Microsoft-beszállítókra vonatkozó adatvédelmi követelmények

Alkalmazás

A Microsoft-beszállítókra vonatkozó adatvédelmi követelmények („**DPR**") minden egyes Microsoft-beszállítóra vonatkoznak, amely személyes Microsoft-adatokat vagy bizalmas Microsoft-adatokat kezel az adott beszállító által nyújtott teljesítéssel összefüggésben (pl. szolgáltatások nyújtása, szoftverlicencek, felhőszolgáltatások), a Microsofttal kötött szerződése feltételei szerint (pl. beszerzési rendelésekben szereplő feltételek, keretszerződés) („**teljesít**", „**teljesítés folyamatban**" vagy „**teljesítés**").

- Amennyiben a DPR, valamint a beszállító és a Microsoft között létrejött szerződéses megállapodásokban rögzített követelmények között ellentmondás lenne, akkor a DPR élvez elsőbbséget, kivéve, ha a beszállító azonosítja a szerződésben azt a megfelelő rendelkezést, amely elsőbbséget élvez az alkalmazandó adatvédelmi követelménnyel szemben (amely esetben a szerződés feltételei élveznek elsőbbséget).
- Amennyiben a jelen dokumentumban rögzített követelmények és bármilyen törvényi vagy jogszabályi követelmény között ellentmondás lenne, a törvényi vagy jogszabályi követelmények élveznek elsőbbséget.
- Amennyiben a Microsoft-beszállító Adatkezelőként tevékenykedik, a beszállítóra csökkentett követelmények vonatkozhatnak a DPR-ben.
- Amennyiben a Microsoft-beszállító nem dolgoz fel személyes Microsoft-adatokat, csak bizalmas Microsoft-adatokat, a jelen DPR vonatkozásában a beszállítóra csökkentett követelmények vonatkozhatnak.

Az adatok nemzetközi továbbítása

Egyéb kötelezettségeinek korlátozása nélkül a beszállító nem végezheti el a személyes Microsoft-adatok nemzetközi továbbítását, kivéve, ha erre a Microsoft előzetes írásos jóváhagyást ad, továbbá a beszállítónak minden esetben meg kell felelnie az Adatvédelmi követelményeknek (Data Protection Requirements – DPR), ideértve az Általános szerződési feltételeket, vagy a – Microsoft belátása szerinti – megfelelő adatvédelmi hatóság vagy az Európai Bizottság által jóváhagyott, hatályos és a Microsoft által bevezetett vagy elfogadott, határokon átnyúló továbbítási mechanizmusokat. Az (i) Európai Bizottság vagy az európai adatvédelmi biztos által elfogadott és az Európai Bizottság által jóváhagyott, (ii) az Egyesült Királyság által az Egyesült Királyság általános szövetségi adatvédelmi törvénye értelmében elfogadott, (iii) Svájc által a svájci szövetségi adatvédelmi törvény értelmében elfogadott általános szerződéses feltételeket, vagy (iv) a Svájcon, az Egyesült Királyságon és az Európai Unió/Európai Gazdasági Térség joghatóságain kívüli más joghatóság által hivatalosan elfogadott, a személyes adatok nemzetközi továbbítását szabályozó rendelkezéseket be kell építeni, és a beszállítóra nézve az elfogadásuk napjától kezdve kötelező érvényűnek kell tekinteni. A beszállítónak emellett azt is biztosítania kell, hogy a fentieknek bármely és minden további (az Általános szerződési feltételekben meghatározott) adatfeldolgozó megfeleljen.

Alapvető fogalommeghatározások

A jelen DPR-ben használt alábbi kifejezések jelentése a következő. A DPR-ben használt példák listái, amelyek olyan kifejezéseket követnek, mint „többek között", „úgymint", „pl.", „például" vagy ehhez hasonló kifejezéseket, úgy értelmezendők, hogy azok magukban foglalják a „korlátozás nélkül" vagy a „nem kizárólagosan" kifejezéseket, kivéve, ha azokat a „csak", „kizárólag" vagy ehhez hasonló szavakkal jelölték. A további meghatározásokat lásd a dokumentum végén található Szószedetben.

Az „**Adatfeldolgozó**" olyan szervet jelöl, amely egy másik szerv nevében személyes adatokat kezel, és magában foglalja a Szolgáltatót, az Adatkezelőt (a kifejezés GDPR szerinti meghatározása alapján), valamint – kontextustól függően – az adatvédelmi törvények egyenértékű kifejezéseit.

Az „**Adatkezelő**" azt a jogalanyt jelöli, amely meghatározza a személyes adatok feldolgozásának céljait és eszközeit. Az „adatkezelő" magában foglalja a Vállalkozást, az Adatkezelőt (a kifejezés GDPR szerinti meghatározása alapján), valamint – kontextustól függően – az adatvédelmi törvények egyenértékű kifejezéseit.

Az „**adatvédelmi incidens**" (1) a biztonság olyan jellegű sérülése, amely a beszállító vagy a beszállító alvállalkozói által továbbított, tárolt vagy más módon kezelt személyes Microsoft-adatok vagy bizalmas Microsoft-adatok véletlen vagy

jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi; vagy (2) a személyes Microsoft-adatok vagy bizalmas Microsoft-adatok beszállító általi kezelésével kapcsolatos biztonsági rés.

Az „**Alvállalkozó**" az a harmadik fél, akire a beszállító a saját teljesítésére vonatkozó szerződéssel kapcsolatos kötelezettségeit átruházza; ide tartozik a beszállító kapcsolt vállalkozása is, amely nem áll közvetlen szerződéses viszonyban a Microsofttal.

A „**bizalmas Microsoft-adatok**" olyan adatok, amelyek titkosságuk vagy sértetlenségük bármilyen eszközzel történő veszélyeztetése esetén jelentős hírnévbeli vagy pénzügyi veszteséget okozhatnak a Microsoftnak. Ez a következőket foglalja magában: Microsoft-hardver- és -szoftvertermékek, belső üzletági alkalmazások, megjelenés előtti marketinganyagok, terméklicenckulcsok, valamint Microsoft-termékekkel és -szolgáltatásokkal kapcsolatos technikai dokumentációk.

Az „**Érintett**" olyan beazonosítható természetes személy, aki közvetlen vagy közvetett módon azonosítható, különösen valamely azonosító, például név, azonosító szám, helyadatok, online azonosító, vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális identitására vonatkozó egy vagy több tényező alapján.

Az „**Érintett joga**" az Érintettnek arra vonatkozó joga, hogy a személyes Microsoft-adatokhoz hozzáférjen, azokat törölje, szerkessze, exportálja, korlátozza vagy azok feldolgozásával kapcsolatosan ellenvetését fejezze ki, amennyiben az jogszabályi kötelezettség.

A „**feldolgozás**" olyan műveletet vagy műveletsort jelent, amelyet a személyes vagy bizalmas Microsoft-adatokon hajtanak végre, akár automatizált, akár nem automatizált módon, úgymint azok gyűjtése, rögzítése, rendezése, strukturálása, tárolása, adaptálása vagy megváltoztatása, lekérése, megtekintése, használata, nyilvánosságra hozatala továbbítással, terjesztése vagy más módon történő elérhetővé tétele, kiigazítása vagy kombinálása, korlátozása, törlése vagy megsemmisítése. A „feldolgozás" és a „feldolgozott” szavak jelentése egymásnak megfeleltethető.

A „**jogszabály**" bármely joghatósággal rendelkező kormányzati szerv (szövetségi, állami, helyi vagy nemzetközi) valamennyi vonatkozó törvénye, szabálya, jogszabálya, törvényerejű rendelete, határozata, utasítása, rendelete, ítélete, törvénykönyve, végrehajtási rendelkezése, állásfoglalása és követelménye. A „**jogszerűtlen**" kifejezés a jogszabályok bármilyen megsértését jelenti.

A „**sütik**” a weboldalak, illetve alkalmazások által az eszközökön tárolt kis méretű szövegfájlok, amelyek egy érintett vagy egy eszköz felismerésére használt információkat tartalmaznak.

„**Személyes adat**" az Érintettel kapcsolatos összes adat, továbbá minden egyéb információ, amely a jogszabály alapján „személyes adatnak" vagy „személyes információnak" minősül.

A „**személyes Microsoft-adatok**" közé tartozik a Microsoft által vagy nevében feldolgozott minden személyes adat.

A „**További feldolgozó**" olyan harmadik fél, akivel a Microsoft teljesítést végeztet, ahol a teljesítés magában foglalja olyan személyes Microsoft-adatok kezelését, amelyek Kezelője a Microsoft.

Beszállítói válasz

A beszállítók a Microsoft által felügyelt online szolgáltatáson keresztül évente megerősítik a fenti követelményeknek való megfelelést. A SSPA program útmutatójában megtalálja, hogyan kell adminisztrálni a megfelelőséget.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	A. szakasz: Menedzsment	
1.	A Microsoft és a beszállító közötti összes vonatkozó megállapodás (pl. keretszerződés, munkaleírás, beszerzési rendelések és más megrendelések) a bizalmas és személyes Microsoft-adatokra vonatkozóan tartalmazza az adatvédelmi és -biztonsági elvek leírását – az alkalmazhatóságnak megfelelően –, beleértve a személyes Microsoft-adatok értékesítésének, valamint a személyes Microsoft-adatoknak a Microsoft és a beszállító közvetlen üzleti kapcsolatán kívüli feldolgozásának tilalmát. A teljesítéssel kapcsolatban Adatfeldolgozóként vagy További feldolgozóként működő vállalatok esetében a személyes Microsoft-adatokra vonatkozóan a szerződésnek tartalmaznia kell a feldolgozás tárgyát és időtartamát, a feldolgozás jellegét és célját, a személyes Microsoft-adatok típusát és az Érintettek kategóriáit, valamint a Microsoft kötelezettségeit és jogait.	A beszállítónak be kell mutatnia a Microsoft és a beszállító között létrejött, vonatkozó szerződést. Az Adatfeldolgozók és További feldolgozók számára az adatfeldolgozás leírását a vonatkozó szerződés (pl. munkaleírás, beszerzési rendelés) tartalmazza. Megjegyzés: A munka közben kiadott beszerzési rendelésekkel rendelkező vállalatoknál az Adatfeldolgozási tevékenységek szükséges leírása később is bekerülhet a beszerzési folyamatba.
2.	Amennyiben a Microsoft megerősíti, hogy Ön a kötelezettségvállalásai alapján További feldolgozó szerepét tölti be, akkor a beszállítónak hatályos adatvédelmi megállapodással kell rendelkeznie a Microsofttal. Megjegyzés: A Microsoft ezt a megnevezést az Ön profilján is megjeleníti, amennyiben ezt kell alkalmazni.	Általános szerződési feltételek, Online ügyféladat-melléklet, illetve Professzionális beszállítói vagy partneri szolgáltatási adatkezelési melléklet.
3.	Az adatvédelmi követelményeknek (DPR) való megfeleléssel kapcsolatos felelősséget és számonkérhetőséget egy kijelölt személyre vagy csoportra kell bízni a vállalaton belül.	A Microsoft beszállítói DPR-jének való megfelelésért felelős személy vagy csoport szerepkörének neve. Az adatvédelmi, illetve -biztonsági szerepkört betöltő személy vagy csoport jogosultságát és számonkérhetőségét leíró dokumentum.
4.	Éves adatvédelmi és -biztonsági oktatást kell kidolgozni, fenntartani és megvalósítani azon alkalmazottak számára, akiknek a teljesítéssel vagy a bizalmas Microsoft-adatokkal kapcsolatban hozzáférése lesz a beszállító által feldolgozott személyes adatokhoz. Ha az Ön vállalata nem rendelkezik ehhez előkészített tartalommal, használhatja ezt a vázlatot, amelyet vállalatára adaptálhat.	Az éves részvételi nyilvántartások elérhetők, és azok kérésre átadhatók a Microsoftnak. Az oktatási anyag magában foglalja az adatvédelmi és -biztonsági alapelveket. A képzési követelményeknek való megfelelés dokumentációja magában foglalja az adatvédelem jogszabályi követelményeivel és a biztonsági kötelezettségekkel kapcsolatos képzést igazoló dokumentumokat, továbbá a vonatkozó szerződéses

	Megjegyzés: A beszállító alkalmazottai kötelezhetők arra, hogy a Microsoft részlegei által szervezett további képzéseken részt vegyenek.	követelményeknek és kötelezettségeknek való megfelelést alátámasztó dokumentumokat is.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	A. szakasz: Menedzsment (folyt.)	
5.	A személyes Microsoft-adatokat csak a Microsoft dokumentált útmutatásának megfelelően dolgozhatja fel, ideértve a személyes Microsoft-adatok harmadik országba vagy nemzetközi szervezethez történő továbbításának eseteit, kivéve, ha arra jogszabály kötelezi; ebben az esetben az Adatfeldolgozónak vagy a További feldolgozónak (szállítónak) a feldolgozás előtt tájékoztatnia kell az Adatkezelőt (a Microsoftot) az adott jogi előírásról, kivéve, ha a jogszabály közérdekbe ütközőnek minősíti az ilyen jellegű tájékoztatást.	A beszállító a Microsoft minden dokumentált útmutatását (pl. szerződés, feladatleírás vagy megrendelési dokumentáció) elektronikusan gyűjti össze és őrzi meg, és a teljesítésben részt vevő beszállítói alkalmazottak és alvállalkozók számára könnyen hozzáférhető helyen tárolja.
	B. szakasz: Értesítés	
6.	A beszállító köteles használni a Microsoft adatvédelmi nyilatkozatát, amikor személyes adatokat gyűjt a Microsoft nevében. Az adatvédelmi értesítőnek egyértelműnek és elérhetőnek kell lennie az Érintettek számára, hogy eldönthessék, átadják-e személyes adataikat a beszállítónak. Megjegyzés: Ha az Ön vállalata az adatfeldolgozási tevékenység Adatkezelője, akkor saját adatvédelmi értesítőjét kell közzé tennie.	A beszállító egy fwdlink hivatkozáson keresztül érheti el az aktuális, Microsoft által közzétett adatvédelmi nyilatkozatot. Az Adatvédelmi nyilatkozat minden olyan összefüggésben közzé van téve, amikor a felhasználó személyes adatainak összegyűjtésére kerül sor. Ahol releváns, az adatgyűjtés előtt elérhető és biztosított az offline verzió. A felhasznált offline Adatvédelmi nyilatkozat minden esetben a legújabb, közzétett verziójú dokumentum a megfelelő dátummal. A Microsoft munkatársainak nyújtott szolgáltatásokhoz a Microsoft adatvédelmi értesítőjét használják.
7.	Ha a személyes Microsoft-adatok gyűjtése élő vagy rögzített hanghívás útján történik, a beszállítóknak fel kell készülniük arra, hogy az Érintettel megbeszéljék a vonatkozó adatgyűjtési, -kezelési, -felhasználási és -megőrzési gyakorlatokat.	A hangfelvételek átirata tartalmazza a személyes Microsoft-adatok feldolgozásának módját, többek között az alábbiakat: ▪ adatgyűjtés, ▪ felhasználás, ▪ megőrzés.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	C. szakasz: Választási lehetőség és beleegyezés	
8.	Amennyiben ez helyénvaló, a beszállítónak be kell szereznie és dokumentálnia kell az Érintett beleegyezését az összes adatfeldolgozási tevékenységéhez (beleértve bármely új és frissített adatfeldolgozási tevékenységet) még azelőtt, hogy elkezdené az Érintett személyes adatainak gyűjtését. A beszállító felügyeli a választási lehetőségek kezelésének hatékonyságát, hogy a preferenciák módosítására vonatkozó kötelezettség betartására rendelkezésre álló időtartam a legkorlátozóbb alkalmazandó helyi jogi követelmény legyen.	A beszállító be tudja mutatni, hogyan adja beleegyezését az Érintett az adatfeldolgozási tevékenységhez, és hogy a beleegyezés a beszállító teljes feldolgozási tevékenységét lefedi az Érintett személyes adatainak vonatkozásában. A beszállító be tudja mutatni, hogyan vonja vissza az Érintett a feldolgozási tevékenységhez adott beleegyezését. A beszállító be tudja mutatni, hogyan történik a preferenciák ellenőrzése az új adatfeldolgozási tevékenység indítása előtt. Megjegyzés: A megfelelést igazolhatják felhasználói interakciókat bemutató képernyőképek, a szolgáltatás kipróbálása kísérletezés céljából vagy a műszaki dokumentáció megtekintésének lehetősége.
9.	Azoknak a beszállítóknak, amelyek Microsoft-weboldalakat és/vagy -alkalmazásokat vagy a Microsoft márkaelemeit tartalmazó oldalakat hoznak létre és kezelnek, az Érintettek számára látható értesítést és választási lehetőséget kell biztosítani a sütik használatával kapcsolatosan, a Microsoft adatvédelmi nyilatkozatában és a helyi jogszabályi követelményekben szereplő kötelezettségvállalásokkal összhangban. A beszállítóknak az 1ES által előállított standard szalagot kell használniuk a választási lehetőségek kezelésére, kivéve, ha a szerződő üzleti egység kifejezetten kéri, hogy ne ezt használják. Ez a követelmény azon esetekben alkalmazandó, amikor az oldal olyan felhasználókat céloz meg, akik az Európai Unióban/Európai Gazdasági Térségben, vagy egyéb, hatályos adatvédelmi törvényekkel rendelkező régiókban tartózkodnak, vagy bárhol máshol, ahol a Microsoft adatvédelmi nyilatkozata használatos. Megjegyzés: A Microsoft üzleti szponzorainak a sütik készletének katalogizálására és kezelésére a belső Web Compliance webes megfelelőségi portálon (http://aka.ms/wcp) kell regisztrálniuk a Microsoft-webhelyeket.	Minden egyes süti célját dokumentálni kell, és tájékoztatást kell nyújtani az alkalmazott süti típusáról. ▪ Állandó sütiket nem szabad használni, ha a munkamenet-sütik is elegendőek. ▪ Állandó sütik használata esetén ezek lejárati dátuma nem haladhatja meg a felhasználó webhelyen tett látogatásától számított 13 hónapot. Igazolja az EU vonatkozó jogszabályainak való megfelelőséget, úgymint: ▪ az egyezményes címkézési jelölések használata, „Adatvédelem és sütik" az adatvédelmi nyilatkozat esetében, ▪ biztonságos felhasználói megerősítő beleegyezés a sütik használata előtt olyan „nem létfontosságú" célokra, mint pl. a hirdetések; és ▪ a beleegyezés legfeljebb 6 hónap után érvényét veszti, illetve újból meg kell szerezni.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	D. szakasz: Adatgyűjtés	
10.	A beszállítónak nyomon kell követnie a személyes, illetve bizalmas Microsoft-adatok gyűjtését annak biztosítására, hogy csak a teljesítéshez szükséges adatokat gyűjtsék össze.	A beszállító be tudja mutatni azt a dokumentációt, amely leírja, hogy az összegyűjtött személyes, illetve bizalmas Microsoft-adatokra szükség van a teljesítéshez. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
11.	Gyermekektől történő adatgyűjtés előtt (a vonatkozó jogszabályban meghatározottak szerint) a beszállítónak a helyi adatvédelmi törvényeknek megfelelően beleegyezést kell kapnia.	A beszállító be tudja mutatni a szülő/gondviselő beleegyezését bemutató dokumentációt. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
	E. szakasz: Megőrzés	
12.	Gondoskodik róla, hogy a személyes és bizalmas Microsoft-adatokat csak addig őrizzék meg, amíg ez a teljesítéshez szükséges, kivéve, ha jogszabály írja elő a személyes, illetve bizalmas Microsoft-adatok további megőrzését.	A beszállító eleget tesz a Microsoft által a szerződésben (pl. a munkaleírásban vagy a beszerzési rendelésben) rögzített, dokumentált megőrzési irányelveknek vagy megőrzési követelményeknek. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
13.	Gondoskodik róla, hogy – a Microsoft kizárólagos rendelkezése alapján – a beszállító a tulajdonában vagy a felügyelete alatt álló személyes vagy bizalmas Microsoft-adatokat visszaküldje a Microsoftnak, vagy megsemmisítse azokat a teljesítés befejezésekor vagy a Microsoft kérésére. Olyan folyamatokat kell beépíteni az alkalmazásokba, amelyek biztosítják, hogy az adatoknak az alkalmazásból történő eltávolításakor – amely történhet közvetlenül, a felhasználók által, vagy egyéb okok, például az adat kora miatt – megtörténjen azok biztonságos törlése. Ha a személyes vagy bizalmas Microsoft-adatok megsemmisítése szükséges, a beszállítónak a személyes, illetve bizalmas Microsoft-adatokat tartalmazó fizikai eszközöket el kell égetnie, porrá kell zúznia vagy össze kell törnie, hogy az adatok ne legyenek olvashatók vagy helyreállíthatók.	A beszállító megőrzi a személyes és bizalmas Microsoft-adatokkal való rendelkezés bizonylatait (ez magában foglalhatja a Microsoftnak történő visszaküldést is megsemmisítés céljából). Ha a Microsoft az adatok megsemmisítését írja elő vagy kéri, a beszállító be tudja mutatni a beszállító tisztviselője által aláírt tanúsítványt az adatok megsemmisítéséről.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	F. szakasz: Érintettek	
	Az Érintetteket a jogszabály alapján különféle jogok illetik meg, így például a személyes adataikhoz való hozzáférés, a személyes adataik törlésének, szerkesztésének, exportálásának, korlátozásának joga, továbbá a személyes adataik kezelése elleni tiltakozás joga (az „**Érintett jogai**”). Ha az Érintett a személyes Microsoft-adatai tekintetében gyakorolni kívánja a jogszabály szerint őt megillető jogokat, a beszállító köteles lehetővé tenni a Microsoft számára az alábbiakat, illetve köteles a Microsoft nevében végrehajtani a következő intézkedéseket:	
14.	A Microsoft támogatása a megfelelő technikai és szervezeti intézkedésekkel, ahol lehetséges, hogy késedelem nélkül teljesíthesse kötelezettségét a jogaik gyakorlását kezdeményező Érintettek kéréseire vonatkozó válaszadással kapcsolatosan. Ha a Microsoft másképp nem rendelkezik, a beszállító átirányít a Microsofthoz minden olyan Érintettet, aki közvetlenül veszi fel vele a kapcsolatot az érintettek jogainak gyakorlására.	A beszállító nyilvántartást vezet az érintettek jogainak végrehajtását támogató dokumentált folyamatokról és eljárásokról. A beszállító nyilvántartást vezet a tesztelésről. A Microsoft kérésére a beszállító rendelkezésre bocsátja a nyilvántartást.
15.	Ha a beszállító közvetlenül válaszol az Érintettnek, vagy ha önkiszolgáló online mechanizmust biztosít, akkor a beszállítónak rendelkeznie kell a kérelmet benyújtó Érintett azonosítására szolgáló folyamatokkal és eljárásokkal.	A beszállító dokumentálja a Microsoft-Érintettek azonosítására használt módszert. A Microsoft kérésére a beszállító rendelkezésre bocsátja a dokumentált bizonyítékot.
16.	Ha a Microsoft az Érintettre vonatkozó olyan személyes Microsoft-adatok helyének meghatározására kéri a beszállítót, amelyekhez nem lehet önkiszolgáló mechanizmuson keresztül hozzáférni, a beszállítónak észszerű erőfeszítést kell tennie a kért adatok helyének meghatározására, és elégséges nyilvántartást kell vezetnie arról, hogy az észszerű mértékű keresést elvégezte.	A beszállító dokumentált nyilvántartást vezet az annak megállapítására szolgáló eljárásokról, hogy megtörténik-e a személyes Microsoft-adatok megőrzése, és a Microsoft kérésére rendelkezésre bocsátja a dokumentációt. A beszállító nyilvántartást vezet az Érintettek jogaival kapcsolatos kérések teljesítése során megtett lépésekről. A dokumentáció tartalmazza: ▪ a kérelem dátumát és idejét, ▪ a kérelemre válaszul adott intézkedéseket és annak a bejegyzését, hogy mikor történt meg a Microsoft tájékoztatása. A Microsoft kérésére a beszállító rendelkezésre bocsátja a nyilvántartás vezetését alátámasztó bizonyítékot.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	F. szakasz: Érintettek (folyt.)	
17.	A beszállítónak tájékoztatnia kell minden Érintettet azokról a lépésekről, amelyeket meg kell tennie ahhoz, hogy hozzáférést nyerjen a Microsoft-adatokhoz, vagy más módon gyakorolhassa a személyes Microsoft-adataival kapcsolatos jogait.	A beszállító dokumentált nyilvántartást vezet a személyes Microsoft-adatokhoz való hozzáféréssel kapcsolatos kommunikációról és eljárásokról. A beszállító dokumentált nyilvántartást vezet, és a Microsoft kérésére rendelkezésre bocsátja azt.
18.	Jegyezze fel az Érintettek jogai alapján indított kérelmek dátumát és időpontját, illetve a beszállító által ezen kérelmek teljesítésére megtett intézkedéseket. A kérelem elutasítása esetén – a Microsoft utasítása alapján – írásos magyarázattal kell szolgálni az Érintettnek. A Microsoft kérésére mutassa be az Érintettek kérelmeiről vezetett nyilvántartást.	A beszállító nyilvántartást vezet a hozzáférési/törlési kérelmekről, és dokumentálja a személyes adatokban végrehajtott változtatásokat. Dokumentálja azokat az eseteket, amelyekben a kérelmet visszautasították, és megőrzi a Microsoft véleményezését és jóváhagyását igazoló bizonyítékot. A beszállító átadja a személyes Microsoft-adatokhoz való hozzáférés iránti kérelmek és a hozzáférés-megtagadások nyilvántartásának bizonyítékát.
19.	A beszállítónak lehetővé kell tennie a Microsoft számára, hogy megfelelő nyomtatott vagy elektronikus formában, illetve szóban jusson hozzá a hitelesített Érintett számára kérelmezett személyes Microsoft-adatok egy példányához.	A beszállító a személyes adatokat az Érintett számára érthető, valamint az Érintett és a beszállító számára megfelelő formában adja át.
20.	A beszállítónak észszerű óvintézkedéseket kell tennie annak érdekében, hogy a Microsoftnak vagy valamely hitelesen beazonosított Érintettnek kiadott személyes Microsoft-adatokat ne lehessen felhasználni másik személy azonosítására.	A beszállító dokumentált nyilvántartást vezet azokról az óvintézkedésekkel kapcsolatos eljárásokról, melyek célja, hogy az Érintettet ne a Megállapodás feltételeit sértő módon azonosítsák be. A Microsoft kérésére a beszállító rendelkezésre bocsátja az ezt alátámasztó bizonyítékot.
21.	Ha egy Érintett úgy gondolja, hogy személyes Microsoft-adatai hiányosak és pontatlanok, a beszállító köteles felterjeszteni az ügyet a Microsofthoz, és az ügy megoldása érdekében – a szükséges mértékben – köteles együttműködni a Microsofttal.	A beszállító dokumentálja a nézeteltérés eseteit, és az ügyet felterjeszti a Microsofthoz. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	G. szakasz: Alvállalkozók	
	Ha a beszállító alvállalkozót kíván alkalmazni a személyes vagy bizalmas Microsoft-adatok feldolgozásához, az alábbiakat kell elvégeznie:	
22.	A szolgáltatások alvállalkozónak történő kiszervezése, valamint az alvállalkozói kör helyettesítését vagy bővítését érintő változtatás előtt értesítenie kell a Microsoftot. Megjegyzés: Akkor is jeleznie kell ezen kötelezettség elfogadását, ha jelenleg nem alkalmaz alvállalkozót, de a jövőben ez előfordulhat.	Igazolnia kell, hogy a személyes Microsoft-adatokat csak a Microsoft számára ismert vállalatok dolgozták fel, amint azt a vonatkozó szerződés (pl. munkaleírás, kiegészítés, beszerzési rendelés) megköveteli, vagy ahogyan azt az SSPA-adatbázisban rögzítették. A beszállítónak online elérhetővé kell tennie az alvállalkozói listáját, és egy linket kell elhelyeznie az SSPA-adatbázisban található oldalon.
23.	Dokumentálnia kell az alvállalkozók által további feldolgozásra kijelölt személyes vagy bizalmas Microsoft-adatok jellegét és mennyiségét, biztosítva, hogy csak a teljesítéshez szükséges adatok legyenek begyűjtve.	A beszállító nyilvántartást vezet az alvállalkozókkal közölt vagy részükre átadott személyes és bizalmas Microsoft-adatokról. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
24.	Abban az esetben, ha a Microsoft a személyes Microsoft-adatok Adatkezelője, gondoskodni kell róla, hogy az alvállalkozó a személyes Microsoft-adatokat kizárólag az érintett által megadott kapcsolatfelvételi módnak megfelelően használja fel.	Be kell mutatnia, hogy az alvállalkozók hogyan alkalmazzák a Microsoft-Érintettek által megadott preferenciákat. Támogató dokumentációt (pl. képernyőkép, szolgáltatási szintre vonatkozó megállapodás (SLA), munkaleírás (SOW)) biztosít, amely az alvállalkozó számára tartalmazza a megadott preferenciamódosítás teljesítéséhez szükséges időtartamot.
25.	A személyes vagy bizalmas Microsoft-adatok alvállalkozó általi feldolgozását azokra a célokra kell korlátoznia, amelyek a beszállító és a Microsoft között érvényes szerződés teljesítéséhez szükségesek.	A beszállító be tud mutatni olyan dokumentációt, amely leírja, hogy a teljesítéshez szükség van az alvállalkozónak átadott személyes Microsoft-adatokra. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
26.	Át kell tekintenie a személyes Microsoft-adatok engedély nélküli felhasználásával vagy jogszerűtlen feldolgozásával kapcsolatos panaszokat.	A beszállító be tudja mutatni, hogy rendszereket és eljárásokat alkalmaz azon panaszok kezelésére, amelyek az alvállalkozó által engedély nélkül felhasznált vagy kiadott személyes Microsoft-adatok esetén merülnek fel. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	G. szakasz: Alvállalkozók (folyt.)	
27.	Azonnal értesítenie kell a Microsoftot, ha tudomására jut, hogy egy alvállalkozó nem a teljesítéssel kapcsolatos célból dolgozta fel a személyes vagy bizalmas Microsoft-adatokat.	A beszállítónak útmutatót és eszközöket kell biztosítania az alvállalkozó számára a Microsoft-adatokkal való visszaélés jelentéséhez. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
28.	Ha a beszállító a Microsoft nevében külső felektől gyűjt be személyes adatokat, a beszállítónak ellenőriznie kell, hogy a külső fél adatvédelmi szabályzatai és gyakorlatai megfelelnek-e a beszállító és a Microsoft között érvényben lévő szerződésnek, illetve az adatvédelmi követelményeknek (DPR).	A beszállító be tudja mutatni az azt leíró dokumentációt, hogy gondosan jár el a harmadik fél adatvédelmi szabályzatait és gyakorlatait illetően. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
29.	Haladéktalanul meg kell tennie a megfelelő intézkedéseket a tényleges vagy lehetséges károk enyhítésére, amelyeket az alvállalkozó azzal okozott, hogy a személyes és bizalmas Microsoft-adatokat engedély nélkül vagy jogszerűtlenül dolgozta fel.	A beszállító dokumentált nyilvántartást vezet a tervről és az eljárásról, és a Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
	H. szakasz: Minőség	
30.	A beszállítónak meg kell őriznie valamennyi személyes Microsoft-adat sértetlenségét, biztosítva azok pontosságát, hiánytalanságát és helytállóságát azokra a megállapított célokra vonatkozóan, amelyek érdekében feldolgozásuk megtörtént.	A beszállító bizonyítani tudja, hogy eljárásokat alkalmaz a személyes Microsoft-adatok ellenőrzésére azok gyűjtésekor, létrehozásakor és frissítésekor. A beszállító igazolni tudja, hogy felügyeleti és mintavételi eljárásokkal biztosítja a pontosság folyamatos ellenőrzését, és szükség esetén annak kijavítását. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	I. szakasz: Felügyelet és végrehajtás	
31.	A beszállító rendelkezik az incidensek esetére kidolgozott cselekvési tervvel, amely megköveteli, hogy a beszállító a szerződéses követelményeknek megfelelően vagy indokolatlan késedelem nélkül – amelyik előbb következik be – értesítse a Microsoftot, amint a beszállító tudomására jut, hogy adatvédelmi incidens történt. A beszállítónak a Microsoft kérésére vagy utasítására együtt kell működnie a Microsofttal az incidens mindennemű kivizsgálása, mérséklése és megoldása során, így többek között a beszállítónak a Microsoft rendelkezésére kell bocsátania a feltáró jelentés elkészítéséhez szükséges adatokat, információkat, hardvert és a beszállító alkalmazottaihoz való hozzáférést. Megjegyzés: Az SSPA program útmutatójában megtalálja, hogyan kell a Microsoftot értesíteni az incidensekről.	A beszállítónak reagálási tervvel kell rendelkeznie incidensek esetére, amely tartalmazza az ügyfelek (Microsoft) értesítésének lépéseit, amint az ebben a szakaszban szerepel. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
32.	Kárelhárítási tervet kell bevezetnie és felügyelnie kell az egyes adatvédelmi incidensek megszüntetését, hogy kellő időben meghozhassa a megfelelő intézkedéseket a probléma megoldására.	A beszállító dokumentált eljárásokkal rendelkezik, amelyekkel az adatvédelmi incidensekre reagál, és azokat megoldja. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.
33.	Amennyiben a Microsoft a személyes Microsoft-adatok Adatkezelője, hivatalos panaszkezelési eljárást kell bevezetnie a személyes Microsoft-adatokkal kapcsolatos valamennyi adatvédelmi reklamáció kezelésére.	A beszállító eszközökkel rendelkezik a személyes Microsoft-adatokkal kapcsolatos panaszok fogadására, és dokumentált panaszkezelési eljárása van a panaszok kivizsgálására. A Microsoft kérésére a beszállító rendelkezésre bocsátja az igazoló dokumentációt.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	J. szakasz: Biztonság	
	A beszállítónak olyan adatbiztonsági programot kell kidolgoznia, bevezetnie és fenntartania, amely olyan szabályokat és folyamatokat foglal magában, amelyek megvédik és fenntartják a személyes és bizalmas Microsoft-adatok biztonságát az iparági jó gyakorlatoknak és az alkalmazandó jogszabályoknak megfelelően. A beszállító biztonsági programjának meg kell felelnie az alább rögzített szabályok 34-50. követelményeinek.	Az érvényes ISO 27001 szabvány megfelelően helyettesíti a J. szakasz követelményeit. Ezen helyettesítés alkalmazásához vegye fel a kapcsolatot az SSPA-val. Megjegyzés: A tanúsítványt be kell mutatni.
34.	Végezzen évenkénti hálózatbiztonsági felmérést, amely magában foglalja a következőket: ▪ a környezetben bekövetkező nagyobb változások felülvizsgálatát, például új rendszerkomponens, hálózati topológia, tűzfalszabályok stb. ▪ a biztonsági résekkel kapcsolatos vizsgálatok végrehajtását; és ▪ módosítási naplók vezetését.	A beszállító dokumentálja a hálózati felméréseket, a módosítási naplókat és a vizsgálati eredményeket. A kötelező módosítási naplóknak nyomon kell követniük a változásokat, információval kell szolgálniuk a változás okáról, és tartalmazniuk kell a kijelölt jóváhagyó nevét és beosztását.
35.	A beszállító kötelessége meghatározni, közölni és bevezetni a mobileszközökre vonatkozó, mobileszközzel elért vagy azokon használt személyes vagy bizalmas Microsoft-adatok védelméről és használatának korlátozásáról szóló szabályzatot.	Ha a személyes vagy bizalmas Microsoft-adatok feldolgozása mobileszköz használatát követeli meg, a beszállítónak be kell mutatnia a megfelelő mobileszköz-szabályzat használatát.
36.	A teljesítés támogatására használt valamennyi eszközzel el kell számolni, és ezeknek azonosítható tulajdonossal kell rendelkezniük. A beszállító felelős ezen információeszközök készletnyilvántartásáért, ezen eszközök elfogadható és jogos használatának meghatározásáért, és megfelelő szintű védelmet kell nyújtania az eszközök számára a teljes életciklusuk során.	A teljesítés támogatására használt eszközkészletek nyilvántartása. Az eszköznyilvántartásnak tartalmaznia kell a következőket: ▪ az eszköz helye, ▪ az eszközön található adatok adatbesorolása, ▪ a munkaviszony vagy az üzleti megállapodás lejáratakor az eszköz visszajuttatásáról szóló feljegyzés, és ▪ az adathordozó megsemmisítéséről szóló feljegyzés, amikor arra már nincs szükség.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	J. szakasz: Biztonság (folyt.)	
37.	A hozzáférési jogok kezelésére vonatkozó eljárások kidolgozása és fenntartása annak érdekében, hogy megakadályozza az illetéktelen hozzáférést a beszállító felügyelete alatt álló bármely személyes vagy bizalmas Microsoft-adatokhoz.	A beszállítónak be kell mutatnia, hogy hozzáférési jogosultságkezelési tervet vezetett be, amely magában foglalja a következőket: ▪ hozzáférés-ellenőrzési eljárások, ▪ azonosítási eljárások, ▪ kizárási eljárások a sikertelen próbálkozásokat követően, ▪ megbízható paraméterek a hitelesítő adatok kiválasztására vonatkozóan, valamint ▪ a felhasználói fiók inaktiválása a foglalkoztatás megszűnésétől számított 48 órán belüli ▪ szigorú jelszó-ellenőrzési szabályok, amelyek hosszú és bonyolult jelszavak használatát írják elő, és megelőzik a korábban használt jelszavak újbóli használatát. A beszállítónak be kell mutatnia, hogy rendelkezik olyan bevezetett folyamattal, amellyel felügyelhető a felhasználók hozzáférése a személyes és bizalmas Microsoft-adatokhoz, érvényesítve a legkisebb jogosultságra vonatkozó alapelvet. A folyamat tartalmaz: ▪ egyértelműen meghatározott felhasználói szerepköröket, ▪ eljárásokat, amelyekkel felülvizsgálható és igazolható a szerepkörökhöz való hozzáférés engedélyezése, valamint ▪ teszteket arra vonatkozóan, hogy a szerepkörökön belüli felhasználók, akik hozzáférnek a Microsoft-adatokhoz, dokumentált igazolással rendelkeznek arra vonatkozóan, hogy ők a csoport/szerepkör tagjai.
38.	Olyan javításkezelési eljárásokat kell meghatározni és bevezetni, amelyek a személyes és bizalmas Microsoft-adatok feldolgozására használt rendszerek biztonsági javításait helyezik előtérbe. Ilyen eljárások többek között az alábbiak: ▪ kockázaton alapuló megközelítés alkalmazása a biztonsági javítások elsődlegességének biztosítására, ▪ a vészhelyzeti hibajavítások kezelésére és végrehajtására való képesség, ▪ operációs rendszerre és kiszolgálótermékre, például alkalmazáskiszolgálóra és adatbázisszoftverre való alkalmazhatóság, ▪ a hibajavítás által mérsékelt kockázatok dokumentálása és a kivételek nyomon követése, és ▪ a szerző vállalat által már nem támogatott szoftverek visszavonási követelményei.	A beszállító be tud mutatni egy bevezetett javításkezelési eljárást, amely megfelel ennek a követelménynek, és minimálisan lefedi a következőket: ▪ Súlyosság megállapítása a prioritásról szóló tájékoztatáshoz. (A súlyosság meghatározásai dokumentálva vannak.) ▪ Dokumentált eljárás a vészhelyzeti javítások megvalósításához. ▪ Annak ellenőrzése, hogy nincsenek használatban olyan operációs rendszerek, amelyeket már nem támogat a szerző vállalat. ▪ Javításkezelési feljegyzések a jóváhagyások és a kivételek nyomon követésével.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	J. szakasz: Biztonság (folyt.)	
39.	Víruskereső és kártevőirtó szoftverek telepítése a hálózathoz csatlakozó minden olyan berendezésre, amelyet személyes és bizalmas Microsoft-adatok feldolgozására használnak, beleérve a kiszolgálókat, valamint a munkához és oktatáshoz használt asztali gépeket, a lehetséges káros vírusok és kártevő szoftverek elleni védelem érdekében. A kártevőirtó-definíciós fájlok napi, vagy a víruskereső/kártevőirtó beszállító által meghatározott intervallumonkénti frissítése. Megjegyzés: Ez az összes operációs rendszerre vonatkozik, beleértve a Linuxot is.	Van nyilvántartás arról, hogy a víruskereső és kártevőirtó szoftvert aktívan használják. Megjegyzés: Ez a követelmény minden operációs rendszerre vonatkozik.
40.	A Microsoft számára szoftvert fejlesztő beszállítóknak a beépített biztonság alapelveit kell alkalmazniuk a szoftverek felépítésének eljárásaiban.	A beszállító műszaki specifikációs dokumentációja ellenőrzési pontokat tartalmaz a biztonság ellenőrzésére a fejlesztési ciklusokban.
41.	A behatolás, a veszteség és más jogosulatlan tevékenységek megelőzésére adatvesztés-megelőzési programot (Data Loss Prevention, „**DLP**”) kell alkalmazni. Az adatokat megfelelően kell besorolni, címkézni és védeni, a beszállító pedig köteles felügyelni a személyes és bizalmas Microsoft-adatok feldolgozására használt információs rendszert, hogy nem történt-e behatolás, adatvesztés vagy más jogosulatlan tevékenység. A DLP-program minimális feltételként megköveteli az alábbiakat: ▪ az iparági szabványnak megfelelő üzemeltetési, hálózati és felhőalapú behatolás-érzékelő rendszerek („**IDS**") használata, ha a beszállító személyes vagy bizalmas Microsoft-adatokat tárol, ▪ fejlett behatolásvédelmi rendszerek („**IPS**") bevezetése, amelyek az adatvesztés felügyeletére és aktív megakadályozására vannak konfigurálva, ▪ a rendszerben történt biztonsági incidens esetén a rendszer elemzése annak biztosítására, hogy minden fennmaradó biztonsági rés kezelése is megtörtént, ▪ a rendszerbiztonság megsértését felügyelő érzékelő eszközök kötelező eljárásainak dokumentálása, ▪ az adatvédelmi incidensek észlelésekor kötelezően végrehajtandó, az incidensre választ adó és azt kezelő folyamat kidolgozása, valamint ▪ a személyes vagy bizalmas Microsoft-adatok jogosulatlan letöltésére vagy használatára vonatkozó	A behatolás, adatvesztés vagy más jogosulatlan tevékenység (és legalább a jelen szakaszban meghatározott összes tétel) megelőzését szolgáló eljárásokkal bevezetett, dokumentált DLP-program.

	tájékoztatás (a beszállítónak a beszállító teljesítéséből kizárt összes munkavállalója és alvállalkozója számára).	
#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	J. szakasz: Biztonság (folyt.)	
42.	Azonnal tájékoztatni kell a felső vezetést és a Microsoftot az incidensre adott válasszal kapcsolatos kivizsgálási eredményekről.	Rendszerek és eljárások vannak érvényben az incidensre adott válasz vizsgálati eredményeinek Microsofttal történő közlésére.
43.	A rendszergazdáknak, a műveleti személyzetnek, a vezetőségnek és a harmadik feleknek évente biztonsági oktatáson kell részt venniük.	Olyan bevezetett biztonsági képzési program, amely tartalmazza a következőket: ▪ éves oktatás az incidensekre adott válaszokról, valamint ▪ szimulált események és automatikus mechanizmusok a krízishelyzetekre adott hatékony válaszok megkönnyítésére. ▪ Incidensmegelőzési tudatosság, úgymint a kártevő szoftverek letöltéséhez kapcsolódó kockázatok.
44.	A beszállítónak gondoskodnia kell arról, hogy a biztonsági mentés tervezési folyamatai megvédjék a személyes és bizalmas Microsoft-adatokat a jogosulatlan használattól, hozzáféréstől, közzétételtől, módosítástól és megsemmisítéstől.	A beszállító be tud mutatni olyan dokumentált válaszadási és helyreállítási eljárásokat, amelyek részletezik, hogy a szervezet hogyan fogja kezelni a működési zavarokat, és olyan előre meghatározott szinten tartja az információbiztonságot, amely megfelel a vezetőség által jóváhagyott információbiztonsági folytonossági céloknak. A beszállító be tudja mutatni, hogy eljárásokat határozott meg és vezetett be a kritikus adatokról történő rendszeres biztonsági másolatok készítésére, valamint azok biztonságos tárolására és hatékony helyreállítására vonatkozóan.
45.	Üzletmenet-folytonossági és vészhelyzeti helyreállítási terveket kell kidolgozni és tesztelni.	A vészhelyzeti helyreállítási tervnek a következőket kell tartalmaznia: ▪ Meghatározott feltételek annak megállapítására, hogy egy adott rendszer létfontosságú-e a beszállító üzleti műveleteire vonatkozóan. ▪ A létfontosságú rendszerek listázása olyan meghatározott feltételek alapján, amelyeket figyelembe kell venni vészhelyzet esetén történő helyreállításkor. ▪ Meghatározott vészhelyzeti helyreállítási eljárás minden egyes létfontosságú rendszerre vonatkozóan, amely 72 órán belül lehetővé teszi a rendszer helyreállítását egy olyan mérnök számára, aki nem ismeri a rendszert.

		▪ A vészhelyreállítási tervek éves (vagy gyakoribb) tesztelése és felülvizsgálata annak biztosítására, hogy a helyreállítási célok teljesüljenek.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	J. szakasz: Biztonság (folyt.)	
46.	Ellenőrizni kell a magánszemély személyazonosságát, mielőtt megkapná a személyes vagy bizalmas Microsoft-adatokhoz való hozzáférést, és biztosítani kell, hogy a hozzáférés az adott egyénnek a teljesítés támogatására megengedett tevékenységi körére korlátozódjon.	Annak biztosítása, hogy minden felhasználói azonosító egyedi, illetve hogy mindegyikhez tartozik az iparági szabványnak megfelelő hitelesítési módszer, például Azure Active Directory. A magasabb szintű hozzáféréshez (rendszergazdai vagy más típusú kibővített jogosultságok) kötelező egy második tényező, például intelligens kártya vagy telefonalapú hitelesítés használata. Dokumentált adatbiztonsági program olyan eljárással, amely biztosítja, hogy a beszállító összes munkavállalójának és alvállalkozójának a személyes vagy bizalmas Microsoft-adatokhoz való hozzáférése a teljesítés támogatásához szükségesnél ne legyen hosszabb vagy szélesebb körű.
47.	A hálózatok közötti továbbítás során a beszállítónak a jelen teljesítéssel kapcsolatosan feldolgozott minden adatot Transport Layer Security („**TLS**”) vagy Internet Protocol Security („**IPsec**”) használatával történő titkosítással kell védenie. Ezek a metódusok a NIST 800-52 és a NIST 800-57 szabványokban vannak leírva, valamint ezekkel egyenértékű iparági szabvány is alkalmazható. A beszállítónak vissza kell utasítania a személyes vagy bizalmas Microsoft-adatok nem titkosított úton történő továbbítását.	A TLS vagy más tanúsítványok létrehozásának, bevezetésének vagy lecserélésének folyamata kötelezően meghatározandó és alkalmazandó.
48.	Minden olyan beszállítói eszközön (hordozható számítógép, munkaállomás stb.), amely személyes vagy bizalmas Microsoft-adatokat ér el vagy kezel, lemezalapú titkosítást kell alkalmazni.	Minden, személyes vagy bizalmas Microsoft-adatok kezelésére használt eszköz titkosítva van, hogy megfeleljen a BitLocker vagy más egyenértékű lemeztitkosítási iparági megoldásoknak.

#	Microsoft-beszállítókra vonatkozó adatvédelmi követelmények	A megfelelés igazolása
	J. szakasz: Biztonság (folyt.)	
49.	Bármely és minden személyes, illetve bizalmas Microsoft-adat nyugalmi állapotban (tárolás közben) végzett titkosításhoz (a jelenlegi ipari szabványokat, például a **NIST 800-111** szabványt használó) rendszereket és eljárásokat kell alkalmazni. Ezek az adatok többek között az alábbiak lehetnek: ▪ azonosító adatok (pl. felhasználónév/jelszó) ▪ fizetési eszköz adatai (pl. hitelkártya- vagy bankszámlaszám) ▪ bevándorlással kapcsolatos személyes adatok ▪ egészségügyi profil adatai (pl. egészségügyi nyilvántartási szám, biometrikus jelölők vagy azonosítók, úgymint hitelesítési célra használt DNS, ujjlenyomatok, retinák és íriszek, hangminták, arcminták és kézméretek) ▪ közigazgatási azonosító adatok (pl. társadalombiztosítási azonosító vagy jogosítvány száma) ▪ a Microsoft-ügyfelekhez tartozó adatok (pl. SharePoint-, O365-dokumentumok, OneDrive-ügyfelek) ▪ be nem jelentett Microsoft-termékekkel kapcsolatos anyagok ▪ születési dátum ▪ gyermek profiladatai ▪ valós idejű földrajzi adatok ▪ személyes (nem vállalati) fizikai cím ▪ személyes (nem vállalati) telefonszámok ▪ vallás ▪ politikai vélemény ▪ szexuális irányultság/beállítottság ▪ biztonsági kérdésekre adott válaszok (pl. kétlépcsős hitelesítés, jelszó -visszaállítás) ▪ anya leánykori neve	Ellenőrizze, hogy a személyes és bizalmas Microsoft-adatok titkosítása nyugalmi állapotban történik-e.
50.	A fejlesztői vagy tesztkörnyezetben használt összes személyes Microsoft-adatot anonimizálni kell.	A személyes Microsoft-adatok nem használhatók fejlesztési vagy tesztkörnyezetekben. Ha nincs más lehetőség, megfelelően anonimizálni kell őket az Érintettek azonosításának vagy a személyes adatokkal való visszaélések megakadályozására. Megjegyzés: Az anonimizált adatok nem azonosak az álnevesített adatokkal. Az anonimizált adatok olyan adatok, amelyek nem kapcsolhatók azonosított vagy azonosítható természetes személyhez, és a személyes adatok Érintettje nem vagy már nem azonosítható.

Szószedet

Az „**EUDPR”** az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről.

Az „**európai uniós mintazáradékok**” és az „**általános szerződési feltételek**” jelentése: (i) az Európai Bizottság 2021. június 4-i (EU) 2021/914 határozata által jóváhagyott és a GDPR 46. cikkében leírt standard adatvédelmi záradékok a személyes adatoknak olyan harmadik országbeli adatfeldolgozóknak történő továbbításáról, akik nem biztosítják az adatok megfelelő szintű védelmét, (ii) minden utód általános szerződési feltételt, amelyet (a) az Európai Bizottság elfogadott, (b) az európai adatvédelmi biztos elfogadott és az Európai Bizottság jóváhagyott, (c) az Egyesült Királyság az Egyesült Királyság általános szövetségi adatvédelmi törvénye értelmében elfogadott, (d) Svájc a svájci szövetségi adatvédelmi törvény értelmében elfogadott, vagy (e) a Svájc, az Egyesült Királyság és az Európai Unió/Európai Gazdasági Térség joghatóságain kívüli más joghatóság elfogadott, ahol a záradékok szabályozzák a személyes adatok nemzetközi továbbítását, be kell építeni, és a beszállítóra nézve az elfogadásuk napjától kezdve kötelező érvényűnek kell tekinteni.

A „**GDPR**" az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).

A „**meghatalmazott képviselő**” az a személy, aki megfelelő szintű jogkörrel rendelkezik a vállalat nevében történő aláírásra. Ennek a személynek rendelkeznie kell a szükséges adatvédelmi és biztonsági ismeretekkel, vagy az SSPA Program intézkedésére adott válaszadás előtt konzultálnia kell a témában jártas szakemberekkel. Ezen felül az SSPA adatlapon neve feltüntetésével igazolja, hogy elolvasta és megértette az adatvédelmi követelményeket.

A „**szabadúszó**” olyan igény szerinti feladatokat ellátó vagy szolgáltatásokat nyújtó személy, akinek alkalmazására digitális platformokon vagy más módon kerül sor.

A „**személyes adatok védelmére vonatkozó követelmények**" a GDPR, az EUDPR, az EU-/EGT-tagállamok helyi adatvédelmi jogszabályai, Kalifornia államnak a fogyasztók személyes adatainak védelméről szóló törvénye (Kalifornia állam polgári törvénykönyve 1798. szakaszának 100. és azt követő cikkei (a továbbiakban: „CCPA")), az Egyesült Királyság 2018. évi adatvédelmi törvénye, valamint minden, az Egyesült Királyságban hatályos, a fentihez kapcsolódó vagy azt követően hozott jogszabály, előírás és minden egyéb, a következőkkel kapcsolatos egyéb jogszabályi követelmény: (a) adatvédelem és adatbiztonság; vagy (b) a személyes adatok felhasználása, gyűjtése, megőrzése, tárolása, biztonsága, közlése, továbbítása, rendelkezésre bocsátása és egyéb más módon történő kezelése.

A „**weboldaltárhely-szolgáltatások**” olyan online szolgáltatások, amelyek a Microsoft nevében, a Microsoft-domainen belül weboldalakat hoznak létre, illetve tartanak fenn, pl. a beszállító biztosítja az összes számukra szükséges eszközt és szolgáltatást az oldal létrehozására és fenntartására, és elérhetővé teszi azt az interneten. A „weboldaltárhely szolgáltató” vagy „web host” az a beszállító, aki biztosítja a weboldal Interneten történő megtekintéséhez szükséges eszközöket és szolgáltatásokat, mint például a sütiket vagy a reklámokhoz szükséges webes adatgyűjtő jeleket (web beacon).