Microsoft-szállítókra vonatkozó adatvédelmi követelmények

Alkalmazhatóság

A Microsoft-szállítókra vonatkozó adatvédelmi követelmények („**DPR**”) érvényesek a személyes vagy bizalmas Microsoft-adatot feldolgozó Microsoft-szállítók mindegyikére az adott szállító teljesítésével (pl. szolgáltatások nyújtása, szoftverlicencek, felhőszolgáltatások) kapcsolatban a Microsofttal kötött szerződése feltételeinek megfelelően (pl. beszerzési rendelésekben szereplő feltételek, keretszerződés) („**Teljesít**”, „**Teljesítés folyamatban**” vagy „**Teljesítés**”).

- Amennyiben a jelen dokumentumban rögzített követelmények, valamint a szállító és a Microsoft között létrejött szerződéses megállapodásokban meghatározottak között ellentmondás lenne, akkor a DPR érvényes, kivéve, ha a vonatkozó szállító azonosítja a DPR-tanúsítási űrlapon a szerződésnek azt a pontos kitételét, amely ellentmond a DPR vonatkozó szakaszának (ebben az esetben a szerződéses feltételek érvényesek).
- Amennyiben a jelen dokumentumban rögzített követelmények és bármilyen jogi vagy törvény által szabályozott követelmények között ellentmondás lenne, a jogi és törvényi követelmények elsőbbséget élveznek.
- Amennyiben a Microsoft szállítója ezen DPR tekintetében Adatkezelőként működik, akkor ennek a szállítónak a feldolgozási tevékenységére csak a J Biztonság és az A Kezelés szakasz követelményei vonatkoznak.
- Amennyiben a jelen DPR tekintetében a Microsoft szállítója nem dolgoz fel személyes Microsoft-adatokat, csak bizalmas Microsoft-adatokat, akkor ennek a szállítónak a feldolgozási tevékenységére csak az A Kezelés, az E Megőrzés és a J Biztonság szakaszok vonatkoznak.

Az adatok nemzetközi átvitele

A szállítónak – más kötelezettségei korlátozása nélkül, és abban az esetben, ha a Microsoft előzetes írásos jóváhagyást adott a személyes Microsoft-adatok nemzetközi átadásához – minden esetben meg kell felelnie a bármely adatvédelmi hatóság, az Európai Adatvédelmi Testület vagy az Európai Bizottság által jóváhagyott és a Microsoft által alkalmazott vagy elfogadott bármely szabványos szerződéses feltételeiből, kötelmi erővel bíró vállalati szabályozásából vagy más szabályrendszeréből következő adatvédelmi követelményeinek, beleértve a következő EU–USA és Svájc–USA megállapodásokat: Az adatvédelmi pajzs keretrendszere és az EU Általános Adatvédelmi Rendelete. A beszállító belegyezik abba, hogy értesíti a Microsoftot abban az esetben, ha a beszállító olyan döntést hoz, amelynek eredményeként a továbbiakban nem lesz képes teljesíteni azon kötelezettségét, hogy az adatvédelmi pajzs alapelvei által megkövetelt szintű védelmet biztosítsa. A beszállítónak azt is biztosítania kell, hogy a fentieknek bármely és minden további feldolgozó megfeleljen (az Európai Bizottság C(2010) 593. számú határozatához függelékként közzétett általános szerződési feltételek (2010) 1 (d) szakaszában meghatározottak szerint).

Kulcsfontosságú meghatározások

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 más ehhez hasonlók, úgy értelmezendők, hogy azok tartalmazzák a „korlátozás nélkül” vagy „a következőre való korlátozás nélkül” kifejezést, kivéve, ha azokat a „csak” vagy a „kizárólag” szavakkal vagy ehhez hasonlókkal jelöljük.

„**Adatkezelő**” az a természetes vagy jogi személy, közjogi hatóság, ügynökség vagy más testület, amely egyedül vagy másokkal közösen meghatározza a Személyes adatok feldolgozásának célját és módját; ahol az Adatfeldolgozás lehetséges célját és módját az Európai Unió („**EU**”) vagy a tagállamok jogszabályai állapítják meg, az adatkezelőt (vagy az adatkezelő kijelölésének feltételeit) pedig ezek a jogszabályok határozzák meg.

Az „**Adatfeldolgozó**” olyan természetes vagy jogi személy, közjogi hatóság, ügynökség vagy más testület, amely a Személyes adatokat az Adatkezelő nevében feldolgozza.

„**Adatszivárgás**” az adatbiztonság olyan megsértése, amely akaratlan vagy jogszerűtlen módon okoz kárt, veszteséget, változást vagy jogosulatlan közzétételt, illetve biztosít hozzáférést az átvitt, tárolt vagy más módon feldolgozott személyes adatokhoz vagy bizalmas Microsoft-adatokhoz.

Az „**Adattulajdonos joga**” az Adattulajdonosnak a rá vonatkozó személyes Microsoft-adatok elérésére, törlésére, szerkesztésére, exportálására, korlátozására vagy a feldolgozásával kapcsolatos ellenvetésének kifejezésére való joga, amennyiben az jogszabályi kötelezettség.

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, kiadás előtti marketinganyagok, terméklicenckulcsok, valamint Microsoft-termékekkel és -szolgáltatásokkal kapcsolatos technikai dokumentációk.

A „**Feldolgozás**” jelentése minden művelet vagy műveletsor, amelyet a személyes Microsoft-adatokon vagy bizalmas adatokon hajtanak végre, akár automatizált módon, úgymint azok gyűjtése, felvétele, rendezése, strukturálása, tárolása, adaptációja vagy megváltoztatása, lekérése, egyeztetése, használata, nyilvánosságra hozatala adatátvitellel, terjesztése vagy más módon történő elérhetővé tétele, igazítása vagy kombinációja, korlátozása, törlése vagy megsemmisítése. A „Feldolgozás” és a „Feldolgozott” jelentése egymásnak megfeleltethető.

„**Jogszabály**” bármely joghatóság (szövetségi, állami, helyi vagy nemzetközi) minden vonatkozó jogszabálya, előírása, rendelete, határozata, döntése, rendelkezése, rendszabálya, törvénye, törvényhozó határozata, állásfoglalása és követelménye. A „**Törvénytelen**” kifejezés jelentése a jogszabályok bármilyen megsértését foglalja magában.

A „**Személyes adatok**” közé tartozik minden olyan adat, amely egy azonosított vagy azonosítható természetes személlyel van kapcsolatban („**Adattulajdonos**”); azonosítható természetes személy az, akinek a személye közvetlen vagy közvetett módon azonosítható egy olyan azonosító segítségével, mint a név, azonosítószám, tartózkodási hely adatai, online azonosító vagy egy vagy több olyan tényező, amely az adott természetes személy fizikai, fiziológia, genetikai, mentális, gazdasági, kulturális vagy közösségi jellemzőire vonatkozik.

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

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	A szakasz: Menedzsment		
1.	A Microsoft és a szállító közötti összes vonatkozó megállapodás (pl. keretszerződés, munkaterv, beszerzési rendelések és más megrendelések) – az alkalmazhatóságnak megfelelően – tartalmazza az adatvédelmi és -biztonsági elvek leírását a bizalmas és személyes Microsoft-adatokra vonatkozóan. Az Adatfeldolgozókként működő vállalatok esetében a szerződésnek tartalmaznia kell a Feldolgozás tárgyát és időtartamát, a Feldolgozás jellegét és célját, a személyes Microsoft-adatok típusát és az Adattulajdonosok kategóriáit, valamint a Microsoft kötelezettségeit és jogait.	A szállítónak be kell mutatnia a Microsoft és a szállító között létrejött, vonatkozó szerződést. Az Adatfeldolgozók számára az adatfeldolgozás leírását a vonatkozó szerződés (*pl.* munkaterv, beszerzési rendelés) tartalmazza. Megjegyzés: A munka közben kiadott beszerzési rendelésekkel rendelkező vállalatoknál a Adatfeldolgozási tevékenységek szükséges leírása később is bekerülhet a beszerzési folyamatba.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
2.	Az adatvédelmi követelményekkel (DPR) kapcsolatos felelősséget és számonkérhetőséget egy kijelölt személyre vagy csoportra kell bíznia a társaságon belül.	A Microsoft szállítói DPR-nek való megfelelésért felelős személy vagy csoport neve. Az adatvédelmi és -biztonsági szerepkört felmutató személy vagy csoport jogosultságát és számonkérhetőségét leíró dokumentum.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
3.	Éves adatvédelmi és -biztonsági oktatást kell létrehoznia, fenntartania és megvalósítania azon alkalmazottak számára, akiknek hozzáférése lesz személyes vagy bizalmas Microsoft-adatokhoz. Ha az Ön vállalata nem rendelkezik ehhez előkészített tartalommal, használhatja ezt a forgatókönyvvázlatot, amelyet vállalatára adaptálhat.	Az éves részvételi nyilvántartások rendelkezésre állnak. Az oktatott tartalom magában foglalja az adatvédelmi és -biztonsági alapelveket.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
4.	A személyes Microsoft-adatokat csak a Microsoft dokumentált útmutatásának megfelelően dolgozhatja fel, ideértve a személyes Microsoft-adatok külső országba vagy nemzetközi szervezethez történő továbbítását, kivéve, ha arra jogszabály kötelezi, amely esetben az Adatfeldolgozónak (szállítónak) értesítenie kell az Adatkezelőt (a Microsoftot) a feldolgozás előtt az adott jogi előírásról, kivéve, ha a jogszabály közérdekbe ütközőnek minősíti az adott információt.	Az utasítások dokumentált bizonyítéka a szerződésben (pl. munkatervben vagy a beszerzési rendelésben) foglaltaknak megfelelően, vagy a Teljesítés nyújtására használt elektronikus rendszer részeként rögzítve.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	B szakasz: Megjegyzés		
5.	A szállító köteles használni a Microsoft adatvédelmi nyilatkozatát, amikor személyes adatokat gyűjt a Microsoft nevében. Az adatvédelmi értesítőnek érthetőnek kell lennie, és rendelkezésre kell állnia az Adattulajdonosok számára, hogy eldönthessék, átadják-e személyes adataikat a szállítónak. Megjegyzés: Ha az Ön vállalata az Adatfeldolgozási tevékenység Adatkezelője, akkor közzé kell tennie a saját adatvédelmi értesítőjét. *A megfelelő Microsoft-értesítők eléréséhez írjon az SSPAHelp@microsoft.com címre.*	A szállító egy fwdlink hivatkozással érheti el az aktuális, Microsoft által közzétett adatvédelmi nyilatkozatot. Az Adatvédelmi nyilatkozat közzé lesz téve minden olyan összefüggésben, amikor gyűjteni fogjuk a felhasználó Személyes adatait. Ha alkalmazandó, az adatgyűjtés előtt elérhetővé tesszük és biztosítjuk az offline verziót. A felhasznált offline Adatvédelmi nyilatkozat a legújabb, közzétett verziójú dokumentum a megfelelő dátummal. A Microsoft munkatársainak nyújtott szolgáltatásokhoz a Microsoft adatvédelmi értesítője használatos.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
6.	Ha a személyes Microsoft-adatok gyűjtése élő vagy rögzített hanghívás útján történik, a szállítóknak fel kell készülniük arra, hogy az Adattulajdonossal megvitassák a vonatkozó adatgyűjtési, -kezelési, -felhasználási és -megőrzési gyakorlatokat.	A hangfelvételek átirata tartalmazza a személyes Microsoft-adatok feldolgozásának módját, többek között ezeket: ▪ adatgyűjtés ▪ felhasználás és ▪ megőrzés.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	C szakasz: Választás és beleegyezés		
7.	Ha a szállító jogalapja az Adatfeldolgozáshoz a beleegyezés, a szállítónak be kell szereznie és dokumentálnia kell az Adattulajdonos beleegyezését az összes Adatfeldolgozási tevékenységhez (beleértve bármely új és frissített Adatfeldolgozási tevékenységet) még azelőtt, hogy elkezdené az adott Adattulajdonos személyes adatainak gyűjtését.	A szállító képes bemutatni, hogyan adja beleegyezését az Adattulajdonos az Adatfeldolgozási tevékenységhez, és hogy a beleegyezés a szállító teljes feldolgozási tevékenységét lefedi az Adattulajdonos személyes adatai vonatkozásában. A szállító képes bemutatni, hogyan vonja vissza az Adattulajdonos a feldolgozási tevékenységhez adott beleegyezését. A szállító képes bemutatni, hogyan történik a választások ellenőrzése az új Adatfeldolgozási tevékenység indítása előtt. A szállító megfigyeli a választások kezelésének hatékonyságát, hogy a választás módosításából eredő kötelezettség betartására rendelkezésre álló időtartam a vonatkozó legkorlátozóbb helyi jogi követelmény legyen. Megjegyzés: A bizonyítékok lehetnek felhasználói interakciókat bemutató képernyőképek, a szolgáltatásban végzett kísérletezés vagy a műszaki dokumentáció megtekintésének lehetősége.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	C szakasz: Választás és beleegyezés (folyt.)		
8.	A cookie-k weboldalak és/vagy alkalmazások által az eszközökön tárolt kis méretű szövegfájlok, amelyek egy Adattulajdonos vagy egy eszköz felismerésére használt adatokat tartalmaznak. Azoknak a szállítóknak, amelyek Microsoft-weboldalakat és/vagy -alkalmazásokat hoznak létre és kezelnek, látható értesítést és választási lehetőséget kell biztosítaniuk a cookie-k használatával kapcsolatban az Adattulajdonosok számára. Azoknak a szállítóknak, amelyek Microsoft-weboldalakat és/vagy -alkalmazásokat hoznak létre és kezelnek, olyan cookie-kat kell használniuk, amely igazodik a Microsoft adatvédelmi nyilatkozatában vállalt kötelezettségekhez és a helyi törvényi előírásokhoz, például az Európai Unió által létrehozott szabályokhoz.	Minden egyes cookie célját dokumentálni kell, és tájékoztatást kell nyújtani az alkalmazott cookie fajtájáról. ▪ Állandó cookie-kat nem szabad használni, ha a munkamenet-cookie-k is megfelelőek. ▪ Állandó cookie-k használata esetén ezek lejárati dátuma nem lehet két évnél hosszabb a felhasználó webhelyen tett látogatásától számítva. Az Európai Unión belüli felhasználók esetén az állandó cookie lejárati napjáig eltelő idő nem lehet 13 hónapnál hosszabb. Igazolja az EU vonatkozó jogszabályainak való megfelelőséget, például ▪ az egyezményes címkézési jelölések használatát, „Adatvédelem és cookie-k” az adatvédelmi nyilatkozat esetében, és ▪ biztosítsa a megerősítő felhasználói beleegyezést a cookie-k használata előtt olyan „nem létfontosságú” célokra, mint a hirdetések.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	D szakasz: Adatgyűjtés		
9.	A szállítónak figyelemmel kell kísérnie a személyes és bizalmas Microsoft-adatok és/vagy -információk gyűjtését annak biztosítása érdekében, hogy csak a Teljesítéshez szükséges adatokat gyűjtsék össze.	A szállító biztosítani tudja azt a dokumentációt, amely bemutatja, hogy a gyűjtött személyes és/vagy bizalmas Microsoft-adatokra szükség van a Teljesítéshez.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
10.	Ha a szállító a Microsoft nevében külső felektől gyűjt be személyes adatokat, a szállítónak ellenőriznie kell, hogy a külső fél adatvédelmi szabályzatai és gyakorlatai megfelelnek-e a szállító és a Microsoft között érvényes szerződésnek, illetve az adatvédelmi követelményeknek (DPR).	A szállító biztosítani tudja azt a dokumentációt, amely bemutatja, hogy gondosan jár el a harmadik fél adatvédelmi szabályzatait és gyakorlatait illetően.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
11.	Mielőtt a szállító az Adattulajdonos eszközén végrehajtható szoftvert telepítve vagy felhasználva gyűjtene személyes Microsoft-adatokat, ezen adatok gyűjtésének szükségességét dokumentálnia kell a Microsofttal kötött érvényes szállítói szerződésben.	A Microsoftnak az Adattulajdonos eszközén használt végrehajtható szoftverre vonatkozó hozzájárulása megjegyzésként bekerül az érvényes szerződésbe.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
12.	Érzékeny jellegű személyes Microsoft-adatok gyűjtése előtt (olyan adat, amely a faji vagy etnikai származásra, politikai véleményre, vallási vagy filozófiai hitre, szakszervezeti tagságra, genetikai adatokra, biometrikus adatokra, az adott természetes személy egészségére, szexuális életére vagy szexuális orientációjára vonatkozik) a személyes Microsoft-adatok gyűjtésének szükségességét a Microsofttal kötött, aláírt szállítói szerződéssel kell dokumentálni.	Az érzékeny jellegű személyes Microsoft-adatok gyűjtésének szükségességét megemlítik a Microsofttal kötött érvényes szerződésben.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	E szakasz: Megőrzés		
13.	Biztosítsa, hogy a személyes és bizalmas Microsoft-adatokat csak addig őrizzék meg, amíg ez szükséges a Teljesítéshez, kivéve, ha jogszabály írja elő a személyes és/vagy bizalmas Microsoft-adatok további megőrzését.	A szállító eleget tesz a Microsoft által a szerződésben (pl. a munkatervben vagy a beszerzési rendelésben) rögzített, dokumentált megőrzési irányelveknek vagy megőrzési követelményeknek.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
14.	Biztosítsa, hogy a szállító a tulajdonában vagy a felügyelete alatt lévő személyes vagy bizalmas Microsoft-adatokat a Microsoft saját belátása szerint a Teljesítés befejezése esetén vagy a Microsoft kérésére visszaküldje a Microsoftnak, vagy megsemmisítsék azokat. Az alkalmazásokban olyan folyamatokat kell elhelyezni, amelyek biztosítják, hogy az adatok az alkalmazásból a felhasználók általi közvetlen módon vagy az egyéb okok, például az adat kora miatt történő eltávolításakor azok biztonságos törlésre kerülnek. Ha a személyes vagy bizalmas Microsoft-adatok megsemmisítése szükséges, a szállítónak a személyes és/vagy bizalmas Microsoft-adatokat tartalmazó fizikai eszközöket el kell égetnie, porrá zúznia vagy összetörnie, hogy az adatok ne legyenek olvashatók vagy helyreállíthatók.	A szállító megőrzi a személyes és bizalmas Microsoft-adatokkal való rendelkezés bizonylatait (esetleg beleértve a visszaküldést a Microsoftnak megsemmisítésre). Ha a Microsoft az adatok megsemmisítését követeli meg vagy kéri, a szállító köteles bemutatni a szállító egyik tisztviselője által aláírt tanúsítványt az adatok megsemmisítéséről.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	F szakasz: Adattulajdonosok		
	Az Adattulajdonosoknak joga van a személyes adataikhoz való hozzáférésre, azok törlésére, szerkesztésére, exportálására, korlátozására és az azok feldolgozására vonatkozó tiltakozásra („**Adattulajdonosi jogosultságok**"). Abban az esetben, ha az Adattulajdonos szeretné jogait gyakorolni a személyes Microsoft-adatokra vonatkozó jogszabály keretein belül, a szállító köteles:		
15.	Segítse a Microsoftot megfelelő technikai és szervezeti intézkedésekkel, amilyen mértékben lehetséges, hogy teljesítse kötelezettségét a jogaik gyakorlását kezdeményező Adattulajdonosok kéréseire vonatkozó válasszal kapcsolatban.	Folyamatok és eljárások vannak érvényben az Adattulajdonosok jogérvényesítésének támogatására.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
16.	Indokolatlan késedelem nélkül válaszolni minden Adattulajdonos jogosultsági kéréseire.	A szállító rendszeres teszteket hajt végre, hogy biztosítsa, hogy képes támogatást nyújtani az Adattulajdonosok jogosultságaival kapcsolatban.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
17.	Hacsak nem kap ellenkező utasítást a Microsofttól, a beszállító továbbirányít a Microsofthoz minden Adattulajdonost, aki közvetlenül veszi fel vele a kapcsolatot az Adattulajdonosi jogosultságaik gyakorlása érdekében. A szállítónak tájékoztatnia kell minden Adattulajdonost azokról a lépésekről, amelyeket meg kell tennie annak érdekében, hogy hozzáférést nyerjen vagy más módon gyakorolhassa jogosultságait a személyes Microsoft-adataival kapcsolatban. *Írjon az SSPAHelp@microsoft.com címre a jelen előírással kapcsolatos segítségért.*	A szállító közli a Személyes adatok elérése érdekében teendő lépéseket, valamint az adatok aktualizálásához rendelkezésre álló módszereket.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
18.	Az Adattulajdonosnak való közvetlen válaszadáskor ellenőrizze a kérelmet benyújtó Adattulajdonos személyazonosságát.	A szállító dokumentálta a Microsoft-adattulajdonosok azonosításához használt módszert.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	F szakasz: Adattulajdonosok (folyt.)		
	Az Adattulajdonos ellenőrzése után a szállítónak az alábbiakat kell elvégeznie:		
19.	Határozza meg, hogy vannak-e a birtokában vagy a felügyelete alatt az adott Adattulajdonosra vonatkozó személyes Microsoft-adatok.	A szállító eljárásokkal rendelkezik annak megállapításához, hogy birtokol-e személyes adatokat.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
20.	Tegyen észszerű erőfeszítéseket a kért személyes Microsoft-adatok megkeresése érdekében, és vezessen megfelelő nyilvántartást az észszerű keresés elvégzésének bizonyítására.	A szállító nyilvántartást vezet az Adattulajdonosok jogosultságkéréseinek teljesítésekor megtett lépésekről. A dokumentáció tartalmazza: ▪ a kérelem dátumát és idejét, ▪ a kérelemre válaszul végrehajtott műveleteket és ▪ annak az időpontját, hogy erről mikor tájékoztatta a Microsoftot.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
21	Jegyezze fel az Adattulajdonosi jogok alapján kezdeményezett kérelmek dátumát és időpontját, illetve a szállító által ezen kérelmek teljesítése érdekében megtett intézkedéseket. A Microsoft kérésére mutassa be az adattulajdonosi kérelmekről vezetett nyilvántartást.	A szállító nyilvántartást vezet a hozzáférési kérelmekről, és dokumentálja a személyes adatokon végrehajtott változtatásokat.	
	Az Adattulajdonos ellenőrzése után, és miután a szállító ellenőrizte, hogy az adott személy kérelmezte-e a személyes Microsoft-adatokat, a szállítónak az alábbiakat kell elvégeznie:		
22	A személyes adatokról készített másolatra vonatkozó kérelmek esetén a személyes Microsoft-adatokat a megfelelő nyomtatott, elektronikus vagy szóbeli formátumban biztosítsa az Adattulajdonos részére.	A szállító a személyes adatokat az Adattulajdonos számára érthető, valamint az Adattulajdonos és a szállító számára megfelelő formában adja át.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	F szakasz: Adattulajdonosok (folyt.)		
23	Amennyiben a Microsoft elutasítja az Adattulajdonos kérelmét, a Microsoft által korábban adott vonatkozó utasításoknak megfelelően küldjön neki írásos magyarázatot. *Írjon az SSPAHelp@microsoft.com címre a jelen előírással kapcsolatos segítségért.*	Dokumentumpéldányok, amelyekben a kérések visszautasításra kerültek, és tanúsítják a Microsoft véleményezését és jóváhagyását.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
24	A szállítónak észszerű óvintézkedéseket kell tennie annak érdekében, hogy az Adattulajdonosnak kiadott személyes Microsoft-adatokat ne lehessen felhasználni másik személy azonosítására.	A szállítónak igazolnia kell, hogy észszerű óvintézkedéseket tett annak érdekében, hogy a kiadott adatokból másik személy ne legyen azonosítható (pl. nem készíthet fénymásolatot egy egész adatoldalról, amikor egy Adattulajdonossal kapcsolatos személyes adat egyetlen sorban található).	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
25	Ha egy Adattulajdonos és a szállító között nézeteltérés támad azzal kapcsolatban, hogy a személyes Microsoft-adatok hiánytalanok és pontosak-e, a szállító köteles felterjeszteni az ügyet a Microsofthoz, és az ügy megoldása érdekében köteles együttműködni a Microsofttal. *Írjon az SSPAHelp@microsoft.com címre a jelen előírással kapcsolatos segítségért.*	A szállító dokumentálja a nézeteltérés eseteit, és az ügyet felterjeszti a Microsofthoz.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	G szakasz: Az adatok kiadása külső feleknek		
	Ha a szállító alvállalkozót kíván alkalmazni a személyes és bizalmas Microsoft-adatok feldolgozásához, az alábbiakat kell elvégeznie:		
26	Szerezze be a Microsoft kifejezett írásos engedélyét a szolgáltatás alvállalkozásba adása előtt vagy bármilyen változtatás végrehajtás előtt, amely az alvállalkozók helyettesítésére vagy bővítésére vonatkozik. *A jelen előírással kapcsolatban az SSPAHelp@microsoft.com címen kérhet segítséget.*	Igazolja, hogy a személyes Microsoft-adatokat csak a Microsoft számára ismert vállalatok dolgozták-e fel, amint azt a vonatkozó szerződés (pl. munkaterv, kiegészítés, beszerzési rendelés) megköveteli, vagy ahogy az az SSPA-adatbázisban rögzítve lett.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
27	Dokumentálja az alvállalkozók által további feldolgozásra kerülő személyes és bizalmas Microsoft-adatok jellegét és mennyiségét, biztosítva, hogy csak a teljesítéshez szükséges adatok legyenek begyűjtve.	A szállító nyilvántartást vezet az alvállalkozókkal közölt vagy részükre átadott személyes és bizalmas Microsoft-adatokról.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
28	Biztosítsa, hogy az alvállalkozó a személyes Microsoft-adatokat kizárólag az Adattulajdonos által megadott kapcsolatfelvételi módnak megfelelően használja fel.	Mutassa be, hogyan használják fel az alvállalkozók a Microsoft-adattulajdonosok által megadott választást. Biztosítson támogató dokumentációt, amely tartalmazza az alvállalkozó számára a megadott választás módosítására való reagáláshoz szükséges időtartamot.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
29	Korlátozza a személyes Microsoft-adatok alvállalkozó általi feldolgozását olyan célokra, amelyek a szállító és a Microsoft között érvényes szerződés teljesítéséhez szükségesek.	A szállító biztosítani tudja azt a dokumentációt, amely bemutatja, hogy az alvállalkozónak átadott személyes Microsoft-adatokra szükség van a Teljesítéshez.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	G szakasz: Az adatok kiadása külső feleknek (folyt.)		
30	Tekintse át a személyes Microsoft-adatok engedély nélkül történő felhasználásával vagy jogszerűtlen feldolgozásával kapcsolatos panaszokat.	A szállító be tudja mutatni, hogy rendszerek és eljárások vannak érvényben olyan esetekkel kapcsolatos panaszok kezelésére, amelyek akkor merülnek fel, ha valamely alvállalkozó engedély nélkül használja fel vagy adja ki a személyes Microsoft-adatokat.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
31	Azonnal értesítse a Microsoftot, ha tudomására jut, hogy egy alvállalkozó nem a teljesítéssel kapcsolatos célból dolgozta fel a személyes vagy bizalmas Microsoft-adatokat.	A szállító útmutatót és eszközöket biztosított az alvállalkozó számára a Microsoft-adatokkal való visszaélés jelentéséhez.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
32	Haladéktalanul tegye meg a megfelelő intézkedéseket, hogy enyhítse a tényleges vagy lehetséges kárt, amelyet az alvállalkozó azzal okozott, hogy a személyes vagy bizalmas Microsoft-adatokat engedély nélkül vagy jogszerűtlenül dolgozta fel.	A szállító be tudja mutatni, hogy rendelkezik tervvel és eljárással arra az esetre, ha egy alvállalkozó nem megfelelően használná fel a személyes és bizalmas Microsoft-adatokat.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
	H szakasz: Minőség		
33	A szállítónak fenn kell tartania minden személyes Microsoft-adat sértetlenségét, biztosítva azok pontosságát, hiánytalanságát és tárgyhoz tartozó jellegét azokra a megállapított célokra vonatkozóan, amelyek érdekében feldolgozásuk megtörtént.	A szállító be tudja mutatni, hogy vannak eljárásai a személyes Microsoft-adatok ellenőrzésére azok gyűjtésekor, létrehozásakor és frissítésekor. A szállító be tudja mutatni, hogy megfigyelési és mintavételezési eljárások vannak érvényben a pontosság folyamatos ellenőrzésére, és szükség esetén a kijavítására.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	I szakasz: Figyelés és végrehajtás		
34	A szállító rendelkezik incidensek esetére kialakított választervvel, amely megköveteli, hogy a szállító indokolatlan késedelem nélkül értesítse a Microsoftot, amint a szállítónak a személyes vagy bizalmas Microsoft-adatok kezelésével kapcsolatos adatszivárgás vagy biztonsági rés jut tudomására. *Incidens bejelentéséhez írjon az SSPAHelp@microsoft.com címre.*	A szállító rendelkezik választervvel incidensek esetére, amely tartalmazza az ügyfelek (Microsoft) értesítésének lépéseit, amint az ebben a szakaszban szerepel.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
35.	Ne bocsásson ki semmilyen sajtóközleményt vagy más nyilvános értesítést a személyes vagy bizalmas Microsoft-adatok kiszivárgásáról a Microsoft jóváhagyása nélkül, kivéve, ha ezt jogszabály írja elő.	A szállító elfogadja a követelmény teljesítését, ha az esemény előfordul.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
36.	Valósítson meg kárelhárítási tervet, és kísérje figyelemmel a személyes vagy bizalmas Microsoft-adatok kiszivárgásának és biztonsági réseinek elhárítását, hogy kellő időben megtehesse a megfelelő intézkedéseket a probléma megoldására.	A szállító rendelkezik dokumentált eljárásokkal, amelyekkel az adatszivárgásra reagál.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
37	Hozzon létre hivatalos panaszkezelő eljárást a személyes Microsoft-adatokkal kapcsolatos összes adatvédelmi reklamáció megválaszolására.	A szállító rendelkezik eszközökkel a személyes Microsoft-adatokkal kapcsolatos panaszok fogadására, és van dokumentált panaszkezelési eljárása a panaszok kivizsgálásához.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság		
	A szállítónak egy olyan adatbiztonsági programot kell létrehoznia, alkalmaznia 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 szállító biztonsági programjának meg kell felelnie az alább rögzített szabályok 38–56. követelményének.	A biztosítékok meghaladhatják a felsoroltakat, ha az a szabályozói programok (pl. HIPAA, GLBA) vagy a szerződéses követelmények teljesítéséhez szükséges. Az ISO 27001 vagy SOC 2 szabvány szerinti érvényes biztonsági jelentések megfelelően helyettesítik a J szakasz követelményeit. A helyettesítés alkalmazásához írjon az SSPAHelp@microsoft.com címre. Megjegyzés: Ezeknek a tanúsítványoknak/jelentéseknek a hatókörleírásához dokumentációt kell biztosítania.	
38.	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 ▪ a módosítási naplók karbantartását.	A szállító dokumentálta a hálózati felméréseket, módosítási naplókat és 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.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
39.	A szállító kötelessége meghatározni, közölni és megvalósítani azt a mobileszközökkel kapcsolatos szabályzatot, amely biztosítja és korlátozza a mobileszközön elért vagy használt személyes vagy bizalmas Microsoft-adatok felhasználását.	A szállító bemutatja a megfelelő mobileszköz-szabályzat használatát, ha a személyes vagy bizalmas Microsoft-adatok feldolgozása mobileszköz használatát követeli meg.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
40.	A teljesítés támogatására használt valamennyi eszközzel el kell számolni, és ezeknek rendelkezniük kell egy azonosítható tulajdonossal. A beszállító felelős ezen információeszközök készletnyilvántartásáért, meghatározva ezen eszközök elfogadható és jogos használatát, és megfelelő szintű védelmet nyújtani 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.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
41.	A hozzáférési jogokra vonatkozó kezelési eljárások kialakítása és fenntartása annak érdekében, hogy megakadályozza az illetéktelen hozzáférést a szállító felügyelete alatti személyes vagy bizalmas Microsoft-adatok bármelyikéhez.	A szállító bemutatja, hogy megvalósított egy tervet a hozzáférési jogosultságok kezeléséhez, amely magában foglalja a következőket: ▪ hozzáférés-vezérlési eljárások; ▪ azonosítási eljárások; ▪ a sikertelen próbálkozásokat követő kizárási eljárások; ▪ új jelszó kérése a szükséges gyakorisággal, de nem később, mint 90 naponta; ▪ erőteljes paraméterek a hitelesítő adatok kiválasztására vonatkozóan; ▪ a felhasználói fiók foglalkoztatás megszűnésétől számított 48 órán belüli inaktiválása. A szállító bemutatja, hogy rendelkezik olyan 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 a szerepkörökhöz való hozzáférés engedélyezése felülvizsgálható; és ▪ annak tesztelését, hogy a szerepkörökön belüli felhasználók, akik hozzáférnek a Microsoft-adatokhoz, dokumentált igazolással rendelkeznek arra vonatkozóan, hogy a csoport/szerepkör tagjai.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
42.	Olyan javításkezelési eljárások meghatározása és megvalósítása, amelyek a személyes és bizalmas Microsoft-adatok feldolgozására használt rendszerek biztonsági javításait helyezik előtérbe. Ilyen eljárások többek között az alábbiak: ▪ meghatározott kockázaton alapuló megközelítés a biztonsági javítások elsőbbségivé tételéhez; ▪ vészhelyzet esetén szükséges hibajavítás kezelésére és megvalósítására 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 kivonási követelményei.	A szállító be tud mutatni megvalósított javításkezelési eljárást, amely megfelel ennek a követelménynek, és minimálisan lefedi a következőket: ▪ Súlyosság hozzárendelése a prioritásról való tájékoztatáshoz. (A súlyosság meghatározásai dokumentálva vannak.) ▪ Dokumentált eljárás a vészhelyzeti javítások megvalósításához. ▪ Annak ellenőrzése, hogy már nincsenek használatban olyan operációs rendszerek, amelyeket már nem támogat a szerző vállalat. ▪ Javításkezelési feljegyzések, amelyek nyomon követik a jóváhagyásokat és a kivételeket.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
43.	Víruskereső és kártevőirtó szoftverek telepítése a hálózathoz csatlakozó minden 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 védelmük érdekében. A kártevőirtó-definíciós fájlok napi, vagy a víruskereső/kártevőirtó beszállító által meghatározott intervallumonkénti frissítése. Megjegyzés: Ez az összes operációs rendszerre, többek között a Linuxra is vonatkozik.	Van nyilvántartás arról, hogy a víruskereső és kártevőirtó szoftvert aktívan használják. Megjegyzés: Ez a követelmény minden operációs rendszerre vonatkozik.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
44.	A Microsoft számára szoftvert fejlesztő szállítóknak a beépített biztonság alapelveit kell felhasználniuk a szoftverek összeépítési eljárásában.	A szállító műszaki specifikációs dokumentációja tartalmaz ellenőrzőpontokat a fejlesztési ciklusokban a biztonság ellenőrzéséhez.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
45.	Adatvesztés-megelőzési („**DLP**”) program alkalmazása. Az adatokat megfelelően besorolni, címkézni és védeni kell, a szállító pedig köteles megfigyelése alatt tartani a használt információs rendszert, amelyben a személyes és bizalmas Microsoft-adatok feldolgozása történik, hogy nem történt-e behatolás, adatvesztés vagy más jogosulatlan tevékenység. A DLP-program minimális feltételként megköveteli az alábbiakat: ▪ iparági szabványnak megfelelő üzemeltetési, hálózati és felhőalapú behatolásészlelő rendszerek („**IDS**”) használata, ha személyes vagy bizalmas Microsoft-adatokat tárol; ▪ speciális behatolásvédelmi rendszerek („**IPS**”) megvalósítása, amelyek az adatvesztés figyelésére és aktív megakadályozására vannak konfigurálva; ▪ a rendszerben történő biztonsági incidens esetén a rendszer elemzése annak érdekében, hogy meggyőződjön arról: minden fennmaradó biztonsági rés kezelése megtörtént; ▪ a rendszerbiztonság megsértését figyelő érzékelőeszközök kötelező eljárásainak dokumentálása; és ▪ az adatszivárgási események észlelésekor kötelezően végrehajtandó, az incidensre választ adó és azt kezelő folyamat létrehozása.	IDS/IPS üzembe helyezésének dokumentálása megfelelő eljárásokkal a válaszadás irányításához biztonsági rés vagy adatszivárgás észlelésekor.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
46.	Azonnal tájékoztassa a felsőbb szintű menedzsmentet és a Microsoftot az incidensre adott válasszal kapcsolatos kivizsgálási eredményekről. *Írjon az SSPAHelp@microsoft.com címre a Microsoft értesítéséhez.*	Rendszereknek és eljárásoknak kell érvényben lenniük az incidensre adott válasz vizsgálati eredményeinek Microsofttal történő közlésére.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
47	A rendszergazdáknak, a műveleti személyzetnek, a menedzsmentnek és a külső feleknek évente részt kell venniük biztonsági oktatáson.	Hozzon létre egy olyan biztonsági tréningprogramot, amely tartalmazza a következőket: ▪ éves incidensválasz-oktatás; és ▪ szimulált események és automatikus mechanizmusok a krízishelyzetekre adott hatékony válaszok megkönnyítése érdekében. Eseménymegelőzési tudatosság, úgymint a kártevő szoftverek letöltéséhez kapcsolódó kockázatok.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
48.	A szállítónak biztosítania kell, hogy a biztonságimentés-tervezési folyamatok megvédjék a személyes és bizalmas Microsoft-adatokat a jogosulatlan használattól, hozzáféréstől, közzétételtől, módosítástól és megsemmisítéstől.	A szállító be tud mutatni dokumentált válasz- és helyreállítási eljárásokat, amelyek részletezik, hogy a szervezet hogyan fog kezelni egy zavaró eseményt, és olyan előre meghatározott szinten tartja az adatbiztonságot, amely megfelel a menedzsment által jóváhagyott adatbiztonsági folyamatossági céloknak. A szállító be tudja mutatni, hogy olyan eljárásokat határozott és valósított meg, amelyek rendszeresen biztonsági másolatot készítenek, biztonságosan tárolják és hatékonyan helyreállítják a kritikus adatokat.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
49.	Hozzon létre és teszteljen az üzleti folyamatosságra és vészhelyreállításra vonatkozó terveket.	Egy vészhelyreállítási tervnek a következők mindegyikét tartalmaznia kell. ▪ Meghatározott feltételek, amelyek segítségével megállapítható, hogy egy adott rendszer kritikus fontosságú-e a szállító üzleti műveleteire vonatkozóan. ▪ Kritikus rendszerek listázása olyan előre meghatározott feltételek alapján, amelyek célja a katasztrófa esetén történő helyreállítás. ▪ Meghatározott vészhelyreállítási eljárás minden egyes kritikus rendszer számára, amely egy olyan mérnöknek is lehetővé teszi a rendszer helyreállítását 72 órán belül, aki nem ismeri a rendszert. ▪ A vészhelyreállítási tervek éves (vagy gyakoribb) tesztelése és felülvizsgálata annak érdekében, hogy a helyreállítási célok teljesüljenek.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
50.	Ellenőrizze a magánszemély személyazonosságát, mielőtt megadná neki a személyes vagy bizalmas Microsoft-adatokhoz való hozzáférést.	Győződjön meg arról, hogy minden felhasználói azonosító egyedi, illetve hogy mindegyikhez tartozik egy iparági szabványnak megfelelő hitelesítési módszer, például az Azure Active Directory. A rendszergazdai hozzáféréshez (rendszergazdai vagy más típusú kibővített jogosultságok) kötelező egy második tényező kérése, például intelligens kártya vagy telefonalapú hitelesítés.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
51.	A szállítónak meg kell védenie a személyes és bizalmas Microsoft-adatokat a hálózatok közötti továbbítás során Transport Layer Security („**TLS**”) vagy IPsec protokoll („**IPsec**”) használatával történő titkosítással. Ezek a metódusok le vannak írva a NIST 800-52-ben és a NIST 800-57-ben; valamint egyenértékű iparági szabvány is alkalmazható. A szállítónak vissza kell utasítania a nem titkosított úton továbbított személyes vagy bizalmas Microsoft-adatok átadását.	A TLS vagy más tanúsítványok létrehozásának, üzembe helyezésének vagy lecserélésének folyamata kötelezően meghatározandó és alkalmazandó.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
52.	Minden olyan szállítói eszköznek (hordozható számítógép, munkaállomás stb.), amely elér vagy kezel személyes vagy bizalmas Microsoft-adatokat, lemezalapú titkosítást kell alkalmaznia.	Titkosítson minden eszközt, hogy megfeleljen a BitLocker vagy más egyenértékű lemeztitkosítási iparági megoldásnak minden olyan eszköz esetében, amelyet személyes vagy bizalmas Microsoft-adatok kezelésére használnak.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
53.	A jelenlegi ipari szabványokat, például a NIST 800-111 szabványt használó rendszereket és eljárásokat kell alkalmazni nyugalmi állapotban (tárolás közben) végzett titkosításhoz az összes személyes és/vagy bizalmas Microsoft-adat tárolására, többek között az alábbiakhoz: ▪ 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); ▪ 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, fizikai (nem vállalati) cím; ▪ személyes (nem vállalati) telefonszámok; ▪ vallás; ▪ politikai vélemény; ▪ szexuális irányultság/beállítottság; ▪ biztonsági kérdésekre adott válaszok (pl. 2fa, jelszó-visszaállítás); ○ anya leánykori neve.	Ellenőrizze, hogy az ebben a sorban felsorolt személyes és bizalmas Microsoft-adatok tárolás közben titkosítva vannak-e.	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*
54.	Amikor a Microsoft nevében kezel hitelkártyákat, tartsa be az alkalmazandó hitelkártya-kezelési szabványokat a kártya kibocsátójának megfelelően.	Igazolja megfelelőségét a Payment Card Industry Data Security Standard („**PCI DSS**”) tanúsítvány éves benyújtásával. *A PCI DSS tanúsítványokat az SSPA részére nyújtsa be. Ha bármilyen kérdése van, írjon az SSPAHelp@microsoft.com címre.*	*<Megfelelő>* *<Nem megfelelő>* *<Nem alkalmazható>* *<Jogi ütközés>* *<Szerződési ütközés>*

#	Microsoft szállítói adatvédelmi követelmények	A megfelelőség bizonyítéka	Válaszlépés
	J szakasz: Biztonság (folyt.)		
55.	A szállítónak a fizikai Microsoft-eszközöket ellenőrzött hozzáférésű környezetben kell tárolnia.	Rendszerek és eljárások vannak érvényben a Microsoft-adatok digitális, papíralapú, archív és biztonsági másolataihoz való fizikai hozzáférés kezelésére. Nyomon kell követni a felügyeleti láncot a Microsoft-adatokat tartalmazó fizikai eszközök mozgásának és megsemmisítésének megfigyelése érdekében.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*
56.	Anonimizáljon a fejlesztői vagy tesztkörnyezetben használt minden személyes Microsoft-adatot.	A személyes Microsoft-adatok nem alkalmazhatók fejlesztési vagy tesztkörnyezetekben. Ha nincs más lehetőség, megfelelően anonimizálni kell, hogy megakadályozzák az Adattulajdonosok azonosítását vagy a személyes adatokkal való visszaélést. 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 tulajdonosa nem, vagy már nem azonosítható.	*<Megfelelő> <Nem megfelelő> <Nem alkalmazható> <Jogi ütközés> <Szerződési ütközés>*