ADATKEZELÉSI SZABÁLYZAT

Swicon IT Services Kft

Hatályos: 2018.06.01

Legutóbbi módosítás: 2024.09.10

Tartalom

1. Bevezetés

Jelen adatvédelmi szabályzatot az **Swicon IT Services Kft.** adja ki adatkezelési tevékenysége szabályozása céljából. A szabályzat rendszeresen aktualizálásra kerül a hatályos hazai és Európai Uniós jogszabályoknak való folyamatos megfelelés érdekében. Az adatvédelmi szabályzat mindenkor hatályos változata megtekinthető a https://swicon.com/it-services/ weboldalon, valamint a recepción nyomtatott formátumban is elérhető.

2. Az adatkezelő adatai

Adatkezelő megnevezése: **Swicon IT Services Korlátolt Felelősségű Társaság** (továbbiakban: ITIL-PRO)

Székhely:	**1031 Budapest, Záhony utca 7.**
Telefon:	+36 (1) 883-9866
Email:	adatvedelem@swicon-itservices.com
Honlap:	https://swicon.com/it-services/
Cégjegyzék szám:	**01-09-739887**

Az adatvédelemi tevékenységeket összefogó munkatárs, ún. adatvédelmi munkatárs:

Tündik László

3. A szabályzat célja

Jelen adatkezelési szabályzat célja, hogy meghatározza az ITIL-PRO által kezelt személyes adatokkal kapcsolatos legfontosabb szabályokat, az adatkezelésekre vonatkozó információkat és alapelveket.

Az adatvédelmi szabályzat célja elsősorban annak biztosítása, hogy az ITIL-PRO megfeleljen a hatályos jogszabályok adatvédelemmel kapcsolatos rendelkezéseinek, így különösen, de nem kizárólagosan

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) 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)
- a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló 2008. évi XLVII. törvény,
- a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény,
- a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény rendelkezéseinek.

4. A szabályzat hatálya

4.1 Időbeli hatály

Jelen szabályzat az eredeti, 2018. június 1. napjától érvényes dokumentum módosításaként, annak értelmében 2024. szeptember 10. napjától hatályos.

4.2 Személyi hatály

Jelen szabályzat hatálya kiterjed

- az Adatkezelőre (Swicon IT Services Kft)
- az adatkezelő Munkavállalóira és Partnereire; valamint
- minden további természetes személyre, akinek adatait e szabályzat hatálya alá tartozó adatkezelések érintik.

4.3 Tárgyi hatály

Jelen szabályzat hatálya kiterjed az Adatkezelő bármely szervezeti egységében folytatott, személyes adatokat érintő adatkezelésre, függetlenül attól, hogy az elektronikusan és/vagy papíralapon történik.

5. Tájékoztatás az adatkezelésről

Az adatkezelő kötelessége tájékoztatni az érintetteket személyes adataik kezeléséről.

Jelen szabályzat elválaszthatatlan részét képezik a mellékletekben található adatvédelmi tájékoztatók. A tájékoztatók részletesen tartalmazzák az egyes adatkezelésekre vonatkozó fontos információkat, így az adatkezelési tevékenység és a folyamat leírását, az érintettek megnevezését, a kezelt adatok körét, az adatok megőrzésének előre látható időtartamát, az adatkezelések jogalapját és céljait. A tájékoztatók tartalmazzák az adatok biztonsága érdekében alkalmazott szabályokat, az érintettek jogait és jogérvényesítési lehetőségeit.

Jelen adatkezelési szabályzat kizárólag ezekkel az információkkal együtt érvényes.

6. Az adatkezelés alapvető elvei

A személyes adatok:

- kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);
- gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet („célhoz kötöttség”);
- az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”);
- pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság”);
- tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé („korlátozott tárolhatóság”);
- kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő

biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

Az adatkezelő felelős a fentieknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

7. Felelősségek

Az ITIL-PRO az adatkezelési tevékenységeiről nyilvántartást készített, mely adatcélonként tartalmazza az adatkezelési tevékenységeket és a hozzájuk kapcsolódó információkat (az adatkezelési tevékenység megnevezését és célját, az érintetteket, adat forrását, adatfajtákat, adatkezelés alapját (pl. hozzájárulás, szervezet jogos érdeke, jogszabály), a tárolási időt, a tárolás módját, az adattovábbítás címzetteit (ha vannak)). Valamennyi adatkezelési tevékenység esetén meghatároztunk felelőst, aki érdemi döntéseket tud hozni az adatkezeléssel kapcsolatosan.

A tevékenységünk során végrehajtandó adatkezelési tevékenységeket (pl. érintettek tájékoztatása, hozzájárulás megszerzése) beépítettük folyamatainkba.

Az ITIL-PRO szervezetén belül a kezelt személyes adatokat - a feladat elvégzéséhez szükséges mértékben és ideig - csak az üggyel érintett szervezeti egység munkavállalói ismerhetik meg és használhatják fel, feltéve, hogy a személyes adatok megismerése nélkül az ügyben érdemben eljárni nem lehet.

Az ITIL-PRO felelős azért, hogy minden adatkezelést végző munkavállalója megismerje jelen szabályzat rendelkezéseit. A szabályzat rendelkezéseinek betartását (általában az integrált irányítási rendszer auditokkal összevonva) rendszeresen ellenőrizni kell.

8. Érintett jogainak biztosítása

Az érintettek az adatvédelmi tájékoztatókban meghatározott csatornákon keresztül jelezve élhetnek jogaikkal. A megkereséseket az adatvédelemmel foglalkozó munkatárs fogadja. A kérés teljesítésébe bevonja az adatkezelésben érintett felelősöket.

9. Adatbiztonság

Az adatok védelmével, biztonságával kapcsolatos rendelkezéseket az ITIL-PRO információbiztonsági szabályzata tartalmazza.

10. Incidensek kezelése

10.1 Az adatvédelmi incidens fogalma

Adatvédelmi incidens a biztonság olyan sérülése, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

10.2 Eljárás adatvédelmi incidens esetén

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek. Ilyen kár lehet többek között a

személyes adataik feletti rendelkezés elvesztése, vagy a jogaik korlátozása, a hátrányos megkülönböztetés, a személyazonosság-lopás vagy a személyazonossággal való visszaélés, a pénzügyi veszteség, a jó hírnév sérelme, stb.

10.2.1. Bejelentés

Az adatkezelő feladata, hogy amint tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órán belül bejelentse a NAIH felé. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

A bejelentésben legalább

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell a további tájékoztatást nyújtó kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- 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.

Amennyiben az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, a bejelentéstől el lehet tekinteni.

10.2.2. Értesítés

Abban az esetben, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő az érintetteket is indokolatlan késedelem nélkül tájékoztatja, annak érdekében, hogy megtehessék a szükséges óvintézkedéseket. Az érintettnek nyújtott tájékoztatás közérthető formában kell, hogy tartalmazza a NAIH felé teljesítendő bejelentésre vonatkozóan a 10.2.1 pontban leírt információkat.

Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást.

Az érintetteket a 3. sz. mellékletben található minta felhasználásával kell tájékoztatni.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

- 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;
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem áll fenn;
- 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.

Felelősségek

Az adatkezelő bármely munkatársa, aki adatvédelmi incidenst észlel, köteles arról haladéktalanul értesíteni az adatvédelmi munkatársat.

Az adatvédelmi munkatárs és az IT vezető gondoskodik a 10.2.1 pontban meghatározott feladatok végrehajtásáról, valamint nyilvántartásba veszi az incidenst (4. sz. melléklet).

Az adatvédelmi munkatárs és az IT vezető ezek mellett haladéktalanul intézkedik, hogy adatkezelő érintett munkatársai megtegyenek minden lehetséges lépést, amivel az érintett személyes adatok biztonságának és jogszerű kezelésének visszaállítása garantálható.

1. sz. melléklet: A munkavállalók személyes adatinak kezelése

2. sz. melléklet: A partnerek személyes adatinak kezelése

3. sz. melléklet: Adatvédelmi Incidens értesítés minta

ÉRTESÍTÉS ADATVÉDELMI INCIDENSRŐL

Az **Swicon IT Services Kft. mint Adatkezelő** (Székhely: **1031 Budapest, Záhony utca 7. ,** Cégjegyzék szám: **01-09-739887,** Telefon: +36 (1) 883-9866, Email: adatvedelem@swicon-itservices.com, GDPR kontakt: Tündik László)

a következőkről értesíti:

…….. napon az Ön személyes adatait is érintő incidens történt.

Az események leírása:	
Az érintettek kategóriái és hozzávetőleges száma:	
Az érintett adatok kategóriái és hozzávetőleges száma:	
Az incidensből eredő, valószínűsíthető következmények:	
Az incidens orvoslására tett vagy tervezett intézkedések:	

Kelt: ……..

……..

aláírás

4. sz. melléklet: Adatvédelmi incidens nyilvántartás minta

Adatvédelmi incidens nyilvántartás

A nyilvántartás vezetéséért felelős személy: a mindenkori adatvédelmi munkatárs

Incidens időpontja	Incidens leírása	Érintettek kategóriái	Az incidens hatásai	Megtett intézkedések	bejelentés időpontja (NAIH)	Értesítés időpontja (érintettek)

5. sz. melléklet: Adatvédelmi tájékoztató honlap