PRODEBT

Prodebt Pénzügyi és Tanácsadó Korlátolt Felelősségű Társaság
(székhelye: 2083 Solymár, Györgyhegy utca 18., cégjegyzékszáma: 13-09-179047, adószáma: 23983470-2-13)

ADATVÉDELMI INCIDENSEK BEJELENTÉSÉRE VONATKOZÓ ELJÁRÁS

Tartalom

Táblázatok jegyzéke

Bevezetés

Az eljárást akkor kell alkalmazni, ha **Prodebt Pénzügyi és Tanácsadó Korlátolt Felelősségű Társaság (székhelye: 2083 Solymár, Györgyhegy utca 18., cégjegyzékszáma: 13-09-179047, adószáma: 23983470-2-13)** társaságnál az alábbiak bármelyike megtörténik a Prodebt társaság által kezelt bármely személyes adat tekintetében:

„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".

A jelen dokumentumot az [*IT Biztonsági Szabályzat]*-tal együtt kell alkalmazni, mely részletesen leírja Prodebt társaság információ-biztonságát érintő biztonsági sérülésekre, incidensekre vonatkozó eljárásának átfogó folyamatát.

Az EU 2016. évi általános adatvédelmi rendelete (GDPR) előírja, hogy az olyan adatkezelési incidenst, amely valószínűleg kockázattal jár az érintettek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb a tudomásszerzéstől számított 72 órán belül be kell jelenteni a felügyeleti hatóságnak. Ha a 72 órás határidő nem tartható, a késedelem okát meg kell jelölni.

Ha az incidens személyes adatot érint, döntést kell hozni az érintettekkel való kapcsolattartás terjedelméről, időzítéséről és tartalmáról. A GDPR előírja, hogy a kapcsolattartásnak „indokolatlan késedelem nélkül" kell megtörténnie, ha az incidens „magas kockázattal jár természetes személyek jogaira és szabadságaira nézve".

A jelen dokumentumban leírt intézkedés csak iránymutatásként szolgál az incidens kezelésére. Az incidensek jellege és hatása előre nem jósolható meg, ezért az egyes incidensekkel kapcsolatos döntéshozatal során nagyon fontos a körültekintés, a józan ítélőképesség, és az objektív, alapos kockázatértékelés.

A jelen szabályzatban leírt lépések ugyanakkor hasznosak lehetnek annak biztosításához, hogy teljesítsük a GDPR-ból eredő kötelezettségeinket.

Adatvédelmi incidens bejelentésére vonatkozó eljárás

Az adatvédelmi incidens fogalma és belső jelentése

A GDPR a következőképpen határozza meg az adatvédelmi incidens fogalmát:

„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".

A mindennapi gyakorlati során többféle incidens is előfordulhat, pl-

(a) titokvédelmi incidens: ide tartoznak a személyes adatokhoz való jogosulatlan hozzáférés és nyilvánosságra kerülés esetei;

(b) adatmódosítási incidens: ide tartoznak azok az esetek, amikor személyes adatok jogosulatlan vagy véletlen módosítása történik.

Amennyiben a társaság bármely munkavállalója vagy a társaság személyes adataihoz hozzáférő egyéb személy bármilyen adatvédelmi incidenst, vagy annak reális veszélyét tapasztalja, azt köteles részletesen és haladéktalanul bejelenteni az alábbi személy részére, és neki minden segítséget időszerűen megadni az adatvédelmi incidens minél teljesebb körű feltárása és kezelése érdekében:

Név:	[]
Cím:	[]
Telefon:	[]
Fax:	[]
Email:	[]
Bejelentés helye:	[ONLINE FELÜLET, PL. INTRANET CÍME]

A bejelentett incidensek értékelést a fenti személy feladata elvégezni és dokumentálni.

Amennyiben az eset valószínűsíthetően adatvédelmi incidensnek minősül, az értékelést elvégző személy köteles haladéktalanul tájékoztatni a 2.3.1 pontban és az [*IT Biztonsági Szabályzat*] []. pontjában megjelölt személyt, ez utóbbit az incidens kezelésével kapcsolatos eljárás megindítása érdekében.

Külső tájékoztatási kötelezettségek

Annak megállapítását követően, hogy adatvédelmi incidens történt, a GDPR két fél tájékoztatását írja elő. Ezek a következők:

1. Felügyeleti hatóság
2. Érintettek

Az incidenst *„a természetes személyek jogaira és szabadságaira” (GDPR 33. cikk)* gyakorolt kockázat értékelésétől függően kell jelenteni, ezért az ilyen esetekben el kell végezni ezt a kockázatértékelést.

Felügyeleti hatóság

A GDPR alapján a társaság tekintetében a felügyeleti hatóság az alábbi:

Név:	Nemzeti Adatvédelmi és Információszabadság Hatóság
Cím:	1125 Budapest, Szilágyi Erzsébet fasor 22/C
Telefon:	+36 1 391 1400
Fax:	+36 1 391 1410
Email:	ugyfelszolgalat@naih.hu

Bejelentés helye:	[NAIH ÁLTAL MEGHATÁROZANDÓ FELÜLET CÍME]

Döntés arról, hogy kell-e értesíteni a felügyeleti hatóságot

A GDPR kimondja, hogy az adatkezelési incidenst be kell jelenteni a felügyeleti hatóságnak, *„kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.” (GDPR 33. cikk).*

Ennek alapján a szervezet köteles értékelni az adatvédelmi incidens által jelentett kockázat szintjét és mértékét, mielőtt dönt arról, hogy tesz-e bejelentést.

A kockázatértékelés körében többek között az alábbi szempontokat érdemes figyelembe venni:

- az incidens jellege (ld. pl. a fenti kategóriákat);
- az incidenssel érintett személyes adatok természete, érzékenysége és mennyisége (a különleges adatokat is érintő, vagy ügyfelek nagyobb csoportját érintő incidensek értelemszerűen magasabb kockázatot jelenthetnek);
- egyéb, relevánsnak tekintett tényezők (ideértve az incidens hatásának értékelését is).

A fenti kockázatértékelés elvégzése, a bejelentéssel kapcsolatos döntés végrehajtása, a megfelelő dokumentáció elkészítése, és az érintettek felé kapcsolattartás és a részükről felmerülő további kérdések megválaszolása és ügyek intézése az alábbi személy feladata, felelőssége és kötelezettsége:

Név:	[]
Cím:	[]
Telefon:	[]
Fax:	[]
Email:	[]

A kockázatértékelés módját, az indokolást és a következtetéseket dokumentálni kell, és azt a felső vezetésnek kell az aláírásával ellátnia. A kockázatértékelés eredményének az alábbi következtetések egyikét kell tartalmaznia:

1. Az adatvédelmi incidens nem igényel bejelentést
2. Az adatvédelmi incidenst csak a felügyeleti hatóságnak kell bejelenteni
3. Az adatvédelmi incidenst a felügyeleti hatóságnak és az érintetteknek egyaránt be kell jelenteni

A felügyeleti hatósági bejelentés módja

Amennyiben a döntés alapján bejelentést kell tenni a felügyeleti hatósághoz, a GDPR megköveteli, hogy azt *„indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott” (GDPR 33. cikk)* kell megtenni. Ha jogszerű indok alapján a bejelentést nem teszik meg az előírt határidőn belül, az indokot fel kell tüntetni a bejelentésben.

A bejelentést az illetékes adatvédelmi hatóság felé megfelelően, és biztonságos módon kell megtenni, és abban a GDPR 33. cikke szerinti információkat kell megadni.

Az adatvédelmi incidensek nyilvántartásáról az [utazási iroda] nyilvántartást vezet.

Érintettek

Döntés arról, hogy tájékoztatják-e az érintetteket

A GDPR kimondja, hogy az adatkezelési incidensről tájékoztatni kell az érintettet, *„ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve" (GDPR 34. cikk)*. Fontos, hogy a GDPR ezt a tájékoztatást csak „magas" kockázat esetén követeli meg.

A GDPR akkor sem követeli meg az érintettek tájékoztatását, ha az *„aránytalan erőfeszítést tenne szükségessé" (GDPR 34. cikk).* Ilyen esetekben azonban az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni.

Az érintettek tájékoztatásának módja

Miután döntés született arról, hogy az incidens indokolja az érintettek tájékoztatását, GDPR alapján a tájékoztatást indokolatlan késedelem nélkül kell megtenni.

Az érintetteknek adott tájékoztatásban *„világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét" (GDPR 34. cikk)* és a következőket:

a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségét;

b) az adatvédelmi incidensből eredő, valószínűsíthető következmények leírását; és

c) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Hatálybalépés időpontja:
Dátum: 2020.02.27

Nagy Dávid
ügyvezető