SANS SECURITY AWARENESS

Havi biztonság tudatossági hírlevél mindenkinek

GDPR

Áttekintés

Talán ismerős lehet az új GDPR-nak nevezett szabályozás, vagyis az általános adatvédelmi rendelet. Ezt a jogszabályt az Európai Unió fogalmazta meg és 2018. május 25-től alkalmazandó. Hatálya kiterjed minden szervezetre, ami európai uniós állampolgárok személyes adatait kezeli, függetlenül attól, hogy az adott cégnek a világ mely részén van a székhelye. A GDPR megköveteli a szervezetektől, hogy védjék a magánszemélyek személyes adatainak biztonságát és bizalmasságát. A GDPR-nak történő megfelelés érdekében több fő alapelv megismerése és végrehajtása szükséges.

Az embereknek joguk van a magánélethez. A szervezeteknek tisztelniük kell az emberek magánéletet egyrészt úgy, hogy korlátozzák, hogy milyen információkat gyűjtenek és dolgoznak fel a magánszemélyekről, valamint ezen az adatokat megvédésével. Az adatvédelmi kötelezettség kiterjed minden olyan információra, mely alapján vagy önmagában, vagy más információkkal együtt alkalmazva egyértelműen be lehet azonosítani az EU területén élő magánszemélyt. Ez az információ lehet akár lakcím, útlevélszám, jogosítványszám, pénzügyi adat, biometrikus adat, szakszervezeti tagság egészségügyi történet, helyadat, vagy információ a személy szexuális, politikai vagy vallási irányultságára vonatkozóan.

A magánszemélyek személyes adatai csak a jogszabályoknak megfelelően, méltányosan és átlátható módon kezelhetőek.

Közölni kell az emberekkel, hogy milyen adatot milyen céllal gyűjt az adatkezelő.

Személyes adat csak célhoz kötve, kifejezett és jogszerű cél érdekében gyűjthető. A személyes adat ezekkel a célokkal ellentétes célokra nem használható fel.

Személyes adat kizárólag csak annyi ideig tárolható és kezelhető, ami a cél eléréséhez szükséges, semmi esetre sem hosszabb ideig.

A kezelt személyes adatot mindig pontosan és naprakészen kell tartani.

A magánszemélyeknek joguk van arra, hogy a tárolt személyes adataikról másolatot kapjanak, megtilthatják a személyes adatuk további kezelését, de bizonyos esetekben akár azok teljes törlését is kérhetik.

Az adatkezelőknek megfelelő biztonsági intézkedéseket kell tenniük a személyes adatok védelme érdekében, különösen a véletlen vagy törvénytelen megsemmisítés, elvesztés, módosítás vagy nyilvánosságra hozatal ellen.

Továbbá, az adatkezelőnek biztosítania kell az adatkezelést végző személyi állományának a biztonságos adatkezelésre és adatvédelemre vonatkozó képzést.

Az alkalmazott védelmi megoldásoknak a kezelt adatok érzékenységének megfelelő szintű védelmet kell biztosítaniuk. Ahogy a személyes adathoz társított kockázat mértéke nő, úgy kell nőnie az adatvédelemre fordított erőfeszítésnek és az intézkedésekre fordított költségének is. Az alkalmazott intézkedéseket rendszeresen felül kell vizsgálni és szükség esetén frissíteni kell. Az adatvédelemmel kapcsolatos döntéseket dokumentálni kell a követelmények való megfelelés tanúsítása érdekében. Mindezeken túlmenően a szervezetek kötelezettek olyan intézkedések meghozatalára, mint például szerződések vagy megfelelősségi ellenőrzések annak érdekében, hogy azon személyes adatok, amik harmadik félnek, vagy különösen az Európai Unión kívüli partnernek kerülnek továbbításra, megfelelő védelmet élvezzenek. Végezetül, személyes adat kiszivárgása esetén a szervezeteknek a tudomásra jutást követően 72 órán belül jelenteniük kell azt. Azon szervezet, amely nem felel meg a GDPR rendelkezéseinek akár az összbevétele 4% -ára is büntethető, ezzel a GDPR lett a világon az egyik “legdrágább” szabály.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

A szerzőről

Brian Honan *a független, konzultációval, kiberbiztonsággal valamint adatvédelemmel foglalkozó BH Consulting ügyvezetője, melynek székhelye Dublinban, Írországban található. Brian az Europol Számítástechnikai Bűnözés Elleni Európai Központ (EC3) különleges tanácsadója volt, Írország első CERT-jének alapítója, és több, biztonsággal foglalkozó innovatív cég tanácsadó testületében is jelen van. Brian megtalálható a LinkedIn-en (* www.linkedin.com/in/brianhonan), illetve követhetjük a twitteren a @brianhonan azonosítót bejelölve.

Hivatkozások

GDPR áttekintés magánszemélyeknek és intézményeknek:	http://gdprandyou.ie
A GDPR rendelet:	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
OUCH! Fordítások és archívum:	https://www.sans.org/u/D88