GDPR Megfelelőségi Audit

ELŐADÓ: MÁRKY DONÁT

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

A GDPR számokban

• Egyes számítások szerint az EU-tagállamokra jelenleg érvényes **28 különböző adatvédelmi szabály** megismerésére irányuló oktatások mintegy **130 millió eurót emésztenek fel.**
• Becslések szerint **a GDPR bevezetése 2,3 milliárd eurót takarít meg a gazdaság számára.**
• Több mint **4** éves előkészületi munka előzte meg a GDPR megjelenését
• A GDPR 88 oldal terjedelmű.
• A GDPR **7 alapelvre** épül.
• A GDPR elvárásait alapvetően **4** területre vonatkozó elvárás-gyűjteménynek is lehet értelmezni:
• Jogi elvárások
• Szervezeti elvárások
• Folyamati elvárások
• Technológia elvárások
• **És végül a legfontosabb szám: 20 millió euró, azaz megközelítőleg 6 milliárd forint.**
• A GDPR megszegéséért ugyanis ennyi lesz a maximálisan kiszabható büntetés.
• Ha tehát eddig az Ön cége még nem kezdte volna meg a rendelet bevezetésére való felkészülést, most még időben reagálhatnak. **2018. május 25**. már igen közel van, különösen ha egy ilyen volumenű változást kell integrálnia vállalkozása életébe.

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

A GDPR alapelvei

1. Jogszerűség, tisztességes eljárás és átláthatóság [5. cikk (1) a)]
2. Célhoz kötöttség [5. cikk (1) bek. b) pont]
3. Adattakarékosság [5. cikk (1) bek. c) pont]
4. Pontosság [5. cikk (1) bek. d) pont]
5. Korlátozott tárolhatóság [5. cikk (1) bek. e) pont]
6. Integritás és bizalmas jelleg (adatbiztonság) [5. cikk (1) bek. f) pont]
7. Elszámoltathatóság [5. cikk (2) bek.]

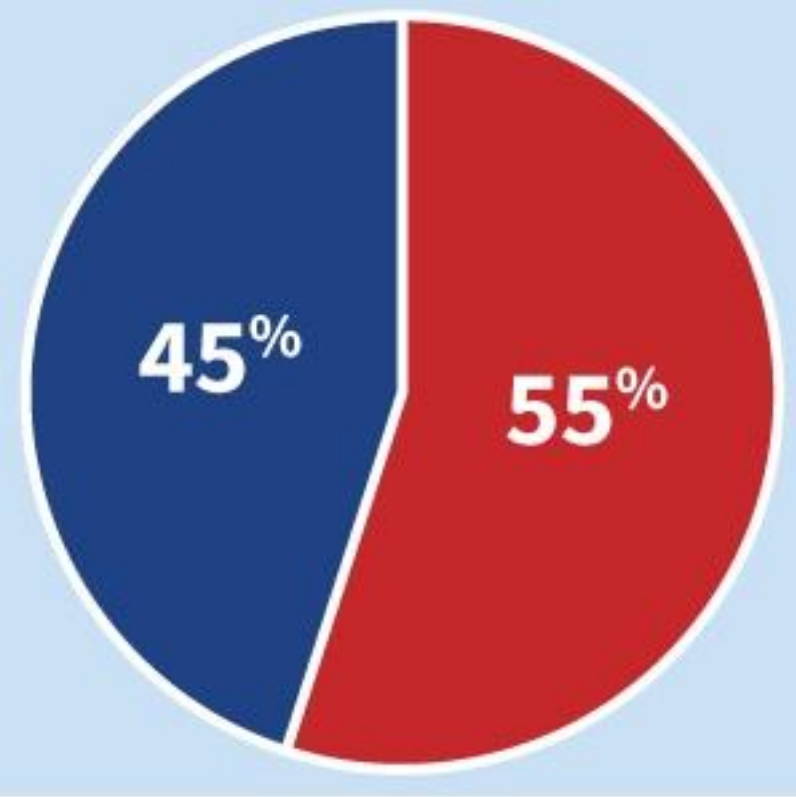
A GDPR legfontosabb alapfogalmai

- **Adatkezelő**
- **Adatfeldolgozó**
- **Érintettek**
- **Személyes adat fogalma:** 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.

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

A GDPR felkészülési projekt összetétele



45% IT feladatok, 55% jogi és folyamatszabályozási feladatok

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

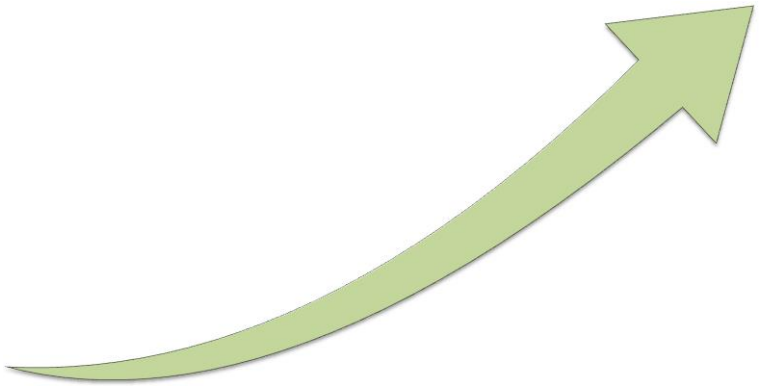
Bizonyára egyetértünk abban, hogy az olaj az évszázad legnagyobb üzlete, viszont a szakértők szerint napjainkban már az adat az új olaj (DATA is the new oil). Amennyiben megértjük és elfogadjuk ezt az új állítást, akkor kijelenthetjük, hogy napjainkban, illetve a jövőben az egyik legfontosabb feladat az új olaj (az adat) megvédése lesz.

Az IBM legutoljára 2014-ben becsülte meg, hogy 24 óra alatt az emberiség mennyi adatot termel, az akkori mérések szerint naponta 2,5 milliárd gigabájtnyi adattal lettünk gazdagabbak. Viszont 2017-ben az egy nap alatt keletkezett adatmennyiséget már megbecsülni sem tudták…

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

Tavaly 86,4 milliárd dollárt költ a világ IT-biztonsági termékekre és szolgáltatásokra, állítja előrejelzésében a Gartner. Ez 7 százalékos bővülést jelent a tavalyi költségez képest. A piac bővülése jövőre is folytatódik, a piackutató becslései szerint 2018-ban eléri a 93 milliárd dollárt. Az egyik leggyorsabb bővülő szegmens a tesztelés lesz, igaz, meglehetősen alacsony bázisról – teszik hozzá az elemzők. Ebben az alkalmazásbiztonsági tesztelés kap nagy szerepet a DevOps terjedése és az adatszivárgási problémák gyakorisága miatt.



A növekedés érthető, a vállalatok menedzsmentje számára egyre nyilvánvalóbb, hogy szoros kapcsolat van a biztonsági incidensek és az üzlet sikere között, így hajlandók több erőforrást biztosítani a területnek.

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

1, Titoktartási Megállapodás

2, Kérdőív:

- Mo-i szervezeti ábra, pozíciókkal, hozzávetőleges létszámmal
- Telephelyek, érdekeltségek az EU_n belül, ahol adatkezelés folyik, folyhat, nagyságrendi létszámok
- Telephelyek, érdekeltségek az EU-n kívül, ahol adatkezelés folyik, folyhat, nagyságrendi létszámok
- Létezik-e adattérkép a szervezet informatikai rendszereiben tárolt adatairól (igen/nem)? Van-e részletes nyilvántartás a tárolt személyes adatokról?
- Létezik-e iratkezelési szabályzat, vagy más belső szabályozás a személyes adatokat tartalmazó dokumentumok kezelésére?

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

- Jelenlegi adatkezelési, adatvédelmi szabályzatok elérhetőségei (elegendő az internetes link)

- Van-e kijelölt adatvédelmi felelős?

- Adatkezelést, adatfeldolgozást megvalósító partnerek, szállítók, vevők csoportjai (pl: munkaerő toborzás, munkaerő kölcsönzés, könyvelés, bérszámfejtés, biztonsági szolgálat, szállítmányozó, kereskedelmi partner, képviselő, IT üzemeltetés (pl nyomtató bérlés is), pénzintézet, franchise partner, kutatásban résztvevők köre stb.)

- Létezik-e adattörlési selejtezési, vagy megsemmisítési szabályzat?

- Létezik-e IT biztonsági szabályzat, amennyiben igen, akkor milyen előírásai vannak?

GDPR Megfelelőségi Audit, 1. Fázis

1, IT RENDSZEREK, KEZELT ADATOK

2, SZABÁLYOZÁSI KÖRNYEZET FELMÉRÉSE

3, ÁTTEKINTŐ ADATTÉRKÉP KÉSZÍTÉSE

4, INFORMATIKAI ADATVÉDELMI KOCKÁZATOK AZONOSÍTÁSA

5, GAP ANALÍZIS

6, INTÉZKEDÉSI/AKCIÓ TERV

GDPR Megfelelőségi Audit, 2. Fázis

1, IT BIZTONSÁGI MEGOLDÁSOK

2, INTÉZKEDÉSI/AKCIÓ TERV MEGVALÓSÍTÁSI FOLYAMAT

3, FOLYAMATSZABÁLYOZÁS

4, ADATVÉDELMI HATÁSVIZSGÁLAT

5, JOGI TANÁCSADÁS, AUDIT

6, ADATVÉDELMI AUDIT

7, GDPR BEVEZETÉS, OKTATÁS

SZÁLLÍTANDÓ DOKUMENTUMOK LISTÁJA
1-es fázis

a.) A személyes adatok kezelésében érintett folyamattérképek, szövegszerűen, folyamatábrákkal, feltűntetve a kezelt adatokat.
b.) Folyamat orientált megközelítés és eszköz/alkalmazás oldali felmérés eredményeképp átfogó adattérkép(ek) készítése, feltüntetve a kezelt személyes adatok előfordulását, fellelhetőségét az érintett rendszereket, folyamatokat, közreműködőket.
c.) GAP analízis - jelenlegi állapot az összegyűjtött és ügyféltől megkapott anyagok, adattérkép és a GDPR elvárások közti eltérések.
d.) Intézkedési terv készítése a GAP analízis alapján – 3-as besorolásban: High/Medium/Low risk. Az elvégzendő feladatok prioritásairara javaslatot teszünk, ennek elfogadása az Megrendelő feladata.

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

SZÁLLÍTANDÓ DOKUMENTUMOK LISTÁJA
2-es fázis

a.) A szükséges hiányzó szabályzatok adatvédelmi bekezdéseinek elkészítése, javaslat a szabályzatok tartalmi elemeire – együttműködve az Ügyféllel - az 1 fázisban elkészített intézkedési terv prioritási sorrendje szerint.
b.) A rendelkezésre álló szabályzatok adatvédelmi bekezdéseinek módosítása tipizált estekre (pl. alvállalkozói, adatfeldolgozói kiegészítések) az Intézkedési terv, illetve annak prioritásai sorrendje alapján időrendben – Megrendelő közreműködésével
c.) Javaslat a szükséges szervezeti, folyamatbeli változtatásokra
d.) Adatvédelmi incidens kezelési eljárás(ok) kidolgozása a feltételezhető tipizált esetek kezelésére.
e.) Adatvédelmi hatásvizsgálat, mely tartalmazza a megvalósult változtatások, változások elemeit, bemutatva a szervezet adatvédelmi megoldásait, folyamatait, szervezeti biztosítékait, kitérve az adatkezelési incidensek kezelésére, valamint a megelőző intézkedésekre.
f.) Oktatás, elkészült módosítások, szabályozási környezet bemutatása, ismertetése 1x3 óra részletes vezetői ismertetés, illetve igény szerint 1x1,5 óra dolgozói tájékoztatás terjedelemben.

Informatikai sérülékenység vizsgálat (Ethical Hacking)

A sérülékenység vizsgálat (Etikus Hack) egy vállalat informatikai rendszerén végzett biztonsági tesztelési folyamat, amely a kritikus biztonsági rések feltárása irányul, ezáltal csökkentve a rosszindulatú támadások sikerességét. A sérülékenység vizsgálat során képet kapunk az adott rendszer aktuális állapotáról

A vizsgálat lehet Black-Box, Grey-Box, illetve White-Box megközelítésű, az előzetesen rendelkezésünkre bocsátott információk függvényébe. A vizsgálat hatóköre (scope) skálázható az átadott információk tükrében.

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO

KÖSZÖNÖM A FIGYELMET!

27 years
DUNA ELEKTRONIKA
ALWAYS BY YOUR SIDE

BDO