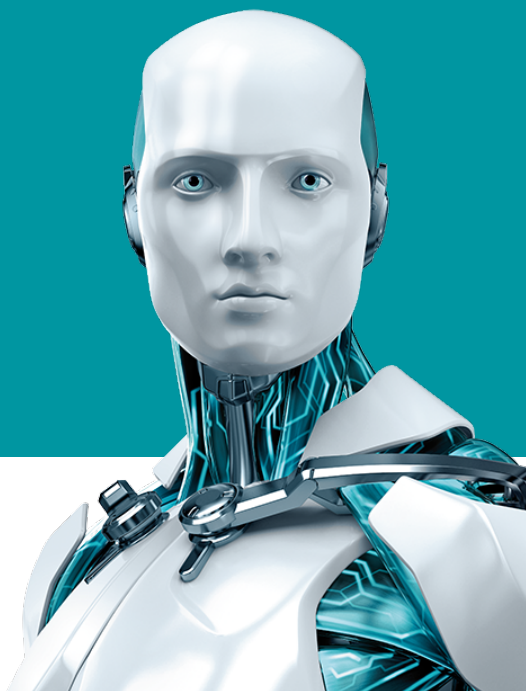
GDPR

Útmutató az EU általános adatvédelmi rendeletéhez



ENJOY SAFER TECHNOLOGY™

Az általános adatvédelmi rendelet (GDPR)[1] felváltja az Európai Unió (EU) 1995-ös, 95/46/EK számú adatvédelmi irányelvét. A GDPR elfogadásának célja az volt, hogy az Európai Unión belül erősítse és egységesítse az egyén online környezetben is érvényesülő, magánszférához fűződő és a személyes adatok védelméhez való jogát, miközben egyszerűsíti az EU polgárokat kiszolgáló vállalkozások adatvédelmi kötelezettségeit azáltal, hogy a 28 különböző tagállami szabályozást egy egységes EU rendelet váltja fel.

2016. április 8-án az Európai Unió Tanácsa, majd április 14-én az Európai Parlament is elfogadta az általános adatvédelmi rendeletet, valamint egy kapcsolódó (bűnüldözési célú adatkezelésekről szóló) irányelvet.

2016. május 4-én a rendelet és az irányelv hivatalos szövege is megjelent az Európai Unió hivatalos lapjában. A rendelet rendelkezéseit 2018. május 25-től kell minden EU tagállamban alkalmazni.

A 28 EU tagállam az 1995-ben elfogadott szabályokat különbözőképpen vette át, ami nehézkessé és költségessé tette az EU vállalkozásai számára a határokon átnyúló működést, és jelentékeny tagállami különbségeket eredményezett a szabályok tényleges érvényesülésében. Becslések szerint e széttöredezettség megszüntetése az üzleti szféra számára nagyjából €2.3 Mrd éves megtakarítást jelent majd Európa szerte.

Melyek a főbb változások?

A reform fontosabb változásai, többek között:[2]

- Tájékoztatáshoz való jog az adatokat ért incidensek (pl. hackertámadás) esetén: A vállalkozások és más szervezetek kötelesek értesíteni a felügyelő hatóságot azon incidensekről, amelyek az egyének számára várhatóan kockázattal járnak, sőt – amilyen gyorsan csak lehetséges – kötelesek tájékoztatni magukat az érintetteket is az összes olyan incidensről, amely valószínűsíthetően magas kockázattal jár rájuk nézve, hogy a felhasználók megtehessék a szükséges intézkedéseket.
- A szabályok határozottabb kikényszerítése: Az adatvédelmi hatóságok a vállalkozásokat akár az éves globális árbevételük 4%-ának megfelelő bírsággal is sújthatják, ha nem felelnek meg az EU szabályozásának. Igaz, a bírság kiszabása nem kötelező, és alkalmazása esetén minden egyes ügyben egyedileg kell mérlegelni, hogy a bírság hatékony, arányos és visszatartó erejű legyen.
- Egy kontinens, egy jog: Egységes, összeurópai adatvédelmi jog váltja a nemzeti jogok jelenlegi kusza rendszerét, így a vállalkozásoknak csupán egy joganyagra kell tekintettel lenniük, nem 28-ra. Az ebből származó haszon évente akár a 2.3 Mrd eurót is elérheti.
- A szervezeteknek indokolt késedelem nélkül (ha lehetséges, legkésőbb 72 órán belül) értesíteniük kell a felügyelő hatóságot a jelentősebb adatvédelmi incidensekről.
- Az EU szabályait akkor is alkalmazni kell, ha a személyes adatokat az EU-n kívül kezelik olyan vállalkozások, amelyek az EU piacain is tevékenykednek és az áruikat és szolgáltatásaikat (az ingyeneseket is ideértve) EU állampolgároknak nyújtják, vagy tevékenységük az érintettek EU-n belüli viselkedésének megfigyeléséhez kapcsolódnak.
- Beépített és alapértelmezett adatvédelem elve: A 'beépített adatvédelem' és az 'alapértelmezett adatvédelem' elvei az EU

1 GDPR szövege hozzáférhető: http://eur-lex.europa.eu/legal-content/HU/TXT/?qid=1485464912091&uri=CELEX:32016R0679

2 Az Európai Bizottság sajtóközleménye (http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm) alapján

adatvédelmi szabályozásának fontos elemei lettek. Az adatvédelmi garanciákat a termékekbe és szolgáltatásokba is be kell építeni a fejlesztés legkorábbi szakaszától kezdve, és követelmény lesz a privacy-barát alapértelmezett beállítások alkalmazása is.

Az EU adatvédelmi szabályozásának erősítésével tehát kötelező a vállalkozások számára, hogy megfelelő védelmet nyújtsanak a kezelt személyes adatoknak, amely:

> *„azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható".*[3]

A személyes adat ilyen tág megfogalmazása magában foglalja a legegyszerűbb dokumentumot vagy nyilvántartást is, amely valahogy – akár csak közvetve is – kapcsolódik vásárlókhoz, ügyfelekhez, munkavállalókhoz, diákokhoz, vagy bármely más természetes személyhez.

Mit mond a szabályozás az adatok biztonságáról?

A 32. cikk az adatkezelés biztonságáról így szól:[4]

> *1. (1) Az adatkezelő és az adatfeldolgozó 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, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve többek között, adott esetben:*
>
> *a) a személyes adatok álnevesítését és titkosítását;*
>
> *b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;*
>
> *c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;*
>
> *d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.*

A titkosítás a legkönnyebb és legbiztosabb módja annak, hogy biztosított legyen az adatok biztonsága, amint azt a GDPR 32. cikke megköveteli. A technológia bevett eszköz azon információk védelmére, amely lopásnak vagy az elvesztés veszélyének van kitéve. A GDPR ugyancsak szorgalmazza hatékony katasztrófa-helyreállítási terv (DRP), jelszó-visszaállítási és kulcskezelési rendszerek alkalmazását.

3 Hozzáférhető: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2001.008.01.0001.01.ENG

4 Az Európai Bizottság sajtóközleménye (http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm) alapján

A GDPR 30. cikke megkívánja az adatkezelési tevékenységek nyilvántartását, ideértve a 32. cikk szerint alkalmazott technikai és szervezési biztonsági intézkedések általános leírását is. Ez azt jelenti, hogy a szervezetnek megfelelő dokumentációval és bizonyítékkal kell rendelkeznie arról, hogy a rendszere biztonságos, és hogy a titkosított adatok visszaállíthatók egy technikai incidenst követően.

Melyek az adatvédelmi incidenssel kapcsolatos szabályok?

A 33. cikk előírja az adatvédelmi incidensek felügyelő hatóságnak történő bejelentését, és rögzíti, hogy annak, ha lehetséges, az incidens észlelésétől számított legkésőbb 72 órán belül meg kell történnie. A határidőn túl küldött értesítés esetén pedig érdemben igazolni kell a késedelem indokait.

A 34. cikk előírja egyes adatvédelmi incidensek esetén az érintettek közvetlen tájékoztatását is:

> 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.*

Mindazonáltal a Rendelet így folytatódik:

> *(3) Az érintettet nem kell az (1) bekezdésben említettek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:*
>
> *a) 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, az (1) bekezdésben említett 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.*

Egyes tanulmányok azt mutatják, hogy minél korábbi az incidensről szóló értesítés, a következmények annál nagyobb kárt okoznak az adatvédelmi incidenssel érintett szervezet számára. Még egyszer hangsúlyozandó, hogy a titkosítás egyértelműen olyan megfelelő biztosítéknak tekinthető, amely meggátolja ezt, és segít a vállalkozás jó hírnevének megtartásában.

Hogyan szankcionálja a GDPR a jogsértőket?

83. cikk a közigazgatási bírságok kiszabására vonatkozó általános feltételekről, 4. pont:[5]

> *(4) Az alábbi rendelkezések megsértése – a (2) bekezdéssel összhangban – legfeljebb 10 000 000 EUR összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-át kitevő összeggel sújtható; a kettő közül a magasabb összeget kell kiszabni:*
>
> *a) az adatkezelő és az adatfeldolgozó tekintetében a 8., a 11., a 25-39., a 42. és a 43. cikkben meghatározott kötelezettségek; ideértve tehát az adatvédelmi incidenseket szabályozó 33. és 34. cikket.*

5 Hozzáférhető: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2001.008.01.0001.01.ENG

A 83. cikk 5 pontja így folytatódik:

(5) Az alábbi rendelkezések megsértését – a (2) bekezdéssel összhangban – legfeljebb 20 000 000 EUR összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeggel kell sújtani, azzal, hogy a kettő közül a magasabb összeget kell kiszabni:

a) az adatkezelés elvei – ideértve a hozzájárulás feltételeit – az 5., 6., 7. és 9. cikknek megfelelően;

Az 5. cikk pedig a személyes adatok kezelésére vonatkozó elvek között említi, hogy:

(1) A személyes adatok:

f) 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").

Egyértelműn látható a törekvés a jogsértők megbüntetésére és eltántorítására. E szabályok kevesebb, mint két év múlva alkalmazandók lesznek – ideje tehát már most cselekedni.

Néhány tagállamban már megkezdődött a felkészülés. A holland törvényhozás 2015 májusában elfogadta az adatvédelmi törvény módosítását, és – elébe vágva a GDPR rendelkezéseinek – Hollandiát az egyik leggyengébb felügyeleti rendszerrel rendelkező tagállamból az egyik legerősebbel rendelkező országgá tette. A GDPR 2018 májusától mind a 28 EU tagállamban érvényesíthető lesz.

Milyen intézkedések szükségesek?

A rendelet méretüktől függetlenül minden vállalatot számos új folyamat és belső irányelv bevezetésére kötelez, amelyek célja, hogy az egyének számára nagyobb kontrollt biztosítsanak a személyes adataikkal kapcsolatban. Ezen folyamatok és irányelvek bevezetése a legtöbb esetben új folyamatleírások és szabályzatok elkészítését, az alkalmazotti állomány újraképzését, és a meglévő rendszer bizonyos fokú átalakítását, frissítését is szükségessé teszi, hogy az megfelelhessen az új elvárásoknak. Ezen felül néhány gyakorlati lépést is szükséges megtenni, ilyen például a kockázatnak kitett adatok titkosítása.

Egy laptop vagy USB kulcs elvesztése nem von magával büntetést, ha az eszközön lévő adatok egy elismert termékkel titkosításra kerültek korábban. A DESlock szoftver hosszú évek óta biztosítja különböző méretű vállalatok számára a laptopok, a cserélhető adathordozók, az e-mailek és a fájlok, mappák titkosítását. Termékeink lefednek minden rendszert a Windows XP-től kezdve egészen a Windows 10-ig, illetve iOS esetén a 7-es vagy az annál frissebb rendszereket. A szoftverünk egy FIPS 140-2 level 1 minősítésű titkosítási alrendszerre épül, a kulcskezelő rendszerünk és az egyedülálló menedzsment szerverünk pedig nemzetközi szabadalmi oltalom alatt állnak.

Vegye fel a kapcsolatot a legközelebbi ESET viszonteladónkkal, akitől további tájékoztatást kaphat, illetve ingyenes próbalicencet vagy termékbemutatót igényelhet.

Az általános adatvédelmi rendelet egyik legfontosabb alapelve (mint az az 5. cikkben olvasható) a személyes adatok megfelelő biztonságának megvalósítása. Erre pedig, ahogyan az a 32., az „adatkezelés biztonsága" című cikkben olvasható, a titkosítás a megfelelő műszaki óvintézkedés. Ahol titkosítást alkalmaznak, ott kötelező biztosítani, hogy egy váratlan eseményt követően az adatok azonnal visszaállíthatók legyenek, és meg

kell tartani azokat a bejegyzéseket is, amelyek bizonyítják, hogy a rendszer biztonságos, és hogy az adatok visszaszerezhetők.

Az ESET DESlock Encryption szoftvere egyszerű és hatékony kezelhetőség mellett felel meg mindezen elvárásoknak.

Célkitűzés	DESlock Encryption by ESET
Tárolt adatok védelme a vállalaton belül	A DESlock Encryption összes licencelt verziója alapfunkcióként tartalmazza a fájlok, a mappák és a cserélhető adathordozók titkosítását a végpontokon
Hordozott adatok védelme	A DESlock+ Pro tartalmaz teljes merevlemez titkosítást, illetve cserélhető adathordozó titkosítást az USB-s eszközök és az optikai lemezek számára, így biztosítja az adatok biztonságos hordozását.
Mobileszközök adatainak védelme, az otthoni munkavégzés biztosítása	A kereskedelmi DESlock Encryption licenc kiterjeszthető a privát-PC-re történő telepítésre is. Mindezen felül a DESlock+ Go megfelelő titkosítást biztosít bármely USB-s adathordozó számára.
Biztonságos adatátvitel	Az összes DESlock Encryption tartalmaz Outlook beépülő modult, az összes levelezőprogrammal és a webes levelezőkkel is kompatibilis vágólap titkosítást és bármely rendszeren működő csatolmány titkosítást. Az optikai tároló titkosítása lehetővé teszi a CD-ken vagy DVD-ken tárolt adatok biztonságos szállítását.
Adathozzáférések tiltása vagy korlátozása	Az egyedülálló, szabadalmazott kulcs-megosztási technológiának köszönhetően egyszerűen hozhatók létre és kezelhetők akár összetett vagy többrétegű felhasználói csoportok és munkacsoportok is.
Igény szerinti hozzáférés a biztonságos adathoz	A DESlock+ Enterprise Server egy titkosított internetkapcsolaton keresztül teszi lehetővé a felhasználók távoli kezelését. A központi felületről a kulcsok gyorsan kioszthatók vagy visszavonhatók.
A személyes adatok védelmének biztosítása	A DESlock Encryption a FIPS 140-2 level 1 minősítést érdemelte ki, és megbízható, elismert, biztonságos, az iparági szabványoknak megfelelő titkosítási algoritmusokat és módszereket alkalmaz.
A felesleges adat biztonságos megsemmisítése	A DESlock+ Desktop Shredder eszköz a DoD-5220.22-M-ben foglaltaknak megfelelően, biztonságosan törli le az adatokat, így azok visszaállítása egyáltalán nem lehetséges.

További információ (angol nyelven)

Hogyan segíthet az ESET az GDPR kapcsán:

https://encryption.eset.com/

Az EU adatvédelmi rendeletének megújítása:

http://ec.europa.eu/justice/data-protection/reform/

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

PRÓBÁLJA KI INGYEN A DESLOCK ENCRYPTION SZOFTVERT

Tudjon meg többet az **encryption.eset.com** oldalon

eset ENJOY SAFER TECHNOLOGY™

Sicontact Kft.
Budapest
Sajka u. 4.
1023