2018 - HAT / 15

15...../2018. számú ügyvezetői utasítás / *Order of the Managing Director No.15...../2018.*

1. Jelen utasítás 1. számú mellékleteként magyar nyelven, 2. számú mellékleteként angol nyelven kiadom a **90/2017. számú ügyvezetői utasítással kiadott, a Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Korlátolt Felelősségű Társaság adatvédelemre és adatbiztonságra vonatkozó szabályzatának (a továbbiakban: Szabályzat) módosítását.** */ I hereby publish the amendment of the Bylaw on data protection and data security of Széchenyi Programme Office Consulting And Service Nonprofit Limited Liability Company published by the Managing Director's order no. 90/2017., in Hungarian version as Annex no. 1. and in English version as Annex no. 2. of the present Managing Director's order.*

2. Jelen ügyvezetői utasítás 2018. május 25. napján lép hatályba azzal, hogy a Szabályzat jelen módosítással nem érintett részei változatlan tartalommal hatályban maradnak. */ The present managing director's order shall enter into force on 25th may 2018., the parts that are not covered by this Amendment will remain in force with unchanged content.*

3. Jelen utasítás a Társaság valamennyi munkavállalója és szervezeti egysége számára kötelező érvényű./ *The present bylaw is binding for all employees and departments of the Company.*

Budapest, 2018. május 24./ 24. may 2018.

Széchenyi Programiroda
Tanácsadó és Szolgáltató Nonprofit
Korlátolt Felelősségű Társaság
Adószám: 18080313-2-41
Tel: 327-08-30, fax: 327-08-31
1053 Budapest, Szép utca 2. IV. emelet

.....

Schultz Gábor/*Gabor Schultz*
ügyvezető/*managing director*

1. számú melléklet a 16./2018. számú ügyvezetői utasításhoz

A Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Korlátolt Felelősségű Társaság adatvédelemre és adatbiztonságra vonatkozó szabályzatának módosítása

1. A Szabályzat II. 1. pontja helyébe az alábbi rendelkezés lép:

„A Társaság a Szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII törvény (a továbbiakban: Infotv.) 15. §-ában meghatározott tájékoztatáshoz való jog, valamint 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 (általános adatvédelmi rendelet) szóló 2016/679 európai parlamenti és tanácsi rendeletben (a továbbiakban: GDPR) foglalt kötelezettségek megvalósulását."

2. A Szabályzat III. pontja helyébe az alábbi rendelkezés lép:

„III. A szabályozás során felhasznált jogszabályok és rövidítéseik

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

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

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

GDPR az Európai Parlament és a Tanács 2016. április 27-i 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 (általános adatvédelmi rendelet) szóló 2016/679 rendelete"

3. A Szabályzat VI. 2. pontja helyébe az alábbi rendelkezés lép:

„A Társaság adatvédelmi rendszerének felügyeletét az ügyvezető látja el, az általa kijelölt adatvédelmi tisztviselő útján."

4. A Szabályzat az alábbi VI/A. ponttal egészül ki:

VI/A. Adatvédelmi hatásvizsgálat

„1. Ha az adatkezelés valamely típusa figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek. Az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.

2. Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

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 kategóriái vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése;

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

3. A hatásvizsgálat kiterjed legalább:

a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
c) az az érintett jogait és szabadságait érintő kockázatok vizsgálatára;
d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat."

5. A Szabályzat VII. 1. pont d) alpontja helyébe az alábbi rendelkezés lép:

„támogatja az adatvédelmi tisztviselő tevékenységét;"

6. A Szabályzat VII. 2. pontja helyébe az alábbi rendelkezés lép:

„Az adatvédelmi tisztviselő az adatvédelemmel kapcsolatosan:

a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az Infotv., a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségekkel kapcsolatban;
b) ellenőrzi az a) pontban hivatkozott jogszabályok, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
d) együttműködik a felügyeleti hatósággal;
e) az adatkezeléssel összefüggő ügyekben – ideértve az előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóságnál, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi."

7. A Szabályzat IX. 3. és 4. pontjai helyébe az alábbi rendelkezések lépnek:

„3. A szervezeti egység vezetője az érintett személyes adatának kezelésével összefüggő kérelmének 2. pont szerinti áttételétől számított 3 napon belül közérthető formában választ készít elő, amelyet véleményezés céljából haladéktalanul megküld az adatvédelmi tisztviselőnek.

4. Az adatvédelmi tisztviselő az előkészített választ haladéktalanul megvizsgálja és az általa jóváhagyott választervezetet - aláírás és az érintett részére történő megküldés céljából - azonnal továbbítja az ügyvezetőnek."

8. A Szabályzat IX. 10-12. pontjai helyébe az alábbi rendelkezések lépnek:

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

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

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

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

9. *A Szabályzat az alábbi IX/A. és IX/B. ponttal egészül ki:*

„IX/A. Az adatvédelmi incidens

1. az „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.

2. Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti 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.

3. Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

4. A 2. pontban hivatkozott bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

5. Amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

6. Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

IX/B. Az érintett tájékoztatása az adatvédelmi incidensről

1. 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.

2. Az 1. pontban hivatkozott, az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a IX/A. 4. pontjában foglalt információkat és intézkedéseket.

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

3. Az érintettet nem kell az 1-2. pontban foglaltak szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat

b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, ún. magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

4. Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a 3. pontban hivatkozott feltételek valamelyikének teljesülését.

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

Amendment of Bylaw on data protection and data security of Széchenyi Programme Office Consulting And Service Nonprofit Limited Liability Company

1. ***Point 1 of Chapter II of the Bylaw shall be replaced by the following provisions:***

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

2. ***Chapter III of the Bylaw shall be replaced by the following provisions:***

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

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

3. ***Point 2 of Chapter VI of the Bylaw shall be replaced by the following provisions:***

„The supervision of the data protection system of the Company is fulfilled by the managing director through the data protection officer appointed by him."

4. ***Chapter VI/A. shall be added to the Bylaw:***

VI/A. Data protection impact assessment

„1. Where a type of processing 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. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the data protection officer, when carrying out a data protection impact assessment.

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

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) processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences.

HUNGARIAN GOVERNMENT
European Union
European Structural and Investment Funds
INVESTING IN YOUR FUTURE

Széchenyi Programme Office Nonprofit LLC
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

3. *The assessment shall contain at least:*

a) *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
b) *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
c) *an assessment of the risks to the rights and freedoms of data subjects;*
d) *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned."*

5. *Paragraph d) of Point 1 of Chapter VII of the Bylaw shall be replaced by the following provisions:*

„support the activity of the data protection officer"

6. *Point 2 of Chapter VII of the Bylaw shall be replaced by the following provisions:*

„Related to data protection the data protection officer shall have the following tasks:

a) *to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the Act, the GDPR this Regulation and to other Union or Member State data protection provisions;*
b) *to monitor compliance with law determined in paragraph a) 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 supervisory authority;*
e) *to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.*

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing."

7. *Point 3 and 4 of Chapter IX of the Bylaw shall be replaced by the following provisions:*

„3. The head of organizational unit shall prepare an answer in an easily understandable form within 3 days from the reference under point 2. concerning the request regarding the personal data processing of the data subject which shall be sent to the data protection officer immediately for his opinion.

4. The data protection officer immediately examines the prepared answer and sends the approved draft to the managing director for signing and for the purpose to send it to the data subject."

8. *Point 10-12 of Chapter IX of the Bylaw shall be replaced by the following provisions:*

„10. For the period of adjudication of the objection of the data subject - but no longer than 5 days - the head of the organizational unit processing data shall suspend the processing, shall examine the merits of the objection, shall draft the decision which he shall send to data protection officer for his opinion. Data subject shall be informed about the decision within the deadlines laid down in point 5. of this chapter by the managing director acting on behalf of the data controller as to Art. 21 (2) of the Act.

11. In case the objection is justified, the head of the organizational unit processing data shall act according to the provisions of the Act.

HUNGARIAN GOVERNMENT
European Union
European Structural and Investment Funds
INVESTING IN YOUR FUTURE

Széchenyi Programme Office Nonprofit LLC
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

12. In case the adjudication of the case lacks clarity when data subject exercises his rights, the head of the organizational unit processing data shall send the documents of the case with his opinion regarding the case to the data protection officer requiring his statement who shall fulfill this request within three days."

9. ***Chapter IX/A. and IX/B. shall be added to the Bylaw:***

„IX/A. Personal data breach

1. „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.

2. 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 competent supervisory 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.

3. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

4. The notification referred to in point 2 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

6. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

IX/B. Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in point 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in point 4 of Chapter IX/A.

3. The communication to the data subject referred to in point 1-2 shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption

HUNGARIAN GOVERNMENT
European Union
European Structural and Investment Funds
INVESTING IN YOUR FUTURE

Széchenyi Programme Office Nonprofit LLC
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu

b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in point 3 are met.

HUNGARIAN GOVERNMENT
European Union
European Structural and Investment Funds
INVESTING IN YOUR FUTURE

Széchenyi Programme Office Nonprofit LLC
1053 Budapest, Szép u. 2. IV. em.
info@szpi.hu www.szpi.hu