SZEMÉLYI ADATSÉRTÉSRŐL SZÓLÓ ÉRTESÍTÉSI ÚTMUTATÓ

CREDITFORTE KFT.

Dr. Saly Gábor
ügyvezető igazgató

BEVEZETŐ

Jelen Személyi Adatsértésről szóló Értesítési Útmutató („Útmutató") az Egységes Európai Adatvédelmi Rendelet (GDPR) jogerőre emelkedésének dátumán lép életbe. A Rendelet elrendeli a felügyelő hatóság értesítését személyi adatsértés esetén (vagy határon túli sértés esetén a vezető hatóságét), és bizonyos esetekben az adatalanyok értesítését a sértésről.

Jelen Útmutató általános célja, hogy lehetővé tegye a Creditforte Kft. számára (Társaság) az adatsértés felismerését, illetőleg annak a kivizsgálását, hogy a sértés az értesítése kötelezettség hatáskörén belül esik-e és szükséges-e a jelentés, valamint az adatalanyok értesítése.

Az informatikai rendszerekben és infrastruktúrákban bekövetkező adatsértésekkel kapcsolatosan további információkat az Informatikai Biztonsági Szabályzat tartalmaz.

Az Útmutató érvényessége

Jelen útmutató a személyi adatsértés esetén érvényes. Az incidensek azonosításával kapcsolatos kérdésekre az Informatikai Biztonsági Szabályzatban találhatóak (Incidens kezelés c. fejezet)

Mit jelent a személyi adatsértés

A GDPR értelmében a személyi adatsértés a biztonság olyan mértékű megsértése, amely a továbbított, tárolt vagy egyéb módon feldolgozott személyi adatok törvénytelen megsemmisítéséhez, elvesztéséhez, módosulásához, illetéktelen nyilvánosságra hozatalához vagy hozzáféréséhez vezet.

Az alábbi leírás rendszerezi az adatsértések általános kategóriáit:

Kategória	Jellemző tevékenység	Megjegyzés
Bizalmasság megsértése	Személyi adatok véletlenszerű, törvénytelen vagy illetéktelen nyilvánosságra hozatala vagy hozzáférése	A személyi adatok megkapására/azokhoz való hozzáférésre nem felhatalmazott személyes megkapják, hozzáfernek az adatokhoz.
Integritás megsértése	Személyi adatok véletlenszerű vagy törvénytelen megváltoztatása (pl.:módosítása)	A „megváltoztatás" a személyi adatok módosítását jelenti.
Hozzáférhetőség megsértése	Személyi adatok véletlenszerű vagy törvénytelen elvesztése vagy megsemmisítése	A „megsemmisítés" azt jelenti, hogy a személyi adatok már nem léteznek, vagy nem teljesek. Az „elvesztés" azt jelenti, hogy a személyi adatok többé nem kezelhetőek és nem hozzáférhetőek (azonban még mindig léteznek)

Személyi adatok megsértéséről kizárólag biztonsági incidens megtörténte után beszélhetünk. Azonban nem minden biztonsági incidens jelenti a személyi adatok megsértését. Arról csak akkor beszélhetünk, ha a biztonsági incidens a személyi adatokat érinti. A GDPR által előírt értesítési kötelezettség alá eső adatsértés olyan egyéneket is érinthet, akik nem az adatsértés alanyai.

Példa esetek:

- illetéktelen harmadik fél általi hozzáférés (pl.: egy informatikai megoldások szolgáltatója, akinek a Cég nem engedélyezte a személyi adatfeldolgozást, hozzáfér az adósok/alkalmazottak adatbázisához)
- személyi adatokat tartalmazó eszközöket elveszítik vagy ellopják (pl.: egy alkalmazott elveszít egy személyi adatokat tartalmaz USB adathordozót)
- személyi adatok hozzáférhetőségének elvesztése (pl.: hackertámadás esetén ellopják a cégben dolgozók személyes adatait)

Adatsértés esetén értesítendő

Felügyelő hatóság: vagy vezető felügyelő hatóság, pl.: minden feldolgozó esetén illetékes adatvédelmi hatóság az adott EU államban és az adatalanyok. A felügyelő hatóságot akkor kell értesíteni, ha az adatsértés magánszemélyek jogait és szabadságait veszélyezteti, míg az adatalanyokat akkor kell értesíteni, ha az adatsértés magánszemélyek jogait és szabadságait magas szinten veszélyezteti. A felügyelő hatóság értesítésének formájával és módszerével kapcsolatos adott követelményeket a nemzeti jogszabályok írják elő.

A felügyelő hatóságot szabályszerűen haladéktalanul értesíteni kell, illetve nem később, mint 72 órával azután, hogy a Cég tudomást szerez az adatsértésről. Az adatalanyt haladéktalanul értesíteni kell.

Biztonsági incidens
A biztonsági incidens a személyi adatok megsemmisítését elvesztését, megváltoztatását, illetéktelen nyilvánosságra hozatalát vagy hozzáférhetőségét eredményezte?

⇓

Adatsértés
Veszélyezteti az adatsértés magányszemélyek jogait és szabadságait?

⇓

Felügyelő hatóság értesítése
Magas szinten veszélyezteti az adatsértés magánszemélyek jogait és szabadságait?

⇓

Adatalany értesítése
Az adatalanynak küldendő értesítés jelen Útmutató 2. számú mellékelte

A személyi adatsértés értesítési kötelezettsége az adatkezelőre és az adatfeldolgozóra is érvényes. Azonban a GDPR különbséget tesz az adatkezelő és az adatfeldolgozó kötelezettségének kiterjedésében. Ha személyi adatsértés történt, az adatkezelő köteles értesíteni a felügyelő hatóságot és bizonyos esetekben az adatalanyokat is, míg az adatfeldolgozó csak az adatkezelő értesítésére köteles. Azonban az adatkezelő megállapodást köthet az adatfeldolgozóval, hogy ez utóbbi vállaljon felelősséget az értesítési kötelezettségért az adatkezelő nevében.

Az értesítési kötelezettség jellegének megállapítása érdekében minden egyes adatsértés esetén meg kell állapítani, hogy:

- a megsértett adatokra vonatkozóan adatkezelői vagy adatfeldolgozói minőségben működik-e
- volt-e bármely további intézkedés az adatsértési értesítés megtételével kapcsolatosan?

Annak meghatározása érdekében, hogy a Társaság által megállapított személyi adatsértés értesítési kötelezettsége hatálya alá esik-e, szükséges az adatsértés veszélyének felmérése.

A felmérési folyamat hasonló az Adatvédelmi Hatáselemzéshez. Azonban a DPIA vizsgálat adatsértés bekövetkezte előtt történik, míg a jelen Útmutató szerinti felmérés akkor végzendő, ha megtörtént az adatsértés.

Annak felmérése során, hogy az adatsértés veszélyt/magas szintű veszélyt jelent-e a magánszemélyek jogaira és szabadságaira, az alábbi tényezőket kell figyelembe venni:

- adatsértés típusa
- az adatsértés által érintett személyi adatok érzékenysége
- érintett adatok célja és érintett adatalanyok száma
- egyének azonosításának nehézségi szintje
- egyénekre való következmények súlyossága
- egyének különleges jellemzői

A Társaság felelőst jelöl ki a személyi adatsértés értesítési kötelezettség betartására: Adatvédelmi Tisztviselő. Az esetleges adatsértést felfedező kollegák az Adatvédelmi Tisztviselő felé tartoznak jelentési kötelezettséggel, amennyiben tudomást szereznek biztonsági incidensről.

Kivételek az értesítési kötelezettség alól

A GDPR bizonyos kivételeket nevez meg: kivételt azok az esetek képeznek, amikor az adatsértés valószínűleg nem jelent veszélyt a magánszemélyek jogaira és szabadságaira.

A Társaság, mint Adatkezelő

Amikor a Társaság adatkezelőként működik és az adatok feldolgozására egy adatfeldolgozót alkalmaz, az adatfeldolgozóval kötött megállapodásokban biztosítani kell, hogy az adatfeldolgozó megfelelő módon garantálja a személyi adatsértés értesítési kötelezettségének betartását. Tekintettel arra, hogy gyakorlatban sokszor az adatfeldolgozó szerez tudomást az adatsértésről, az efféle megállapodások előírásainak lehetővé kell tennie, hogy a Társaság betartsa a személyi adatsértési kötelezettségét. Különösen biztosítani kell, hogy az adatfeldolgozó időben értesíti a Társaságot az adatsértésekről és a sértések fejleményeiről. A Társaság megegyezhet az adatfeldolgozóval, hogy adatsértés esetén ez utóbbi értesíti a felügyelő hatóságot és/vagy adatalanyokat a Társaság nevében. Azonban biztosítani kell, hogy ebben az esetben az adatfeldolgozó minden, a felügyelő hatóságnak/alanynak tett értesítést jelenti a Társaságnak, valamint értesíti a Társaságot minden olyan esetről, amely során a veszélyek felmérése alapján az adatfeldolgozó úgy döntött, hogy nem küld értesítést az adatsértésről.

Felelősségre vonási elv betarthatósága

Az adatkezelőnek belső nyilvántartást kell kezelnie minden személyi adatsértésről. Ennek az alábbiakat kell tartalmaznia:

- dátumot, amikor az adatsértés a tudomására jutott
- az adatsértés részletes leírását és hatásait
- a Társaság általi helyreállító intézkedéseket

A Társaság felelőst jelöl ki a nyilvántartás vezetéséért és frissítéséért: Adatvédelmi tisztviselő

Teendők személyi adatsértés esetén

1. adatsértés-kezelő csapat kijelölése
2. vizsgálat megkezdése
3. veszély felmérése
4. értesítési kötelezettség: kell-e értesíteni, és ha igen, akkor kit
5. felügyelő hatóság és szükség esetén az adatalany(ok) értesítése
6. helyreállító intézkedések elvégzése
7. felügyelő hatóság és adatalanyok értesítése a fejleményekről (ha vannak)
8. adatsértés nyilvántartásba vétele

Büntetés az értesítési kötelezettség megszegése esetén

A személyi adatsértés értesítési kötelezettségének megsértése esetén, a felügyelő hatóság az adatkezelőre adminisztratív büntetést szabhat ki, melynek értéke 10.000.000 euróig vagy az előző pénzügyi évi teljes globális éves árbevétel 2%-ig terjedhet.

Továbbá, ha a hatóság biztonsági intézkedések hiányát, vagy a meglévő biztonsági intézkedések megfelelőtlenségét észleli, a felügyelő hatóság szankciókat szabhat ki értesítés mulasztásáért és a biztonsági intézkedések hiányáért, mivel az két külön sértést jelent.

ADATSÉRTÉSI FOLYAMATÁBRÁK

Adatfeldolgozói minőségben tett értesítés (késedelem nélkül)

1. Az adatfeldolgozó meghatározza, hogy személyi adatsértés történt
2. Adatkezelő értesítése

Adatkezelői minőségben tett értesítés

1. Biztonsági incidens megállapítása és annak meghatározása, hogy történt-e személyi adatsértés
2. Az adatsértés veszélyt jelent-e a magánszemélyek jogaira és szabadságaira?
    a. nem
    b. igen: 72 órán belül, ha lehetséges
3. Ha igen: felügyelő hatóságot értesíteni kell, amennyiben több, mint egy tagállamban lévő személyt érint akkor a vezető felügyelő hatóságot.
4. Az adatsértés magas szintű veszélyt jelent-e a magánszemélyek jogaira és szabadságaira?
    a. nem
    b. igen
5. Ha igen: adatalany értesítése

ADATKEZELŐ ÁLTAL A FELÜGYELŐHATÓSÁG ÉRTESÍTÉSE

Szempont	Követelmény	Megjegyzés
Adatsértés kategóriája	- személyi adatsértés, amely valószínűleg veszélyt jelent a magánszemélyek jogaira és szabadságaira	- pl.: személyes adatokat érintő biztonsági elem elvesztése - nem szükséges értesítést küldeni, amennyiben az adatsértés „valószínűleg

		nem jelent veszélyt", pl.: személyi adatok már nyilvánosan elérhetőek és az ilyen adatok nyilvánosságra hozatala nem jelent veszélyt az egyén számára.
Értesítési időkeret	- késedelem nélkül - ahol lehetséges, nem több, mint 72 órával az adatsértésről való tudomásszerzés után ahol a 72 órán belüli értesítés nem lehetséges, az értesítéssel együtt meg kell küldeni a késedelem indoklását amennyiben nem lehetséges az információt ugyanabban az időben megadni, akkor azt a fázisokban lehet megadni további indokolatlan késedelem nélkül	- „tudomásszerzés" alatt azt kell érteni, hogy a Társaság biztos abban, hogy személyi adatokat veszélyeztető biztonsági incidens történt - késedelem indoka: pl. ha az adatkezelőnek több hasonló, nagyszámú adatalanyt ugyanolyan módon érintő adatsértést rövid időn belül kell kezelnie. - az adatfeldolgozókkal kötött megállapodásoknak rendelkeznie kell a feldolgozó kötelezettségéről, hogy adatsértés esetén értesítse a Társaságot, ilyen megállapodásokban az is elfogadható, hogy a feldolgozó felhatalmazást kap, hogy a kezelő nevében értesítést küldjön. - egyéb kezelőkkel kötött megállapodásoknak (pl.: közös kezelés esetén) rendelkeznie kell arról, hogy a Társaság vagy más adatkezelő vigyázzon vagy feleljen az értesítési kötelezettség megszegéséért.
Értesítés formája	- jogszabály alapján	- jogi követelmények szerint - a felelősségre vonhatóság elvének való megfelelés érdekében az értesítést

		írott/elektronikus formában kell megküldeni, hogy az értesítési kötelezettségnek való megfelelés bizonyítható legyen.
Értesítés tartalma	- személyi adatsértés jellegének leírása, ahol lehetséges, ott az érintett adatalanyok kategóriái és száma - adatvédelmi tisztviselő nevének és elérhetőségének megadása - a várható következmények leírása - a személyi adatsértés orvoslása érdekében tett, vagy tenni javasolt intézkedéseket, beleértve adott esetben az adatsértés lehetséges mellékhatásainak mérséklési intézkedéseit	- a GDPR előírja az értesítés minimális tartalmát - javasolt felmérni, hogy az adatsértés melyik további információi relevánsak a felügyelő hatóság szemszögéből - a Társaságnak nyomon követési vizsgálatot követően informálnia kell a felügyelő hatóságot, a Társaságnak kell meghatároznia, hogy a biztonsági incidenst sikerült megfékeznie, és nem történt személyi adatsértést.
Egyéb követelmények	- a kezelőnek bármely személyi adatsértést dokumentálnia kell, amely által összefoglalja a személyi adatsértéssel kapcsolatos tényeket, az adatsértés hatásait és a megtett helyreállítási intézkedéseket	- lehetővé kell tennie a felügyelő hatóság számára a GDPR követelményeknek való megfelelést (felelősségre vonhatóság elve)

ÉRTESÍTÉS AZ ADATKEZELŐNEK AZ ADATFELDOLGOZÓ ÁLTAL

Szempont	**Követelmény**	**Megjegyzés**
Adatsértés kategóriája	- személyi adatsértés	- minden személyi adatsértést jelenteni kell az adatkezelőnek – az adatkezelő feladata annak az ellenőrzése, hogy az adatsértés valószínűleg veszélyes-e a magánszemélyek jogaira és szabadságaira
Értesítési időkeret	- az adatsértés	- ezen kötelezettség

	megállapítását követően késedelem nélkül - amennyiben nem lehetséges az információt ugyanabban az időben megadni, akkor azt a fázisokban lehet megadni további indokolatlan késedelem nélkül	határidejét meg kell határozni az adatkezelővel kötött megállapodásban (pl.: adatmegbízási megállapodás vagy személyi adatvédelemre vonatkozó szerződés előírás) - meg kell határozni, hogy az adatkezelőnek – szabályszerűen 72 órája van, hogy a sértésről értesítse a felügyelő hatóságot. - a feldolgozónak azonnal értesítenie kel a kezelőt az adatsértéssel kapcsolatos bármely további információról, amikor az a következő fázisokban a tudomására jut.
Értesítés formája	- a GDPR nem írja elő	- a felelősségre vonhatóság elvének való megfelelés érdekében az értesítést írott/elektronikus formában kell megküldeni, hogy az értesítési kötelezettségnek való megfelelés bizonyítható legyen
Értesítés tartalma	- a személyi adatsértés jellegét és ahol lehetséges az érintett adatalanyok kategóriáit és körülbelüli számát, valamint az érintett adatrekordok kategóriáit és körülbelüli számát - a személyi adatsértés valószínű következményeinek leírása - a személyi adatsértés orvoslása érdekében tett, vagy tenni javasolt intézkedések leírása	- az értesítés alapján az adatkezelőnek képesnek kell lennie az adatsértéssel kapcsolatos kötelezettségének eleget tenni

CREDITFORTE Kft.
Adószám: 14656257-2-43
Cégjegyzékszám: 01-09-345193
Székhely: 1118 Budapest
Pannonhalmi út 36-38.

ELÉRHETŐSÉGEK:
Lev. cím: 1506 Budapest Pf.74.
E-mail: info@creditforte.hu
Web: http://www.creditforte.hu
Adatkezelési azonosító: 02807-0001

ADATALANYOK ÉRTESÍTÉSE

Szempont	Követelmény	Megjegyzés