

SZABÁLYZAT

ADATVÉDELMI INCIDENSEK KEZELÉSE

A **VAREG HUNGARY Korlátolt Felelősségű Társaság** mint adatkezelő (továbbiakban Adatkezelő) a hatályos jogszabályok előírásai alapján adatkezelése során köteles 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 kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket végrehajtani annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

Adatvédelmi incidensnek minősül 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. Adatvédelmi incidens így különösen az Adatkezelő működése során használt, személyes adatokat tároló laptop vagy mobiltelefon elvesztése, a személyes adatokat tartalmazó adathordozók nem biztonságos tárolása, megsemmisítése, továbbítása és az Adatkezelő által használt informatikai rendszerek elleni támadások, honlap feltörése.

Adatkezelő törekszik az adatvédelmi incidensek megelőzésére, azok kezelésére, orvoslására és nyilvántartására vonatkozó intézkedéseit és eljárását jelen Szabályzat tartalmazza.

I. Megelőző intézkedések

Adatkezelő adatvédelmi rendszert épített ki, amelyben az adatkezelésre vonatkozó valamennyi releváns körülmény szabályozásra került. **Adatkezelő gondoskodik arról, hogy munkavállalói az adatkezelésre vonatkozó kötelezettségeket megismerjék és megtartsák**, az adatvédelmi szabályzatok betartását lényeges munkaköri kötelességnek minősíti, a személyes adatokkal kizárólag meghatározott jogosultságok alapján, munkakörüknek megfelelő célból és módon kerülhetnek kapcsolatban, azokat csak a taxatíve meghatározott módon kezelhetik. Az adatkezelést végző munkavállalók és adatfeldolgozók az adatkezeléssel kapcsolatosan titoktartási nyilatkozatot tesznek.

Adatkezelő a személyes adatok védelméről **mind elektronikus, mind papír alapú nyilvántartásaiban gondoskodik**. Az elektronikusan kezelt adatok védelme érdekében Adatkezelő informatikai rendszereit tűzfallal védi és vírusvédelemmel látja el, az általa használt programokat pedig úgy választja meg, hogy azok a mindenkori információbiztonsági követelményeknek megfeleljenek. Informatikai rendszereihez különböző jogosultsági szinteket határoz meg és az információkhoz való hozzájutást jelszóvédelemmel korlátozza, gondoskodik továbbá az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, így különösen rendszeres biztonsági mentésekről és a másolatok elkülönített, biztonságos tárolásáról. Az elektronikusan tárolt adatokhoz kizárólag Adatkezelő ügyvezetői és a közvetlen irányítása alá tartozó, magas beosztású munkavállalók férhetnek hozzá, jogosultságuk elektronikus igazolása és jelszó használata mellett.

A személyes adatokat tartalmazó iratokat Adatkezelő elzártan, fizikai védelmet biztosítva, saját iratkezelési rendszerezésnek megfelelően tárolja és gondoskodik arról, hogy ahhoz jogosulatlan személy ne férhessen hozzá.

II. Kockázatértékelés adatvédelmi incidens bekövetkezése esetén

Adatvédelmi incidens bekövetkezése esetén azt az Adatkezelő az alábbi körülmények szerint vizsgálja:

- a) az érintett adatok köre, azok osztályozása (személyes adat vagy annak valamely különleges kategóriája), az érintettek száma és kategóriája és az érintett azonosíthatósága az adatvédelmi incidenssel érintett adatokból
- b) az adatkezelés körülményei

- c) további sérelem elhárításához vagy a bekövetkezett sérelem csökkentéséhez azonnali intézkedés szükséges-e, az adatvédelmi incidens kezelése a normális ügyvitelen túli munkavégzést szükségessé tesz, a normális ügyvitelben fennakadást eredményez-e
- d) a sérelem tartós hátrányos eredményt okozott-e az érintettnek
- e) büntetőjogi vagy szabálysértési eljárási jogkövetkezményei lehetnek-e
- f) a sérülés körülményeinek vizsgálata, a biztonság csökkenésének mértéke, az adatvédelmi incidens bekövetkezése kapcsán fennálló szándékosság vizsgálata

III. Eljárás adatvédelmi incidens bekövetkezése esetén

Amennyiben Adatkezelő bármely munkavállalója adatvédelmi incidens bekövetkezését észleli, úgy köteles azt késedelem nélkül bejelenteni a munkáltatói jogkör gyakorlójának, valamint annak körülményeit feljegyezni, így különösen

- az észlelés napját és időpontját, valamint, ha megállapítható a (feltételezett) adatvédelmi incidens bekövetkezésének napját és időpontját;
- azoknak a személyes adatoknak a körét, amelyet az adatvédelmi incidens érint;
- a bekövetkezés okát és terjedelmét

Adatvédelmi incidenst bejelenthet bármely személy Adatkezelő fent megadott elérhetőségein.

Az adatvédelmi incidens orvoslása érdekében a munkáltatói jogkör gyakorlója, illetőleg azon munkavállaló, aki munkaköre alapján eljárni jogosult vagy köteles, késedelem nélkül megteszi a szükséges intézkedéseket, és azokat részletesen dokumentálja. Ilyen intézkedés különösen a munkavállalók egyes jogosultságainak megszüntetése, jelszavak módosítása, informatikai rendszerek átmeneti zárolása.

Adatkezelő ezen intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából **nyilvántartást vezet**, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat, amennyiben jogszabály ilyeneket előír.

Az adatvédelmi incidens fentiek szerint történő értékelését a tudomásszerzést követő 24 órán belül kell végezni. Az Adatkezelő indokolatlan késedelem nélkül – ha lehetséges, legkésőbb 72 órával azt követően, hogy az adatvédelmi incidens a tudomására jutott – **bejelentést tesz a Nemzeti Adatvédelmi és Információszabadság Hatóságnak** az 1. számú melléklet szerint, kivéve, ha az adatvédelmi incidens a fentiek szerint kockázattal valószínűsíthetően jár.

Jelentős kockázat esetén Adatkezelő tájékoztatja az érintettet az adatvédelmi incidensről, közli annak jellegét és a valószínűsíthető következményeket, valamint az orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket. Az érintettet nyilvánosan közzétett információk útján kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

- 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 valósul meg
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé.