajzát a későbbi esetleges felhasználás céljából iktatjuk és kategorizáljuk, hogy amennyiben Önnek megfelelő munkakörre keresünk leendő munkavállalót, akkor Ön is a lehetséges jelöltek közé kerülhessen. Ennek megfelelően önéletrajzát és az abban szereplő személyes adatait az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 5. § (1) bekezdés a) pontjában meghatározott jogalappal, a megfelelő munkavállaló kiválasztását elősegítendő rögzítjük, és a továbbiakban a Társaság Adatvédelmi és Adatbiztonsági Szabályzata szerint a felvételre jelentkezők személyes adataira vonatkozó szabályok alapján egy évig nyilvántartjuk.

Személyes adatainak törlését bármikor kérelmezheti az alábbi elérhetőségen:  
HR\_adatok@szechenyiprogramiroda.hu

Bizalmát és érdeklődését köszönjük, a jövőben sok sikert kívánunk céljai eléréséhez.

.....; 20.....

Üdvözlettel:

.....






### BYLAWS ON DATA PROTECTION AND DATA SECURITY

COMPANY NAME:	SZÉCHENYI PROGRAMME OFFICE NONPROFIT LLC
REGISTERED SEAT:	1053 Budapest, 2 Szép street, IV.th floor
TAX NUMBER:	18080313-2-41
COMPANY REGISTRY NUMBER:	01-09-916-308
hereinafter referred to as:	Company

The present Bylaws on Data protection and Data security (hereinafter referred to as the Bylaws) comprises the rules on keeping registration of procedures of internal data processing and guarantee arrangements ensuring the rights of data subjects.

The Bylaws is obligatory and binding for all employees and organizational units of the Company

Prepared by: Péter Vigh, Dr. iur. 	Supervised by László Kongorác, Dr. iur. 	Approved by: Csilla Hajasné Kurka, dr. iur. 
Based on Article 17 (2) of the Act I of 2012 on Labour Code Bylaws of the Employer shall be considered delivered if published by means considered customary for, and commonly known in the area.		



## Content

I. Introduction.....	3
II. The aim and scope of the Bylaws .....	3
III. Acts and their abbreviations used in relation to the rules .....	3
IV. Explanatory notes.....	3
V. General rules of the data processing .....	5
VI. Data protection system of the Company .....	6
VII. Responsibilities.....	6
VIII. Rules on data security.....	7
IX. Enforcement of the rights of data subjects .....	8
X. Data processes carried out at the Company .....	9
1. Data processing relating to the use of Monitoring System (MS).....	9
2. Data processing relating to newsletter service.....	10
3. Personnel data processing.....	10
3.1. Data processing of employees regarding their employment relationship .....	10
3.2. Data processing regarding the control of the employees.....	11
3.2.2. Data processing in connection with biometric identifier access control system .....	11
3.3. Data processing of applicants for work.....	12
Appendix no. 1.....	14
Non-disclosure declaration.....	14
Appendix no. 2.....	15
Data protection information sheet and declaration.....	15
Appendix no. 3.....	16
Information on data processing regarding the use electronic systems.....	16
Appendix no. 4.....	17
Answer letter for incoming CVs.....	17



## I. Introduction

The Company constitutes the following Bylaws on Data protection and Data security (hereinafter referred to as the Bylaws) in order to ensure the registration of procedures of internal data processing and the rights of data subjects. The present provisions shall be interpreted in accordance with provisions of other bylaws of the Company. In case there is a discrepancy regarding the personal data protection between the present provisions and any other Bylaws' provisions which came into effect before the present Bylaws' has entered into force, the present provisions shall prevail.

## II. The aim and scope of the Bylaws

1. By constituting and accessing the present Bylaws the Company wishes to ensure the implementation of the right to be informed determined in Article 15 of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as the Act).

2. The aim of the present Bylaws is that data subjects shall receive adequate information concerning the data relating to him, including those processed by the Company or a data processor on its behalf or according to its notice, the sources from where they were obtained, the purpose, the grounds and the duration of processing, the name and address of the data processor who might be involved in data processing, its activities relating to data processing and –in case of data transfer – the legal basis and the recipients.

3. By the present Bylaws the Company wishes to ensure the rule of law of the registries, the constitutional principles of the data protection and to facilitate the implementation of the data security's requirements. The Company wishes to prevent the illegitimate access of data and their illegitimate alteration or disclosure.

4. The material scope of the Bylaws is extended to all processes concluded at all organizational units when personal data processing is realized subject to Art. 3. Point 2. of the Act.

5. Besides the named data processes the Company may - as laid down there - carry out additional data processes connected to programmes, or project of which program or project specified details will be published on the website of the Company or on the website of programme or of the project. The regulations of the present Bylaws applies to these additional data processes.

## III. Acts and their abbreviations used in relation to the rules

the Act.	Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
LC	Act I of 2012 on Labour Code
PIT	Act CXVII of 1995 on Personal Income Tax

## IV. Explanatory notes

The definition-system of the present Bylaws is in compliance with definitions determined in Art.3 of the Act, in particular:

1.Data subject: shall mean any natural person directly or indirectly identified or identifiable by reference to specific personal data;

2. Personal Data: shall mean any (identified or identifiable) data relating to a natural person (hereinafter referred to as the data subject) and conclusions drawn from the data in regard to the data subject. In the course of data processing, the data in question shall be treated as personal as long as the data subject remains identifiable through it. A person shall be deemed identifiable - directly or indirectly - in particular by



reference to the name and identification number or one or more physical, physiological, mental, economic, cultural or social factor based on which the identity of the data subject might be identified.

**3. Special data shall mean:**

- a) personal data revealing racial origin or belonging to national and ethnic minorities, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership,
- b) personal data concerning health, pathological addictions, data concerning sexual life or criminal record.

**4. Criminal personal data:** shall mean personal data relating to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings.

**5. The data subject's consent:** shall mean any freely and expressly given specific and informed indication of the wish of the data subject by which he/she signifies his/her agreement to the process of personal data relating to him/her fully or to the extent of specific operations.

**6. The data subject's objection:** shall mean a declaration made by the data subject objecting the processing of his/her personal data and requesting the termination of data processing, or the deletion of the data processed.

**7. Controller:** shall mean natural or legal person, or organisation without legal personality which determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor.

**8. Data processing:** shall mean any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use. Taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans) shall also be deemed as data processing.

**9. Data transfer:** shall mean ensuring access to the data for a third party; Disclosure shall mean ensuring open access to the data for the public.

**10. Data deletion:** shall mean making data unrecognisable in a way that it can never again be restored

**11. Blocking of data:** shall mean making impossible further data transfer, dissemination, access, transformation, modification, destruction, deletion, synchronisation or link of the data with utterly or for a determined period.

**12. Data destruction:** shall mean complete physical destruction of the data or the data carrier recording the data.

**13. Data process:** shall mean performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data.

**14. Data processor:** shall mean any natural or legal person or organisation without legal personality processing the data on the grounds of a contract, including contracts concluded pursuant to legislative provisions;

**15. Data set:** shall mean all data processed in the same filing system.





16. Authority: Hungarian National Authority for Data Protection and Freedom of Information

17. Personal data filing system (hereinafter referred to as filing system) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

In case definitions of the legislation on data protection in force at any time (the Act at the time of creation of the present Bylaws) deviate from the definitions of the present Bylaws, the definitions of the legislation shall prevail.

## V. General rules of the data processing

During its proceedings the Company shall carry out data processing in compliance with the legislation in force, in particular:

1. Personal data may be processed only for the exercising of certain rights and fulfillment of obligations at the Company. Using personal data for private purposes processed by the Company is prohibited.

2. Data processing shall always comply with the principle of purpose limitation under which

- the Company may process personal data only for specified and explicit purposes, where it is necessary for exercising of certain rights and fulfilment of obligations, to the minimal extent and for the duration necessary to achieve its purpose.
- data processing must comply with its purpose in all stages of data processing operations– and in case the purpose of the processing has ceased or becomes unlawful, data shall be deleted.

3. The Company may process personal data only with the prior consent of the data subject or as decreed by law or based on authorization conferred by law. In case of special data consent shall be given in writing.

4. In all cases the Company shall communicate the purpose and the legal basis of the data processing to the data subject before recording data.

5. Employees processing data at organizational units of the Company and employees of organizations participating in processing data and carrying out a certain operation of the data processing on behalf the Company on an occasional basis shall keep personal data acquired as business secret. Persons processing personal data and persons who have possible access to these data shall make a Non-disclosure declaration (Appendix 1.). Data processing employee of the Company shall have liability for disciplinary action, damages, misdemeanor or criminal sanctions to process personal data acquired during exercising his duties and powers lawfully and exercise access rights to the registries of the Company lawfully.

6. Should a person subject to the Bylaws becomes aware that the personal data processing by the Company is erroneous, incomplete or untimely, he is obliged to rectify or initiate rectification from his colleague responsible for recording.



## VI. Data protection system of the Company

1. The managing director of the Company considering the specialities of the Company shall define the organization of data protection, the duties and powers relevant to data protection and activity connected to it, and designates the person who supervises the data processing.
2. The supervision of the data protection system is fulfilled by the managing director through the internal data protection officer appointed by him. The internal data protection officer of the Company is the Head of the Human Resources and Network Development Department (hereinafter referred to as HR) at all times.

## VII. Responsibilities

1. With regard to the data protection the managing director:

a) shall be responsible to ensure the conditions necessary for data subjects to exercise their rights determined in the Act

b) shall be responsible for ensuring the personal, material and technical requirements necessary for the protection of personal data processed by the Company

c) shall be responsible for ceasing any defects and unlawful conditions defined during the control in respect of data control and to initiate and conduct procedure to establish personal responsibility

d) supervises the activity of the internal data protection officer

e) may order examination

f) issues bylaws of the Company regarding data protection and data security

### 2. Relating to the data protection the internal data protection officer:

a) shall provide help for the data subject to ensure his/her rights

b) shall initiate registration procedure defined in the Act at the Authority

c) shall provide report until every 31 of January for the managing director about the enforcement of the Company's data protection

d) shall be entitled to control how certain organizational units ensure the compliance with the present bylaws

e) shall keep the data transfer register

f) shall monitor the legislative amendments of data protection and freedom of information and initiates the alteration of the present bylaws accordingly if needed.

g) shall contribute to answer requests from the Authority and shall participate in investigations initiated by the Authority and in administrative proceedings of data protection.

h) shall draft request towards the Authority in order to provide standpoint when a question arises and cannot be answered through legal interpretation clearly

i) shall fulfill ad hoc cases determined by the managing director

3. Heads of all organizational units are responsible to ensure the compliance of the provisions of the Bylaws according to their concerned function.



4. Employees of the Company shall ensure during their work that unauthorized persons shall not have access to personal data and the storage and placement of personal data shall be formed in such way that for unauthorized persons may not be accessible, may not become available to be aware of it, may not be alterable or destroyable.

### **VIII. Rules on data security**

#### **1. The Company adopts the following measures in respect of the security of the personal data processed on paper format:**

- a) data may be accessible only for entitled persons others may not access it and it may not detect it
- b) documents shall be placed in a well lockable, dry space with fire control equipment
- c) documents under permanently active processing may be accessible only for competent persons
- d) the Company's employee processing data may leave the place where data is under process in such way that he locks away the durable medium or locks up the office.
- e) the Company's employee processing data after finishing his work locks away the paper based durable medium
- f) in case personal data processed on paper based are digitalized, provisions regarding documents stored digitally shall be applied by the Company

#### **2. The Company adopts the following measures and guarantees in respect of the security of the personal data stored on computer or network in compliance with the Information Security Bylaws:**

- a) personal computers and laptops used during the data processing are owned by the Company or it has rights equivalent to ownership rights.
- b) data stored on the computer shall be accessible only with valid, personalised, identifiable access rights and at least with user name and password. The Company ensures the regular exchange of the passwords in compliance with the provisions of the Information Security Bylaws.
- c) all records with data on the computer are logged in a monitorable way.
- d) data stored on network server computer (hereinafter referred to as: server) shall be accessible only with appropriate access rights and only for persons appointed for it
- e) in case the purpose of the data processing had been realised, the deadline of the data processing elapsed the file compromising the data will be deleted in an unrestoreable way, the data may not be retrievable which shall ensure the head of the organizational unit ( hereinafter referred to as head of the organizational unit) who has powers and duties at the lowest level
- f) in order to the security of the data stored on the network the Company avoids the data loss by continuous reflection on the server
- g) makes savings daily from the active data base containing personal data. The saving shall apply for all data set of the central server and it is made on magnetic data medium
- h) the magnetic data medium containing the saved data is stored in a fireproof way in a lockbox made for this purpose and placed in a fireproof space
- i) the Company shall ensure the anti-virus protection on the personal data platform



j) prevents the access of unauthorised persons to the network with the computing instruments available

## **IX. Enforcement of the rights of data subjects**

1. The data subject may request information on his personal data being processed and may request the rectification and the erasure or blocking of his/her personal data, save where processing is rendered in a legislative.
2. The Company shall refer within three days from the receipt of the request received or the objection to the head of organizational unit who has powers and duties concerned data processing.
3. The head of organizational unit shall prepare an answer in an easily understandable form within 3 days from the reference under point 2. concerning the request regarding the personal data processing of the data subject which shall be sent to the internal data protection officer immediately for his opinion.
4. The internal data protection officer immediately examines the prepared answer and sends the approved draft to the managing director for signing and for the purpose to send it to the data subject.
5. The managing director as acting on behalf of the data controller informs in writing the data subject in connection with his request on the data processing within 25 days - in case of exercising objection right within 15 days - from the receipt by the Company.
6. The information shall contain information defined in Art 15 (1) of the Act if providing information cannot be rejected based on law.
7. The information is in principle free of charge, the Company may charge only in cases determined in the Act.
8. The Company may refuse request only on the grounds referred to in the Act, in written format and providing information in compliance with the regulations of the Act.
9. Data deemed as inaccurate shall be corrected by the head of the organizational unit processing data - if relevant data and documents proving them are at disposal – in case reasons defined in Art. 17 (2) of the Act he takes measures for the deletion of the data processed.
10. For the period of adjudication of the objection of the data subject – but no longer than 5 days - the head of the organizational unit processing data shall suspend the processing, shall examine the merits of the objection, shall draft the decision which he shall send to internal data protection officer for his opinion. Data subject shall be informed about the decision within the deadlines laid down in point 5. of this chapter by the managing director acting on behalf of the data controller as to Art. 21 (2) of the Act.
11. In case the objection is justified, the head of the organizational unit processing data shall act according to the provisions of the Act.
12. In case the adjudication of the case lacks clarity when data subject exercises his rights, the head of the organizational unit processing data shall send the documents of the case with his opinion regarding the case to the internal data protection officer requiring his statement who shall fulfill this request within three days.
13. The Company shall pay for damages caused to a data subject as a result of unlawful processing or by any breach of data security requirements and shall pay restitution for violation of the personal rights of the data subject by unlawful data processing or by breaching data security rules. The data controller shall be released from liability for damages and from paying restitution if he proves that the damage or the violation of personal rights were brought about by reasons beyond his data processing activity. Also no compensation shall be paid where the damages was caused by intentional or serious negligent conduct on the part of the



aggrieved party.

14. In the event of any infringement of his rights data subject may turn to the court competent according to the Act or may turn to the Authority:

name: Hungarian National Authority for Data Protection and Freedom of Information

registered office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

website: [www.naih.hu](http://www.naih.hu)

#### **X. Data processes carried out at the Company**

The place of data processing: 1053 Budapest, Szép street 2.

##### **1. Data processing relating to the use of Monitoring System (MS)**

The Company is processing personal data by using MS during the realization of project with identification number KÖFOP-3.3.3-15-2016-00001 (hereinafter referred to as: the Project) and with title 'Supporting and assisting the capacity of the applicants and the beneficiaries during the planning and implementation of projects'

The purpose of the data processing: evaluation of tender materials, giving back information, proper due process in connection with tasks regarding the implementing of the Project, fulfilling obligations of the Company concerning the Project

The legal basis of the data processing: consent of the data subject (Art.5 (1) point a) of the Act)

Duration of the data processing: data are stored until the withdrawal of the consent of the data subject, but 5 years after the Project's financial closure at the latest.

Processed data: name, address, phone number, e-mail address

The method of data processing: electronic



## 2. Data processing relating to newsletter service

The Company processes personal data in connection with the subscription for the newsletter on the website [www.szpi.hu](http://www.szpi.hu) (hereinafter referred to as the Website).

The purpose of data processing: ensuring the use of the Website's services (sending informative newsletter). During the maintenance of the internet connection technical data automatically arise in the computer system of the Company concerning internet browser used by the visitor of the Website, the domain name (URL), the time of the visit and the viewed webpages. The Company uses these only for the analysis in connection with the Website and for statistical information.

Processed data: name, e-mail address

The legal basis of the data processing: consent of the data subject (Art.5 (1) point a) of the Act)

Duration of the data processing: data are stored until the withdrawal of the consent of the data subject, but for 5 years after the Project's (KÖFOP-3.3.3-15-2016-00001) financial closure at the latest

The method of the data processing: electronic

## 3. Personnel data processing

### 3.1. Data processing of employees regarding their employment relationship

Data may be processed only with regard to data referred to LC – particularly set forth in Art-10-11.

The purpose of the data processing: establishment, fulfillment or termination of employment relationship, and recognition and proof of rights and obligations in connection with them

Data processed in relation with employees:

name, name at birth, place and date of birth, photo, citizenship, identification number, mother's maiden name, permanent address, place of residence (in case it is different from the permanent address), the fact of being a member of a private retirement scheme, starting date of the membership (year, month, day), tax number, social security number (TAJ number), retirement identification number (in case of a pensioner), bank account, the name of the bank, starting date of the employment relationship, the type of the insurance, working hours per week, telephone number, family status, copy of the document supporting the qualification, occupational health certificate supporting working ability, the fact of working ability, original copy of judicial record, copy of documents necessary for using extra vacation time according to Art. 120, of the LC for the purpose of using extra vacation and/or consumption of family tax allowance place and date of birth, permanent address, mother's maiden name, social security number (TAJ number), tax number of relatives under the age of 16 years; exit documents of the former workplace for the past two years; the characteristics of engagement besides the fulltime employment, the employer's name and address of that engagement, the average worktime at workplace beside the fulltime employment, the activity which is carried out, the fact of participation in a company, the status and beginning of the participation, the activity of the company

The legal basis of the data processing: authorization conferred by law (Art. 10. (1) and (3) of the LC) and the consent of the data subject Art.5 (1) point a) of the Act)

Deadline of the data storing: until the data processing achieved the purpose, in principle regarding the rights and obligations of the employment relationship until the termination of the employment relationship, regarding rights stemming from the employment relationship until the deadlines defined in laws in connection with pension paying.



The method of data processing: electronic and paper based

Data gained in connection with third persons may not exceed the content which is necessary for the recording and processing (e.g. extra vacation time, family tax allowance)

An information sheet is drafted about the data processing of the employees in order to provide them prior information about data processing (Appendix 2.). The information is signed by the employee immediately after the entry into force of the present Bylaws. New employee is obliged to sign the information sheet simultaneously to the establishment of the employment relationship.

The legal basis of data processing of the personnel field might be different law case by case. The duration of data processing is defined by the relevant legislation. (e.g. PIT, LC)

In case of those data processing within personnel field which are not directly stemmed from employment relationship consent of the data subject shall be acquired indicating the purpose and the duration of the data processing.

### **3.2. Data processing regarding the control of the employees**

#### **3.2.1. Data processing in connection with using electronic systems**

The Employer may control the employees regarding the fulfillment stemming from their obligations in connection with their conduct within the employment relationship. The legal basis for the control stems from Art. 11 (1)-(2) of the LC. The Company provides computer for working, e-mail address, internet access when necessary. The Company shall inform the employees in writing about the rules of the use and the possibility of control in advance. The written information shall be provided according to the Appendix 3. of the present Bylaws which the Company shall acquaint Employees with.

As the Company provides personal computers and laptops which is its own property, and company e-mail addresses for the purpose of working, in case the employee stores private personal data (e.g. family photos, directories, own databases) on these devices the Company may learn these data during the control of the computer. The employee cannot object against this data processing as storing personal data on Company's device - by conduct – should be deemed as the consent of the data subject according to Art- 5 (1) a) of the Act. The Company informs the employees in writing about this fact (and about the archiving and about the activity of the computer administrator) prior to the use of devices.

All e-mail addresses which involve the Company's name as extension (...@.....hu) and which has a function to carry out activities in relation with the Company's operation(e.g.: .....@vati.hu) shall be the property of the Company. Mailing via these addresses by the employees of the Company shall be deemed as mailing for working purpose. The Company has right of access to correspondence from such addresses based on Art.11 (1) of LC.

The Company has right to make backups at specified intervals of correspondence of the abovementioned addresses and in order to ensure the continuity and stability of the electronic mail system has right to delete any data files for data security reason. In case the employee stores his/her private personal data in the abovementioned company e-mail addresses without explicit reference to it then the Company may learn these data during the control of the e-mail address. The employee cannot object against this data processing as storing personal data on Company's device - by conduct – should be deemed as the consent of the data subject according to Art. 5 (1) a) of the Act. The Company is entitled to control the workplace mailbox and the use of the internet. Besides these, generally the employer is not entitled to get to know the content of the private mails in order to enforce his rights arising from employment relationship.

#### **3.2.2. Data processing in connection with biometric identifier access control system**

The Company is operating a biometric identifier access control system (hereinafter referred to as access control system) in rented areas (floor 2., 3., 4. and 7.) of the building at 1053 Budapest, Szép street 2. in order to identify the employees and keep register of the presence.



The employees working on a permanent basis in offices on a given floor are obliged to use the access control system when arriving (start of the worktime) and when leaving (at the end of worktime).

The reason for the use of the access control system:

Within the framework of the management of programs relating to applications for EU, other international or national budgetary resources (as an assisting function to perform public services) the employer processes business and economic data during which the utilization of a blocking system is essential for the purpose of the highest protection of these data which is in the business interest of the applicants and in the interest of national economy protected by the organizations providing the sources. Secondly, the utilization of a blocking system is necessary for the control of the availability of employees during working time. Other, less intensive ways (such as attendance register or magnetic card) does not ensure that the entered data really indeed origins from that time and from that person who is tied in the registry with.

During the utilization of the blocking system the Company pays particular attention to the protection of the personality rights of the employees.

The purpose of the data processing: the control of the employees based on Art.11 (1) of LC

Data processed: personal data (certain points of friction ridges of the fingerprint) recorded during the control

The legal basis of the data processing: Art. 11 (1) of LC and Art 5 (1) a) of the Act

Deadline of the data storing: only for the duration of the employment relationship, data are deleted after the termination of employment.

The method of the data processing: electronic

### **3.2.3. Data processing regarding the application of electronic monitoring system**

The Electronic Monitoring System Bylaws which had been entered into force with managing director's order No. 7/2017 on 7 March 2017 comprises the rules relating to data processing concerning the application of electronic monitoring at the Company

### **3.3. Data processing of applicants for work**

The Company does not differentiate between the way of arriving Curriculum Vitae (hereinafter referred to as CVs) for the purpose of applying for job positions containing personal data: CVs sent on a paper format and electronically fall under the same evaluation.

In case of CV-s arriving via post, provided that the applicant sends it to the address advertised at recruitment with the expected sign then the Company guarantees data processing according to the present point.

In case the paper based CV does not arrive in the way it was advertised then according to the rules on document management the person who constitutes as the addressee shall ensure that the CV is given to the head of HR. In case this not happens the Company applies the relevant general rules on document management regardless of the content of the letter.

In case of application for non-advertised job position (hereinafter referred to as incoming CV) the Company shall send an answer letter to the applicant in which he informs about the fact and the legal basis of data processing and the forms of the objection of data processing. The 'Answer letter for incoming CVs' is Appendix 4. of the Bylaws.





### 3.3.1 Special rules regarding recruitment

As the main rule the Company stores the CVs with the aim of using them later – this applies also when the CV arrives for an advertised position. The Company is processing CV and personal data in it with regard to the present Bylaws and its provisions. The Company considers the submission of the CV as a consent for processing personal data in it. In case the data subject does not wish that the Company should process his data according to the present Bylaws then he shall indicate this simultaneously with sending the CV or later on by the withdrawal of his consent given by sending the CV.

Further data processing (such as the decision on suitability) of data subjects selected based on the CV is carried out with the purpose of establishing employment relationship so data processing regarding this is laid down in point 3.1.

The purpose of the data processing: selecting appropriate future employee for filling open job positions, processing personal data of applicants

Data processed: name, place and date of birth, mother's maiden name, address, training data, photo, other data given by the data subject

The legal basis of data processing: the consent of the data subject (Art.5 (1) point a) of the Act)

Deadline of data storing: 1 year from the registration of data

The method of the data storing: paper based and electronical



### Non-disclosure declaration

We hereby lay down in the present declaration, that certain information - in particular business secrets, client's data and other owner's information and personal data under the scope of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as the Act) (together information) - which were disclosed and will be disclosed in the future by Széchenyi Programme Office Nonprofit Limited Liability Company (hereinafter refer to as : the Company) to ..... ( mother's maiden name.... place and date of birth: .....), are confidential.

By signing the declaration ..... accepts that neither a part nor a fragment of the information will he disclose, he will not make available or reveal it in other way to a third party without the prior written consent of of the managing director or of a person entitled to give this authorization except these information may be disclosed as document of evidence. Such information may not be considered as it may be disclosed only for the reason that further general information may be gained from them or because they may be collected from one or more sources or because they were disclosed as a result of breaching the provision of the present Bylaws or of a similar declaration concluded with a third person or legal entity.

Declarant hereby declares that he will take all reasonable precautionary measures in order to ensure the appropriate protection of information disclosed orally, in written material or via electronic data storage device or in other way against unauthorized disclosure of any third person, especially complies with the provisions of the Bylaws on data protection and data security.

Declarant hereby declares the he will not make copy of the material for himself or for an unauthorised third person and he will immediately deliver back the copy of such material upon request.

Declarant hereby accepts that the owner of all such kind of information is the Company, all information is confidential, valuable and indispensable.

Declarant hereby declares that he keeps such kind of information and will not use for his own or for a third party's benefit.

The signiture of the present declaration does not give any entitlement or other right to the declarant.

Personal data (under the scope of the Act) given in the present non-disclosure declaration are processed by the Company according to the Bylaws on Data Protection and Data Security.

....., 20.....

.....  
Declarant

.....  
on behalf of the Company



### Data protection information sheet and declaration

The Széchenyi Programme Office Consulting And Service Nonprofit Limited Liability Company (hereinafter referred to as the Company), as Employer processes personal data of the employees only in respect of the set of data laid down in Act I of 2012 on Labour Code - particularly in Art. 10-11 of the LC – and only in connection with the employment relationship.

Registration and process of data of third persons gained in connection with the employment relationship may not exceed the set of data which is necessary. (e. g.:extra vacation, family tax allowance)

The purpose of the data processing: establishment, fulfillment or termination of employment relationship, and recognition of rights and obligations in connection with them.

The legal basis of the data processing: authorization conferred by law (Art. 10. (1) and (3) of the LC) and the consent of the data subject Art. 5 (1) point a) of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

Deadline of the data storing: until the aim of data processing achieved, in principle regarding the rights and obligations of the employment relationship until the termination of it, or until the deadlines defined in laws in connection with pension paying regarding rights stemming from the employment relationship.

The method of the data processing: electronic and paper based

Law enforcement possibilities: the employee according to Art. 14-19 of the Act and according to the Company's Bylaws on Data protection and Data security may request information on his personal data processed, may request the rectification of his personal data, and - except for the data processing conferred by law - the erasure or blocking of his personal data.

I, the undersigned ..... (place and date of birth:.....– mother's maiden name: .....) hereby declare, that I have acknowledged the abovementioned information. I hereby give my consent as to the Art 5 (1) a) of the Act that the Company as employer may process my personal data<sup>1</sup> defined in the Art 3 point 2. of the Act:

- name, mother's maiden name, place and date of birth, number of the identity card, permanent address, details from the CV, my company e-mail address

and in order to carry out its activity may transfer to a third person as necessary.

Date

.....  
(name)

<sup>1</sup> personal data: data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject



### Information on data processing regarding the use electronic systems

Dear Employee,

We hereby inform you regarding your employment relationship that the Széchenyi Programme Office Nonprofit Limited Liability Company (hereinafter referred to as: the Employer) based on the Article 11 (1)-(2) of the Act I of 2012 on Labour Code has right to control the employees regarding the fulfillment of their obligations in connection with their conduct within the employment relationship.

The Employer may provide computer, e-mail address, internet access for working. The internal bylaws and procedures shall contain the detailed rules about the use.

Taking into account the fact that, the Employer provides personal computers and laptops which is its own property and company e-mail addresses only for the purpose of working, in case the employee stores private personal data (e.g. family photos, directories, own databases) on these devices then the Employer may learn these data during the control of the computer. The employee cannot object this data processing as storing personal data on Employer's device - by conduct - should be deemed as the consent of the data subject according to Article 5 (1) a) of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

All e-mail addresses which involve the Employer's name as extension (...@.....hu) and which has a function to carry out activities in relation with the Employer's operation (e.g.: .....@vati.hu) shall be the property of the Employer. Mailing via these addresses by the employees shall be deemed as mailing for working purpose. The Employer has right of access to correspondence from such addresses based on Art.11 (1) of LC.

The Employer has right to make backups at specified intervals of correspondence of the abovementioned addresses and in order to ensure the continuity and stability of the electronic mail system has right to delete any data files for data security reason. In case the employee stores his private personal data in the abovementioned company e-mail addresses without explicit reference to it then the Employer may learn these data during the control of the e-mail address. The employee cannot object this data processing as storing personal data on Employer's device - by conduct - should be deemed as the consent of the data subject according to Art- 5 (1) a) of the Act.

The Employer has right to control the devices provided for work, workplace mailbox and the use of the internet. Besides these, in principal the Employer is not entitled to get to know the content of the private mails in order to enforce his rights arising from employment relationship.

Budapest, .....

Gábor Schultz  
Managing director  
Széchenyi Programme Office Nonprofit LLC

I have received and acknowledged it in Budapest on .....

Employee



European Union  
European Structural  
and Investment Funds



HUNGARIAN  
GOVERNMENT

INVESTING IN YOUR FUTURE

Széchenyi Programme Office Nonprofit LLC  
1053 Budapest, Szép u. 2. IV. em.  
[info@szpi.hu](mailto:info@szpi.hu) [www.szpi.hu](http://www.szpi.hu)

**Answer letter for incoming CVs**

**Dear..... ,**

Thank you for sending your CV to Széchenyi Programme Office Nonprofit LLC (hereinafter referred to as the Company).

We regret to inform you, that currently there is no selection process at the Company for a position which is suitable for your qualification and experience.

We hope we can offer a position in the future which is suitable for your qualification and experience. In view of this and the Company's Bylaws On Data Protection And Data Security we record and categorize your CV for a possible use in case we will looking for an appropriate employee for a position that might be suitable for you. In this case you could be selected among the possible candidates. Accordingly, in order to facilitate the selection of the appropriate employee your CV and all of your personal data in it will be recorded and stored for one year on the legal basis determined in Article 5 (1) in Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and according to the provisions on the personal data of applicants for admissions of the Bylaws On Data Protection And Data Security..

You may request the deletion of your personal data at any time on the following contact:  
[HR\\_adatok@szechenyiprogramiroda.hu](mailto:HR_adatok@szechenyiprogramiroda.hu)

Thank you for your trust and interest, we wish you many success to achieve your future goals.

.....; 20.....

Yours sincerely

.....



