Iktatószám / *Reg. no.:* UTI/1-38/2020

A Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Korlátolt Felelősségű Társaság ügyvezetőjének

31./2020. számú ügyvezetői utasítása / *Managing Director's Order no. 31./2020.*

of the Széchenyi Programme Office Consulting and Service Nonprofit Limited Liability Company

1. §

A Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Korlátolt Felelősségű Társaság Az INTERREG+ Informatikai Rendszer adatvédelméről és adatkezeléséről szóló szabályzatát és annak függelékét jelen utasítás 1. számú mellékleteként magyar nyelven, 2. számú mellékleteként angol nyelven kiadom. / *I hereby publish the Data protection and data processing Regulation of the INTERREG+ IT system in Hungarian version as Annex No. 1 and in English version as Annex No. 2 of the present managing director's order and its appendix.*

2. §

Jelen ügyvezetői utasítás **2020. szeptember 7.** napján lép hatályba. / *The present managing director's order shall enter into force on* ***7th September 2020.***

Budapest, 2020. szeptember 7/ *7th September 2020*

.....

Szakács Áron László / *Áron László Szakács*
ügyvezető / *Managing Director*

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

1. számú melléklet a 31. számú ügyvezetői utasításhoz

AZ INTERREG + INFORMATIKAI RENDSZER ADATVÉDELMÉRŐL ÉS ADATKEZELÉSÉRŐL SZÓLÓ 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 ügyvezetői utasítás szabályozza az INTERREG+ Informatikai Rendszerben kezelt adatok általános adatvédelmi és adatkezelési szabályait.

Szakmai tartalomért felelős szervezeti egység vezetője:	Kodifikációért felelős:	Jogi megfelelőség tanúsítása:	Jóváhagyta:
dr. Futó Adrienn nemzetközi igazgató	dr. Káplár Anikó osztályvezető Jogi Osztály	dr. Dékány Anita jogi igazgató Pénzügyi megfelelőség tanúsítása: Biró Teréz gazdasági igazgató	dr. Nyerges Judit Ildikó adatvédelmi tisztviselő
A munka törvénykönyvéről szóló 2012. évi I. törvény 17. § (2) bekezdése alapján a munkáltatói szabályzatot közöltnek kell tekinteni, ha azt a helyben szokásos és általában ismert módon közzé teszik.			

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

Az INTERREG+ Informatikai Rendszer adatvédelmi és adatkezelési szabályzata

I. A Szabályzat célja

Az INTERREG+ Informatikai Rendszer (a továbbiakban: rendszer) tekintetében biztosítani szükséges a személyes adatok biztonságos kezelését, az adatvédelmi alapelvek és az érintettek jogainak érvényesülését, amelynek érdekében az adatkezelő köteles megfelelő technikai és szervezési intézkedéseket végrehajtani.
A Szabályzat célja, hogy adatkezelő megfeleljen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendeletben (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infó tv.) foglaltaknak.

II. A Szabályzat hatálya

Személyi hatály: a Szabályzat személyi hatálya kiterjed az adatkezelőre, az adatkezelő adatfeldolgozóira, valamint a rendszer tekintetében valamennyi adatkezelést végző felhasználóra.

Tárgyi hatály: a Szabályzat tárgyi hatálya kiterjed az adatkezelő, az adatfeldolgozó és a felhasználók által folytatott valamennyi – a rendszerben tárolt személyes adatot érintő –, részben vagy egészben automatizált módon történő adatkezelésre, valamint a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek a rendszerek részét képezik vagy amelyeket a rendszerekben rögzítenek.

III. Definíciók

a) adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzettadatkezelési műveletek összessége;

b) adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

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

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

e) adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

f) érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;

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

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

i) Hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság;

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

IV. Adatvédelmi alapelvek

1. Alapvető jogok védelmének elve

A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog. Az Európai Unió Alapjogi Chartája 8. cikk (1) bekezdése és az Európai Unió működéséről szóló szerződés 16. cikk (1) bekezdése rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

2. Jogszerűség, tisztességes eljárás és átláthatóság elve

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. A személyes adatok kezelése kizárólag akkor jogszerű, ha legalább a következők egyike teljesül:

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

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

3. Célhoz kötöttség elve

   A személyes adatok kezelése csak meghatározott, egyértelmű és jogszerű célból történhet, az adatok nem kezelhetők e célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

4. Adattakarékosság elve

   A személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük és a szükséges adatmennyiségre kell korlátozódniuk.

5. Pontosság elve
   A személyes adatoknak pontosan és szükség esetén naprakésznek kell lenniük. Az adatkezelőnek minden észszerű intézkedést meg kell tennie annak érdekében, hogy az adatkezelés célja szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

6. Korlátozott tárolhatóság elve

   A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, ha a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatás céljából vagy statisztikai célból kerül majd sor, az adatvédelmi jogszabályokban az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.

7. Integritás és bizalmasság elve

   A személyes adatok kezelését olyan módon kell elvégezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítható legyen a személyes adatok megfelelő biztonsága, különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szemben.

8. A beépített adatvédelem elve

   Az adatkezelő a tudomány és a technológia állása, a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során megfelelő technikai és szervezési intézkedéseket hajt végre. Ezen intézkedések célja az adatvédelmi elvek megvalósítása, az érintettek jogainak védelme, valamint az adatvédelmi jogszabályok további követelményeinek teljesítéséhez szükséges garanciák beépítése az adatkezelés folyamatába.

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

9. A felelősség elve

Az adatvédelmi szabályok megsértői – a vonatkozó jogszabályok rendelkezéseinek megfelelően – szabálysértési, polgári jogi és büntetőjogi, valamint a felhasználó jogviszonyának függvényében a fegyelmi felelősséggel tartoznak.

10. Az ellenőrzés elve

Az adatkezelő adatvédelmi tisztviselője köteles gondoskodni a vonatkozó jogszabályok és a szabályzat rendelkezéseinek betartásáról és rendszeresen ellenőrizni előírásainak érvényesülését, valamint szükség esetén kezdeményezni annak frissítését.

11. Elszámolhatóság

Az adatkezelő felelős a fenti alapelveknek való megfelelésért, továbbá a képesnek kell lennie a megfelelés igazolására, dokumentált alátámasztására.

V. Az érintettek jogai

1. tájékoztatáshoz való jog

Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintettek részére személyes adataik kezelését megelőzően megfelelő tájékoztatást adjon. A tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva szükséges nyújtani. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

Ha olyan adatvédelmi incidens következik be, amely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

2. Hozzáféréshez való jog

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz hozzáférést és az adatok kezelésével kapcsolatban tájékoztatást kapjon.

Az érintett jogosult megismerni az adatkezelő által kezelt személyes adatainak a körét, az adatkezelés célját és időtartamát, az adatok közlésének címzettjeit és a közlés célját, a másodlagos adatforrásból gyűjtött adatok forrását.

Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

3. Helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Az adatkezelő minden olyan címzettet tájékoztat a személyes adatok helyesbítéséről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére az adatkezelő tájékoztatást ad e címzettekről.

4. Törlés és elfeledtetés joga

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, ha a következő indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását és az adatkezelésnek nincs más jogalapja;
c) az érintett tiltakozik az adatkezelés ellen;
d) a személyes adatokat jogellenesen kezelték;
e) a személyes adatokat az adatkezelőre vonatkozó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
f) a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan kerül sor.

Az adatkezelő minden olyan címzettet tájékoztat a személyes adatok törléséről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére az adatkezelő tájékoztatást ad e címzettekről.
Ha az adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve a technikai intézkedéseket is – annak érdekében, hogy tájékoztassa az adatokat kezelő további adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy a személyes adatok másolatának, illetve másodpéldányának törlését.

5. Az adatkezelés korlátozásának joga
Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha a következők valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
b) az adatkezelés jogellenes és az érintett ellenzi az adatok törlését, ehelyett kéri azok felhasználásának korlátozását;
c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
d) az érintett tiltakozott az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

Az adatkezelő minden olyan címzettet tájékoztat a személyes adatok kezelésének korlátozásáról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére az adatkezelő tájékoztatást ad e címzettekről. Az adatkezelő azon érintettet, akinek a kérésére az adatkezelés korlátozásra került, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

6. Adathordozhatósághoz való jog

Az érintett jogosult arra, hogy az adatkezelő rendelkezésére bocsátott személyes adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa, vagy – ha ez technikailag megvalósítható – a személyes adatok adatkezelők közötti közvetlen továbbítását kérje. A fentiek feltétele, hogy az adatkezelés hozzájáruláson vagy szerződésen alapuljon, vagy az adatkezelés automatizált módon történjen.

Az adathordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű.

7. A tiltakozás joga

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozhasson személyes adatainak kezelése ellen, ha:

a) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
b) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

VI. Az érintetti kérelmek benyújtása

Az érintett a hozzáférés, helyesbítés, korlátozás, törlés, tiltakozás vagy adathordozás iránti kérelmét elektronikus úton nyújthatja be az adatkezelő adatvédelmi tisztviselőjének.

A kérelem benyújtása során a kérelmezőnek biztosítania kell, hogy személye egyértelműen azonosítható legyen és a kérelemben meg kell adnia a következő adatait:

- családi és utóneve,
- születéskori családi és utóneve,
- születési helye és ideje,
- anyja születési családi és utóneve,
- adóazonosító jele,
- adószáma (egyéni vállalkozók esetén),
- e-mail címe.

Az adatkezelő a kérelem beérkezésétől számított legrövidebb idő alatt, de legfeljebb 30 napon belül tájékoztatja az érintettet a kérelem nyomán meghozott intézkedésekről. Ez a határidő a kérelem összetettségére vagy a kérelmek számosságára tekintettel egy alkalommal, legfeljebb 60 nappal meghosszabbítható, amelyről adatkezelő a kérelmezőt az igény beérkezését követő 30 napon belül hivatalosan tájékoztatja.

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

VII. Az adatkezelő adatvédelmi intézményrendszere

A Társaság ügyvezetője határozza meg az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személyt.

Az adatkezelő tevékenységet az adatvédelmi tisztviselő támogatja, amelynek feladatai:

a) tájékoztat és szakmai tanácsot ad az adatkezelő és az adatfeldolgozó, továbbá az intézményi felhasználók részére az uniós és tagállami adatvédelmi rendelkezések szerinti kötelezettségekkel kapcsolatban;
b) ellenőrzi az adatvédelmi rendelkezéseknek, továbbá a személyes adatok védelmével kapcsolatos belső szabályoknak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi az adatvédelmi hatásvizsgálatok elvégzését;
d) együttműködik a Hatósággal;
e) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a Hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;
f) kivizsgálja a hozzá érkező bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelő vezetőjét, illetve javaslatot tesz a jogszerű adatkezelést megsértő személy felelősségre vonására;
g) szükség szerint javaslatot tesz jelen Szabályzat aktualizálására, módosítására;
h) vezeti az adatkezelő adatkezelési nyilvántartását;
i) vezeti az incidenskezelési nyilvántartást (jelen Szabályzat 1. számú mellékletében foglalt minta alapján);
j) együttműködik az adatkezelő adatvédelmi és adatbiztonsági intézményrendszerének kiépítésében, működtetésében, valamint ennek keretében a személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó intézkedések megtételében;
k) igény szerint bemutatja az adatkezelő adatvédelmi és adatbiztonsági intézményrendszerét.

Az adatkezelő adatvédelmi tisztviselőjének munkáját az adatkezelő és az adatfeldolgozó szakértői támogatják az adatbiztonsággal összefüggő kérdésekben. Az adatvédelmi tisztviselőhöz bármely érintett fordulhat.
A rendszerek adatfeldolgozói adatvédelmi feladataik ellátása tekintetében adatvédelmi tisztviselőt nevezhetnek ki.

VIII. Az adatfeldolgozó igénybevételének követelményei

1. Az adatfeldolgozó köteles megfelelő garanciát nyújtani az adatkezelés adatvédelmi jogszabályok követelményeinek való megfelelésére. Az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a felmerülő kockázatok mértékének megfelelő szintű adatbiztonságot garantálja.

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

2. Az adatfeldolgozó az adatkezelő előzetesen, írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változásokkal szemben kifogást emeljen.

3. Az adatfeldolgozó által végzett adatkezelés olyan – aza adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő és az adatfeldolgozó kötelezettségeit és jogait meghatározó – szerződés szabályozza, amely köti az adatkezelővel szemben.

4. Az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasítása szerint kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő. Ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha ezen értesítést az adott jogszabály fontos közérdekből tiltja.

5. Az adatfeldolgozó biztosítja, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak.

6. Az adatfeldolgozó az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti aza adatkezelőt abban, hogy teljesíteni tudja a kötelezettségét az érintettek jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében.

7. Az adatfeldolgozó segíti az adatkezelőt az adatkezelés biztonságát, az incidensek kezelését, az adatvédelmi hatásvizsgálatot, valamint az előzetes konzultációt illető kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat.

8. Az adatfeldolgozó az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő.

9. Az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti a tagállami vagy uniós adatvédelmi rendelkezéseket.

10. Az adatfeldolgozó az adatkezelő rendelkezésére bocsát minden olyan információt, amely az adatkezelő feladatai teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

IX. A felhasználók személyes adatainak kezelése

Az adatkezelő a felhasználók személyes adatait a rendszerek elérésére, használatára vonatkozó jogosultságok létesítése és megszüntetése, valamint azok használata (a rendszerekben történő munkavégzés és adatrögzítés) során, az adatvédelem elveinek figyelembevételével kezeli. Erről és a további adatkezelési célokról az adatkezelő köteles a felhasználót tájékoztatni.

A felhasználótól jogosultságainak beállításához csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely a személyhez fűződő jogát nem sérti és a felhasználói jogosultságok létesítése,

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

megszüntetése vagy rendeltetésszerű használata szempontjából lényeges. A rendszerek használatához szükséges jogosultságok beállításához és a felhasználói nyilvántartás vezetéséhez az érintett felhasználó közvetlenül vagy adott esetben a felhasználókat támogató munkatársak segítségével szolgáltat adatokat. A felhasználói nyilvántartás adatkörében beállt változásról az érintett köteles haladéktalanul, írásban bejelentést tenni.

A felhasználó hozzáférési jogosultságait jogviszonyuk, feladatkörük és a rendszerekben általuk végezhető adatkezelési műveletek teljesítéséhez szükséges mértékben kell megállapítani.

A támogatást igénylő, kedvezményezett felhasználó szavatol, hogy a támogatás igénylése és a projekt megvalósítása során benyújtott adatlapokon és mindezek mellékleteiben feltüntetett további ügyfelek (a kedvezményezett és esetleges konzorciumi partnereinek, szállítóinak, tulajdonosainak nevében és érdekében eljáró más személyek, valamint a projekt végső kedvezményezettjei) személyes adatainak a támogatást igénylő, kedvezményezett általi kezelése és a támogatói intézményrendszer számára történő rendelkezésre bocsátása megfelelő jogalappal és az érintettek megfelelő tájékoztatását követően történik.

A felhasználót az adatkezeléshez való hozzájárulásának beszerzése előtt dokumentáltan tájékoztatni kell a következőkről:

a) az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a neve és elérhetőségei;
b) az adatvédelmi tisztviselő neve és elérhetőségei;
c) a személyes adatok kezelésének a célja, jogalapja, tervezett időtartama;
d) az adatok közlése esetén annak címzettjei;
e) az adatkezeléssel kapcsolatos jogok érvényesíthetőségének lehetőségei;
f) az elérhető jogorvoslati lehetőségek;
g) az adatkezelő vagy harmadik fél jogos érdekei, ha az adatkezelés jogalapját e tényezők képezik;
h) a hozzájáruláson alapuló adatkezelés esetén a hozzájárulás visszavonása jogáról;
i) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása.

Az adatkezelő köteles biztosítani, hogy a felhasználó a róla kezelt személyes adatokat elektronikus úton megismerhesse.

X. Adatbiztonság

Az adatkezelő gondoskodik az adatok biztonságáról a rendszerekben tárolt adatállományok tekintetében. Az adatkezelő megteszi azon technikai és szervezési intézkedéseket, továbbá kialakítja azon eljárási szabályokat, amelyek az irányadó jogszabályokban előírt adatbiztonsági, adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatkezelő az adatokat alkalmazott eljárásaival és technikai eszközeivel védi a jogosulatlan hozzáférés, továbbítás és nyilvánosságra hozatal, valamint a megváltoztatás, törlés, megsemmisítés vagy véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Az adat- és információbiztonság szabályainak érvényesüléséről az adatkezelő az előírt dokumentumok kiadásával gondoskodik.

Az adatkezelő az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor köteles tekintettel lenni a technika mindenkori fejlettségére. Az adatkezelő több lehetséges adatvédelmi

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

és adatbiztonsági megoldás közül köteles azt választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

Az adatkezelő az informatikai védelemmel kapcsolatos feladatai körében gondoskodik különösen:

a) a jogosulatlan hozzáférés elleni védelmet biztosító intézkedésekről, ezen belül a szoftver, hardver eszközök védelméről, illetve fizikai védelemről;
b) a felhasználók hozzáférési jogainak felülvizsgálatáról;
c) az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről;
d) az adatállományok vírusok elleni védelméről;
e) az adatállományok, illetve az adatokat hordozó eszközök fizikai védelméről, ezen belül a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról.

A szabályzat hatálya alá tartozó személyek az általuk használt vagy birtokukban lévő, a rendszerekből származó személyes adatokat is tartalmazó adathordozókat és külső nyilvántartásokat – függetlenül az adatok rögzítésének módjától – kötelesek biztonságosan őrizni és védeni a jogosulatlan hozzáférés, továbbítás, nyilvánosságra hozatal, valamint a megváltoztatás, törlés, megsemmisítés, vagy a véletlen megsemmisülés és sérülés ellen.

XI. Adattovábbítás

Személyes adatok továbbítása során minden esetben meg kell győződni az adatkezelés jogalapjáról, kétség esetén jogi szakértő közreműködését kell kérni. Személyes adatot továbbítani csak abban az esetben lehet, ha annak jogalapja egyértelmű, célja és a címzett személye pontosan meghatározott. A továbbítást minden esetben dokumentálni kell oly módon, hogy annak menete és jogszerűsége bizonyítható legyen.

A jogszabály által előírt és szerződéses kötelezettségen alapuló adattovábbítást az adatkezelő köteles teljesíteni. A fentieken túl személyes adatot továbbítani az adatkezelő alátámasztható érdekmérlegelésén alapuló jogos érdekből lehet vagy, ha ahhoz az érintett egyértelműen hozzájárult. Annak érdekében, hogy a hozzájárulás bizonyítható legyen, azt dokumentálni kell. Az érintettek hozzájárulásához kötött adattovábbítás esetén az érintett a nyilatkozatát az adattovábbítás címzettje és célja ismeretében adja meg.

A rendszerek az adattovábbításokat naplózzák, valamint az adatkezelő a rendszerekből kinyert adatok továbbítását nyilvántartja annak megállapíthatósága érdekében, hogy a személyes adatokat kinek, milyen jogalappal és célból továbbítják.

Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha az Európai Bizottság határozatában megállapította, hogy a harmadik ország, a harmadik ország valamely területe, a harmadik ország egy vagy több meghatározott ágazata vagy a nemzetközi szervezet megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély. Az Európai Bizottság az Európai Unió Hivatalos Lapjában és annak honlapján közzéteszi az olyan harmadik országok, harmadik országon belüli területek és meghatározott ágazatok, valamint a nemzetközi szervezetek jegyzékét, amelyek esetén úgy ítélte meg, hogy biztosítják vagy többé nem biztosítják a megfelelő védelmi szintet.

A fenti határozat hiányában az adatkezelő csak abban az esetben továbbíthat személyes adatokat harmadik országba vagy nemzetközi szervezet részére, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

A fenti határozat és garanciák hiányában az adatkezelő a következő feltételek legalább egyikének teljesülése esetén továbbíthat adatokat harmadik országba vagy nemzetközi szervezet részére:

a) az érintett kifejezetten hozzájárult a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;
b) az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
c) az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
d) az adattovábbítás fontos közérdekből szükséges;
e) az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
f) az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
g) a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely a nyilvánosság vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

XII. Ellenőrzés

Az adatvédelemmel kapcsolatos jogszabályi előírások és belső szabályozási dokumentumok betartását az adatkezelő köteles folyamatosan ellenőrizni. Az adatvédelmi tisztviselő általános és célellenőrzéseket végez.

A végrehajtott ellenőrzésnek különösen a következőre kell kiterjednie:

a) a felhasználók betekintési és hozzáférési jogosultságának naprakészsége;
b) a jelszavak időnkénti cseréje;
c) e szabályzat, valamint az informatikai biztonságra vonatkozó szabályzatok rendelkezéseinek betartása.

Ha hivatalos ellenőrző szerv az adott időszakban végzett olyan ellenőrzést, amelynek a fentiek tárgyát képezték, akkor az adott tételre vonatkozó ellenőrzési kötelezettség ezzel az adott időszak vonatkozásában teljesült.

Az ellenőrzésre feljogosított az ellenőrzés céljára figyelemmel az ellenőrzés érdekében az adatkezelést végzőktől felvilágosítást kérhet, minden olyan adatkezelést megismerhet vagy abba betekinthet, amely az ellenőrzött adatkezelési tevékenységgel összefügg.

A Hatóság jogosult az adatkezelőnél ellenőrizni az adatvédelmi szabályok betartását, továbbá kivizsgálni a hozzá érkező bejelentésben foglaltakat.

A más közigazgatási vagy bírósági jogorvoslatok sérelme nélkül minden érintett jogosult arra, hogy panaszt tegyen a Hatóságnál, ha megítélése szerint az adatkezelő a rá vonatkozó személyes adatok kezelése során megsérti az adatvédelmi jogszabályok rendelkezéseit.

Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a Hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.

A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok – köztük a Hatóságnál történő panasztételhez való jog – sérelme nélkül, minden felhasználó hatékony bírósági jogorvoslatra

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

jogosult, ha megítélése szerint az adatkezelő a személyes adatainak a nem megfelelő kezelése következtében megsértette az adatvédelmi jogszabályok szerinti jogait.

Az adatkezelő a Hatósággal együttműködik, a Hatóság kérésének a Hatóság által megállapított határidőn belül eleget tesz, illetve, ha a Hatóság által tett megállapításokkal, a Hatóság által meghozott határozatokkal nem ért egyet, megteszi az adatvédelmi jogszabályokban meghatározott lépéseket.

A Hatóság elérhetőségei:

levelezési cím: 1534 Budapest, Pf. 834
cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.
telefon: +36-1-391-1400
fax: +36-1-391-1410
internet: www.naih.hu
e-mail: ugyfelszolgalat@naih.hu

XIII. Az adatkezelési nyilvántartás

Az adatkezelő adatkezelési nyilvántartást készít a felelősségébe tartozóan végzett adatkezelési tevékenységekről. Az adatfeldolgozók nyilvántartást vezetnek az adatkezelők nevében végzett adatkezelési tevékenységek minden kategóriájáról. A nyilvántartást írásban kell vezetni, ideértve az elektronikus formátumot is.

A belső adatvédelmi nyilvántartás célja annak alátámasztása, hogy az érintett mely adatkezelések alanya lehet és ezen adatkezelésnek melyek a jellemző elemei. Az adatkezelési nyilvántartás azonosítja az adatkezeléseket, azonban nem helyettesíti az érintett részletes tájékoztatását. Az adatkezelési nyilvántartást az adatvédelmi tisztviselő vezeti.

Az adatkezelési nyilvántartás naprakészsége érdekében az adatkezelő legalább évente megvizsgálja annak tartalmát.

XIV. Adatvédelmi hatásvizsgálat, előzetes konzultáció

Ha az adatkezelő által végzett adatkezelések valamely típusa – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

Az adatvédelmi hatásvizsgálatot különösen a következő adatkezelési kategóriák esetén kell elvégezni:

a) a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
b) a személyes adatok különleges kategóriáira vonatkozó adatkezelés;
c) a nyilvános helyek nagymértékű, módszeres megfigyelése;
d) az adatok nagy számban történő kezelése;
e) az adatkészletek egymásnak való megfeleltetése vagy összevonása;
f) a kiszolgáltatott helyzetben lévő érintettek adatainak kezelése;
g) új technológiai vagy szervezési megoldások innovatív használata és alkalmazása;

h) ha az adatkezelés megakadályozhatja, hogy az érintettek jogaikat gyakorolják, szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek.

A hatásvizsgálat elvégzése során figyelembe kell venni a Hatóság honlapján elérhető iránymutatásokat.

Ha az adatvédelmi hatásvizsgálat alapján megállapítható, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelő konzultál a Hatósággal.

XV. Az incidenskezelés eljárásrendje

Az adatvédelmi incidens a biztonság olyan sérülését jelenti, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre az adatvédelmi incidensek megelőzése és hatékony kezelése – ideértve az incidensek észlelését, feltárását és megszüntetését, dokumentálását és a releváns értesítések megtételét – érdekében.

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a Hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.
Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Ha a rendszer valamely felhasználójának a tudomására jut, hogy
a) adatvédelmi incidens történt;
b) olyan esemény vagy biztonsági incidens történt, amely felveti az adatvédelmi incidens lehetőségét

akkor az adatvedelmitisztviselo@szpi.hu elérhetőségen haladéktalanul tájékoztatnia kell az adatkezelőt. A Társaság egyéb mail címére küldött tájékoztatás nem minősül jelen szabályzat szerint adatvédelmi incidens bejelentésének.

Az adatvédelmi incidens bejelentése angol vagy magyar nyelven történhet.

A bejelentést az adatkezelő megvizsgálja a következő szempontok szerint:
a) információbiztonsági incidens megtörténte,
b) személyes adatok érintettsége.

Az adatkezelő adatvédelmi tisztviselője a bejelentéssel kapcsolatos álláspontjáról tájékoztatja az adatkezelőt, valamint az adatvédelmi incidenskezelési bizottság tagjait.

Az adatvédelmi incidenskezelési bizottság tagjai:
a) az adatvédelmi tisztviselő,
b) a bejelentéssel érintett szakmai és módszertani szervezeti egységek vezetői.

Az adatvédelmi incidenskezelési bizottság valamely tagjának távolléte vagy akadályoztatása esetén helyettesítés lehetséges.

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

Az adatvédelmi tisztviselő az incidens megtörténtének felderítésével kapcsolatos intézkedéseket és információkat kérhet az adatvédelmi incidenskezelési bizottság tagjaitól és esetlegesen az adatkezelő által igénybe vett adatfeldolgozóktól.

Az adatvédelmi incidenskezelési bizottság tagjai a rendelkezésre álló információk alapján és a Hatóság honlapján közzétett módszertani ajánlások figyelembe vételével értékelik a bejelentés részleteit, valamint:

a) megállapítást tesznek az incidens tényleges megtörténtét illetően, ha lehetséges;
b) értékelik az incidens személyiségi jogokra vonatkozó kockázatait, ha lehetséges;
c) az incidens megszüntetéséhez szükséges szervezési és technikai intézkedéseket fogalmaznak meg;
d) az incidens megtörténtének felderítésével kapcsolatos intézkedéseket határoznak meg, ha az incidens fennállása nem egyértelmű.

Az adatvédelmi incidenskezelési bizottság tagjai döntési javaslatot is tartalmazó összegző jelentést készítenek a bejelentés tekintetében. Az adatvédelmi incidenskezelési bizottság döntési javaslatai kiterjednek a Hatóság és az érintettek tájékoztatására.

A döntési javaslat a Hatóság tájékoztatása tekintetében lehet:

a) a Hatóság teljes körű tájékoztatása;
b) a Hatóság tájékoztatása nem szükséges;
c) a Hatóság részleges tájékoztatása, ha incidens történt, de a Hatóság tájékoztatásához szükséges minden információ nem áll rendelkezésre 72 órán belül;
d) a Hatóság halasztott és a késedelem indokát tartalmazó teljes körű tájékoztatása, ha incidens történt, de a Hatóság tájékoztatásához szükséges minden információ nem áll rendelkezésre 72 órán belül.

A döntési javaslat az érintettek tájékoztatása tekintetében lehet:

a) az érintettek tájékoztatása szükséges;
b) az érintettek tájékoztatása nem szükséges.

A döntési javaslatokat a bejelentést követő 48 órán belül ki kell dolgozni. Ha a bejelentés alapján az adatvédelmi incidens megtörténte nem egyértelműsíthető, akkor ennek azonosításához haladéktalanul vizsgálatot szükséges lefolytatni, a javaslattételre pedig az incidens azonosítását követően 48 órán belül van lehetőség.
Az adatvédelmi incidenskezelési bizottság javaslatai alapján az adatvédelmi tisztviselő összegző jelentést készít, amely tartalmazza az egyes bizottsági tagok javaslatait, valamint a bizottsági álláspontot.

Az összegző jelentés alapján az adatkezelő képviselője a bejelentést, vagy az incidens azonosítását követő 60 órán belül:

a) jóváhagyja az adatvédelmi incidenskezelési bizottság összesített javaslatát;
b) indoklással más döntést hoz a hatósági bejelentés és az érintettek tájékoztatását illetően.

Az adatkezelő képviselőjének döntése szerint az adatvédelmi tisztviselő megteszi a tájékoztatással kapcsolatban szükséges intézkedéseket.

Ha a vizsgálatok alapján tényleges incidens történt, az adatvédelmi tisztviselő az 1. mellékletben meghatározott módon rögzíti annak adatait.

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

XVI. Kártérítés és sérelemdíj

Minden olyan személy, aki az adatvédelmi jogszabályok megsértése eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult a vonatkozó jogszabálynak megfelelően.

Ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett az adatkezelőtől sérelemdíjat követelhet.

Az érinettel szemben az adatkezelő felel az adatfeldolgozó által okozott kárért és az adatkezelő köteles megfizetni az érintettnek az adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be az adatvédelmi jogszabályokban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

Az adatkezelő, illetve az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

Nem kell megtéríteni a kárt és nem követelhető sérelemdíj, ha a kár a károsult vagy a személyiségi jog megsértésével okozott jogsérelem az érintett szándékos vagy súlyosan gondatlan magatartásából származhatott.

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

1. számú függelék a …./2020. számú ügyvezetői utasításhoz

INCIDENSKEZELÉSI JEGYZŐKÖNYV

az adatvédelmi incidens sorszáma	az adatvédelmi incidens időpontja és körülményei	az adatvédelmi incidens tárgya	az érintettek száma és köre	az incidens kezelésére hozott intézkedések	az incidens kockázati besorolása	a Hatóság értesítésének időpontja	az érintett értesítésének időpontja	egyéb releváns információ

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

Annex no. 2 to Managing Director's Order No. _____.

Data protection and data processing Regulation of the INTERREG+ IT system

COMPANY NAME:	**SZÉCHENYI PROGRAMME OFFICE NONPROFIT LLC.**
REGISTERRED OFFICE:	H-1053 Budapest, Szép utca 2. IV. emelet
TAX NUMBER:	18080313-2-41
COMPANY REGISTRATION NUMBER:	01-09-916-308
hereinafter referred to as:	Company

This Managing Director's Order regulates the general data protection and data management rules of the data managed in the INTERREG + IT System.

Leader of the organisational unit in charge of professional content:	in charge of codification:	Attestation of legal comformity:	approved by:
..... dr. Futó Adrienn international director	..... dr. Káplár Anikó Head of Legal Unit	..... dr. Dékány Anita legal director Attestation on financial conformity: ..... Biró Teréz financial director	..... dr. Nyerges Judit Ildikó data protection officer
Subject to Section (2) Article 17 of Act I of 2012, The employer's internal policy shall be considered delivered if published by means considered customary for, and commonly known in, the area.			

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

Data protection and data processing Regulation of the INTERREG+ IT system

I. Purpose of the regulation

With regard to INTERREG+ IT system the secure processing of personal data, the application of principles of data processing and the rights of data subjects shall be ensured for which purpose the controller shall implement appropriate technical and organizational measures.
The purpose of the regulation is the controller to comply with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the Act CXII of 2011 on information self-determination and freedom of information (hereinafter referred to as 'Info Act').

II. Scope of the regulation

Personal scope: the personal scope of the regulation extends to the controller, the processor on behalf of the controller and all users processing data with regard to the system.

Material scope: the material scope of the regulation extends to the processing on behalf of the controller, the processor and all users processing data – of personal data recorded in the system – wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are recorded in the system.

III. Definitions

a) processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

b) processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

c) controller: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

d) personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

e) data subject: identified or identifiable natural person on the basis of any information;

f) recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

g) third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

h) Authority: National Authority for Data Protection and Freedom of Information;

i) personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

IV. Data protection principles

1. Principle on the protection of fundamental rights

The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

2. Lawful and fair processing of data and principle of transparency

Any processing of personal data should be lawful and fair and it should be transparent to natural persons that personal data concerning them are collected. Any processing of personal data is only considered lawful if at least one of the following conditions are met:

a) the natural person concerned has given consent to the processing of his or her personal data for one or more specific purposes;
b) the processing of data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) the processing of data is necessary for compliance with the legal obligation to which the controller is subject;
d) the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person;
e) the processing of personal data for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3. Principle of purpose limitation

Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

4. Principle of data minimization

   Personal data for processing shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5. Principle of accuracy
   Personal data shall be accurate and, where necessary, kept up to date. The controller must take every reasonable step to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

6. Principle of storage limitation

   Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by data protection regulations in order to safeguard the rights and freedoms of the data subject.

7. Principle of integrity and confidentiality

   Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. Principle of data protection by design

   Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures. These measures are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

9. Principle of liability

   In case of the infringement of data protection regulations – in accordance with the provisions of the relevant regulations – those concerned shall render themselves liable to disciplinary action depending on their administrative, civil and criminal law and user relationship.

10. Principle of monitoring

    The data protection officer on behalf of the controller shall ensure the compliance with the provisions of the relevant regulation and rules and regularly check the application of regulation initiating the amendment of regulation if necessary.

11. Accountability

    The controller shall be responsible for, and be able to demonstrate compliance with the abovementioned principles.

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

V. Rights of data subjects

1. Principle on rights of information

The controller shall take appropriate measures to provide any information and any communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person.

2. Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information.

The data subject shall have the right to access information about the categories of personal data concerned, the purposes and period of processing, the recipients to whom the personal data will be disclosed, and where the personal data are not collected from the data subject, any available information as to their source.

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

3. Right to certification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

The controller shall communicate any rectification of personal data carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients at request.

4. Right to erasure and right to be forgotten

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

c) the data subject objects to the processing;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services.

The controller shall communicate any erasure of personal data carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.
Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

5. Right to restriction of processing

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

The controller shall communicate any restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients. The controller shall inform the data subject at whose request the restriction was performed about the lifting of restriction beforehand.

6. Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller or – where technically feasible – enquire transmitted directly from one controller to another. The conditions of the above are that the processing is based on consent or on a contract or the processing is carried out by automated means.

The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest.

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

7. Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, if:

a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
b) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

VI. Submission of data subject request

The data subject shall have the right to submit a request to the data protection officer on behalf of the controller in relation to access, rectification, restriction, erasure, object or data portability.

The data subject submitting a request shall ensure that his or her identity is clearly identifiable and provide the following data in the request:

- surname and first name
- surname and first name at birth
- place and date of birth
- mother's surname and first name at birth
- tax identification number
- tax number (in the case of self-employed)
- e-mail address.

The controller shall provide information on action taken on a request to the data subject without undue delay and in any event within 30 days of receipt of the request. That period may be extended once by 60 days where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within 30 days of receipt of the request,

VII. Institutional system of the controller

The Managing Director of the Company assigns the data protection organization, task and responsibilities related to data protection and appoints the person for data protection supervision.

On behalf of the controller the data protection officer shall have the following tasks related to data processing:

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c) to provide advice where requested as regards the data protection impact assessment and monitor its performance;
d) to cooperate with the Authority;

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

e) to act as the contact point for the Authority on issues relating to processing, including the prior consultation and to consult, where appropriate, with regard to any other matter;
f) to investigate notifications, in case of unauthorized data processing detected, to call the head of controller to terminate the unauthorized processing and to propose to hold liable the person who breaches lawful data processing
g) to initiate the amendment, modification of the present Regulation if necessary;
h) to keep a data protection record on behalf of the controller;
i) to keep the incident management report (in accordance with the template in Annex 1 of the present Regulation);
j) to cooperate in the organization and management of the data processing and data protection organization system and to take necessary measures to ensure the necessary personal, material and technical conditions for the operation thereof;
k) to introduce the data protection and data security system of the controller.

The controller and processor shall support the data protection officer in performing the tasks related to data protection issues. Any data subject may contact the data protection officer.
The processors of the systems in performing their tasks may appoint a data protection officer.

VIII. Requirements for engaging data processor

1. The processor shall take the proper measures to ensure the compliance with the requirement of data protection law. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

4. The processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

5. The processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6. The processor taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

7. The processor assists the controller in security of data processing, management of incidents and in performing tasks related to data protection impact assessment and prior consultation taking into account the nature of processing and the information available for the processor.

8. The processor at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.

9. The processor shall immediately inform the controller if, in its opinion, an instruction infringes Union or Member State data protection provisions.

10. The processor makes available to the controller all information necessary to demonstrate compliance with the obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

IX. Processing of user's personal data

The controller shall process the user's personal data in system access, establishment and termination of rights to use and the use of system (working and data recording int he systems) in accordance with data protection principles. The controller is obliged to inform the user about the above and further data management purposes.

In order to establish his / her rights, the user may only be required to make a statement or provide information that does not infringe his / her rights and is relevant to the establishment, termination or proper use of the user rights. In order to set the rights required to use the systems and to operate the user register, the user concerned shall provide data directly or, where appropriate, with the assistance of user support colleagues. The data subject is obliged to report the change in the data scope of the user register immediately in writing.

The user's access rights must be established to the extent necessary to perform their legal relationship, their responsibilities and the data processing activities they may perform in the systems.

The beneficiary submitting payment application guarantees that the personal data of additional partners (other persons acting on behalf and for the benefit of the Beneficiary and any consortium partners, suppliers, owners and final beneficiaries of the project) listed in the data sheets submitted in the payment application and project implementation documents and their annexes is processed by the beneficiary and transferred to the supporting institutional system on an appropriate legal basis and after appropriate information has been provided to the data subjects.

The user must be informed in a documented manner of the following before obtaining his or her consent to data processing:

a) the name and contact details of the controller and, where applicable, the name and contact details of the controller's representative;
b) the name and contact details of the data protection officer;
c) the purpose, legal basis and envisaged duration of personal data processing;
d) the recipients to whom the personal data have been or will be disclosed;
e) the enforcement possibilities related to data processing;
f) the available legal remedies;
g) the legitimate interests of the controller and the third party, provided that they are the legal basis of the data processing;
h) the right to consent in the case of consent-based data processing;

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

i) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

The controller ensures the users to access the personal data processed about him or her electronically.

X. Security of processing

The controller ensures the security of data related to the records in the system. The controller takes the technical and organizational measures and develops rules of procedures that are necessary to comply with the relevant data security, data and confidentiality rules.

The controller takes measures to ensure the appropriate level of security in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or inaccessibility due to alteration in the technique used.

The controller provides the relevant documents to ensure the application of data and information security rules.

The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures taking into account the state of art. The controller shall ensure several possible data protection and data security solutions that provide a higher level of protection unless this involves disproportionate effort.

The tasks of the controller related to IT protection involves in particular:

a) measures taken to protect against unauthorized access, involving the protection of software and hardware instruments and physical protection;
b) revision of the access rights of users;
c) possible measures taken to default set of data files, involving the regular backup and the separate, secure handling of copies;
d) protection of data files against viruses;
e) physical protection of data files and data carriers, involving protection against fire, water damage, lightning or other elemental damage, and the recovery of damage resulting from such events.

Those persons covered by the current Regulation shall ensure the safe storage of the data carriers and external records used by or held by them containing personal data from the system – regardless the method of recording – against unauthorized access to, transmission, disclosure of, alteration, deletion, accidental or unlawful destruction and damage.

XI. Transfers of personal data

When transferring personal data, the legal basis for data processing must be ascertained in all cases, in case of doubt, the assistance of a legal expert should be sought. Personal data may be transferred only if the legal basis is clear and the purpose and recipient is clearly defined. The transfer shall be recorded in such way that the process and legality thereof is evident.

A transfer of personal data required by law and based on a contractual obligation shall be performed by the controller. Personal data may be transferred by the legitimate interest based on a substantiated balance of interests of the controller or if the data subject unambiguously consents thereto. The consent can be demonstrated only if documented. In the case of the personal data transfer related to consent the statement of data subject is provided with the acknowledgement of the recipient and purpose thereof.

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

The systems record transfers and the controller records transfers from the system in order to determine to whom on what legal basis and purpose the personal data are transferred to.

A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation. The Commission shall publish in the *Official*

Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

In the absence of the above decision the controller shall only transfer personal data to a third country or to an international organisation, if the controller or processor provided appropriate safeguards and only with the condition that rights and effective remedies are available to the data subjects.

In the absence of an adequacy decision above or of appropriate safeguards, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
d) the transfer is necessary for important reasons of public interest;
e) the transfer is necessary for the establishment, exercise or defence of legal claims;
f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

XII. Verification

The compliance with legal provisions and internal regulatory documents must be continuously verified by the data controller. The data protection officer performs general and target verification.

The verification shall assess in particular:

a) the up-to-datedness of users' access and access rights;
b) from time to time change of passwords;
c) compliance with the present Regulation and the provisions of IT security regulations.

In case an official authority conducted a verification mission in the period of which the above were subject, the verification obligation for the given item shall be considered fulfilled in the given period.

The authorized regarding the purpose of verification may request information from data controllers and may have an insight in data processing which is related to the verified data processing activity.

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

The Authority is entitled to check compliance with data protection rules at the data controller and to investigate the content in the notification received.

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes the provisions of data protection regulations.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy against a legally binding decision of the Authority concerning them.

Without prejudice to any available administrative or non-judicial remedy, - including the right to lodge a complaint with the Authority – the data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted have been infringed as a result of the processing of his or her personal data in non-compliance with the provisions of data protection regulations.

The controller shall cooperate with the Authority and comply with the Authority's request within a time limit set by the Authority and in case of disagreement with the findings shall take the appropriate steps set out in data protection legislation.

Contact details of the Authority:

Postal address: 1534 Budapest, Pf. 834
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Telephone: +36-1-391-1400
Fax: +36-1-391-1410
Website: www.naih.hu
E-mail: ugyfelszolgalat@naih.hu

XIII. Data processing register

Each controller shall maintain a record of processing activities under its responsibility. Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller. The records shall be in writing, including in electronic form.

The purpose of the internal data processing register is to demonstrate which data processing the data subject may be affected by and what the elements of these processing are. The data processing register identifies data processing however, it does not replace the detailed information of the data subject. The data processing register shall be kept by the data protection officer.

In order to keep the data processing register up to date, the data controller shall review its content at least annually.

XIV. Data protection impact assessment, prior consultation

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

A data protection impact assessment shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) data processing for special categories of personal data;
c) a systematic monitoring of a publicly accessible area on a large scale
d) processing large amounts of data;
e) matching or merging data sets;
f) data processing of vulnerable data subjects;
g) innovative use and application of new technological or organizational solutions;
h) the processing may prevent the data subjects from exercising their rights, using services or enforcing a contract.

The guidance available on the Authority website shall be taken into account in the process of impact assessment.

The controller shall consult the Authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

XV. Incident management procedure

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The controller shall implement appropriate technical and organizational measures to prevent and effectively manage data protection incidents including incident detection, detection and resolution, documentation and relevant notifications.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
Where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

In case a user becomes aware of
a) the occurrence of data protection incident;
b) an event or security incident occurred that raises the possibility of a data protection incident

the controller shall be informed without delay via the e-mail address dataprotectionofficer@szpi.hu. Any notification sent to other e-mail addresses of the Company shall not be considered as notification on data protection incident.

The data protection incident may be reported in English or Hungarian.

The notification is examined by the controller according to the following criteria:
a) the existence of information security incident,
b) personal data concerned.

The data protection officer of the controller shall inform the controller and the members of the data protection incident management committee of his/her position on the notification.

MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Strukturális és Beruházási Alapok
BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

The members of the data protection incident management committee are:

a) data protection officer,
b) the heads of the professional and methodological departments concerned by the notification.

Replacement is possible in the absence or impediment of a member of the data protection incident management committee.

The data protection officer may request measures and information relating to the detection of an incident from the members of the data protection incident management committee and, where appropriate, from the data processors employed by the controller.

The members of the data protection incident management committee shall assess the details of the notification on the basis of the information available and taking into account the methodological recommendations published on the Authority's website and:

a) establish, where possible, the actual occurrence of the incident;
b) assess the personal rights risks of the incident, if possible;
c) formulate the organizational and technical measures necessary to deal with the incident;
d) take measures to detect the occurrence of the incident if the existence of the incident is not clear.

The members of the data protection incident management committee shall prepare a summary report on the notification, including a proposal for a decision. The data protection incident management committee's decision proposals include informing the Authority and data subjects.

The proposed decision to notify the Authority may be:

a) full notification provided to the Authority;
b) notification to the Authority is not required;
c) partial notification to the Authority if an incident has occurred but all information necessary to inform the Authority is not available within 72 hours;
d) full notification to the Authority of the delay and the reason for the delay if an incident has occurred but all the information necessary to inform the Authority is not available within 72 hours.

The proposed decision to notify the data subjects may be:

a) notification to data subjects is required;
b) notification to data subjects is not required.

Proposals for decisions must be made within 48 hours of notification. If, on the basis of the report, the occurrence of the data protection incident cannot be clarified, an investigation must be carried out immediately to identify it, and a proposal can be made within 48 hours after the identification of the incident.
On the basis of the proposals of the data protection incident management committee, the data protection officer shall prepare a summary report containing the proposals of each committee member as well as the position of the committee.

Based on the summary report, the representative of the data controller shall, within 60 hours of the notification or identification of the incident:

a) approve the overall proposal of the data protection incident management committee;
b) take a different decision with regard to the notification and the information of the data subjects concerned, giving reasons.

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

At the discretion of the controller's representative, the data protection officer shall take the necessary measures with regard to the information.

If an investigation has led to an actual incident, the data protection officer shall record its details as set out in Annex 1.

XVI. Right to compensation and damages

Any person who has suffered material or non-material damage as a result of an infringement of data protection regulations shall have the right to receive compensation from the controller or processor for the damage suffered in accordance with relevant legislation.

If the controller violates the data subject's right to privacy by unlawfully processing the data subject's data or by violating data security requirements, the data subject may claim damages from the controller.

Against the data subject, the controller is liable for the damage caused by the processor and the controller is also obliged to pay the data subject damages in the event of a personal data breach caused by the processor. The processor shall only be liable for damages caused by the data processing if he or she has not complied with the obligations specified in the data protection legislation, which are specifically imposed on the processors, or if he or she has disregarded or acted contrary to the controller's lawful instructions.

The controller or processor shall be released from liability if he or she proves that he or she is not liable in any way for the event giving rise to the damage.

No damages shall be payable and no damages shall be claimed if the damage was caused by the intentional or grossly negligent conduct of the injured party or the breach of the right to privacy.

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

Annex 1 to Managing Director's Order No...../2020

INCIDENT MANAGEMENT RECORDS

serial number of incident	date and circumstances of incident	subject of the incident	the range and number of 'data subject'	the potential consequences of the incident	measures taken to deal with the incident	classification of risk	date of notification to the Authority	date of notification to the 'data subject'	other relevant information

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Strukturális és Beruházási Alapok

BEFEKTETÉS A JÖVŐBE

Széchenyi Programiroda Nonprofit Kft.
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu