Microsoft Beszerzés

Szállítói biztonsági és adatvédelem-biztosítási (SSPA) program útmutató

8. verzió

2022. június

Bevezetés

Mi a Microsoftnál hiszünk benne, hogy az adatvédelem alapvető jog. Küldetésünk során, hogy a bolygó minden magánszemélyét és szervezetét segítsük abban, hogy többet érhessen el, minden nap azon fáradozunk, hogy kiérdemeljük és megőrizzük ügyfeleink bizalmát.

A szigorú adatvédelmi és biztonsági gyakorlatok kritikus fontosságúak küldetésünk teljesítéséhez, létfontosságúak ügyfeleink bizalmához, és számos illetőségi területen a törvény is megköveteli azokat. A Microsoft adatvédelmi és biztonsági irányelveiben rögzített normák a vállalatként képviselt értékeinket tükrözik, és ezek kiterjednek beszállítóinkra (mint például az Önök vállalatára) is, akik a nevünkben adatokat dolgoznak fel.

A szállítói biztonsági és adatvédelmi biztosítási program (**SSPA**) a Microsoft érvényben lévő vállalati programja, amelyben a Microsoft az alapvető adatfeldolgozási utasításait a szállítói számára a Microsoft szállítói adatvédelmi követelményeiben (**DPR**) összefoglalja, és amely megtalálható az SSPA Microsoft.com/Procurement oldalán. Ne feledje: előfordulhat, hogy a szállítóknak egyéb, szervezeti szintű követelményeknek is meg kell felelniük, amelyekről az SSPA kereteink kívül tájékoztatja a szállítóval való együttműködésért felelős Microsoft csoport.

Az SSPA kulcskifejezéseit a DPR definiálja. A programról bővebben a Gyakran ismételt kérdések (GYIK) oldalunkon olvashat, illetve a globális csoportunktól érdeklődhet a SSPAHelp@microsoft.com címen.

Az SSPA program áttekintése

Az SSPA a Microsoft beszerzés, a vállalati külkapcsolatok és jogi ügyek, valamint a vállalati biztonság csoportok közötti partneri együttműködés annak biztosítása érdekében, hogy szállítóink betartsák az adatvédelmi és biztonsági alapelveinket.

Az SSPA hatálya kiterjed globálisan minden olyan szállítóra, akik személyes adatokat és/vagy bizalmas Microsoft adatokat kezelnek az adott szállító teljesítésével összefüggésben (pl. szolgáltatások nyújtása, szoftverlicencek, felhőszolgáltatások), a Microsofttal kötött szerződése feltételei szerint (pl. beszerzési rendelésekben szereplő feltételek, keretszerződés) („**teljesít**”, „**teljesítés folyamatban**” vagy „**teljesítés**”).

Az SSPA lehetővé teszi a szállítók számára a szerződésük teljesítésével érintett termékeknek és/vagy szolgáltatásoknak megfelelő adatfeldolgozói profil kiválasztását. Ezek a választások érvénybe léptetik a hozzájuk tartozó követelményeket, amelyek a megfelelőségi biztosítékot nyújtanak a Microsoft számára.

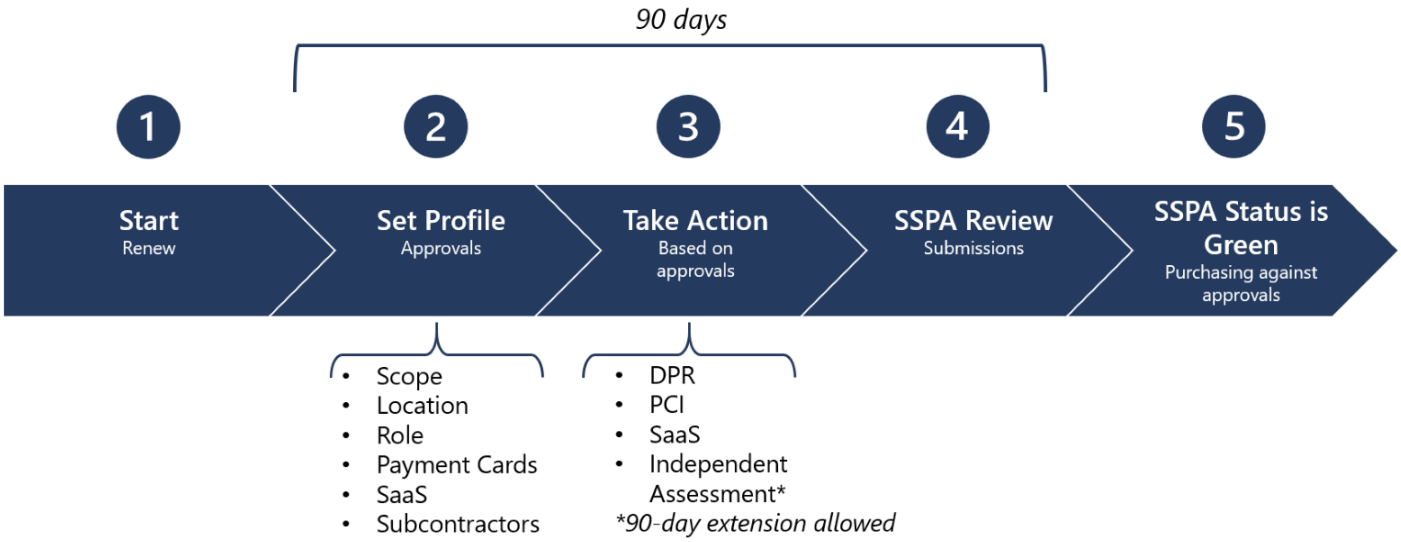
Minden regisztrált szállító évente önbevallást tesz a DPR-nak való megfelelőségéről. Az adatfeldolgozói profilja határozza meg, hogy a teljes DPR, vagy a követelmények egy része vonatkozik-e a vállalatára. Előfordulhat, hogy azoknak a szállítóknak, akik a Microsoft megítélése szerint magasabb kockázatú adatokat dolgoznak fel, további követelményeknek is eleget kell tenniük, például független megfelelőségi tanúsítványt kell biztosítaniuk. Azoknak a szállítóknak, akik közzétett

Microsoft megbízott adatfeldolgozói listán szerepelnek, szintén független megfelelőségi tanúsítvánnyal kell rendelkezniük.

Fontos: A megfelelőségi tevékenységek alapján az SSPA állapot zöld (megfelelő) vagy vörös (nem megfelelő) lehet. A Microsoft beszerzési eszközei ellenőrzik, hogy az SSPA-állapot zöld legyen (az SSPA hatálya alá tartozó minden szállító esetében), mielőtt a megállapodás tovább léphetne.

SSPA eljárási diagram – Új szállító Regisztráció

SSPA eljárási diagram – Éves szállítói megújítás



Az SSPA hatálya

Annak meghatározásához, hogy Ön (a szállító) dolgoz-e fel személyes adatokat és/vagy Microsoft bizalmas adatokat, az alábbi táblázatokban található listák nyújtanak segítséget. Ne feledje, hogy ezek csak példák, nem pedig kimerítő lista.
Megjegyzés: Egy Microsoft vállalkozás tulajdonosa kérheti a regisztrációját a listán kívüli esetekben is a feldolgozott adatok bizalmasságára tekintettel.

Személyes adatok adattípus szerint

Például, de nem kizárólagosan:

Érzékeny adatok
Gyermekekkel kapcsolatos adatok
Genetikai adatok, biomertikus adatok vagy egészségügyi adatok
Rassz vagy etnikai hovatartozás
Politikai, vallási vagy filozófiai hitrendszer, vélemény vagy hovatartozás
Szakszervezeti tagság
Természetes személy nemi élete vagy szexuális irányultsága
Bevándorló státusz (vízum, munkavállalási engedély stb.)
Kormányzati azonosítók (útlevél, jogosítvány, vízum, társadalombiztosítási azonosító számok, nemzeti azonosító számok)
Pontos felhasználói helyadatok (300 méteren belüli)
Személyes bankszámlaszámok
Hitelkártya száma és lejárata
Ügyfél kapcsolattartási adatai
Dokumentumok, fényképek, videók, zene stb.
Egy termékre vagy szolgáltatásra adott érékelések és/vagy minősítések
Kérdőívre adott válaszok
Böngészési előzmények, érdeklődési körök és kedvencek
Szabadkézi elemek, gépelt szövegek és beszédelemek (hang és/vagy csevegés/robot)
Hitelesítő adatok (jelszavak, jelszó-emlékeztetők, felhasználónév, azonosításra használt biometrikus adatok)
Támogatási esettel kapcsolatos ügyféladatok

Rögzített és generált adatok
Pontatlan helyadatok
IP-cím
Eszközbeállítások és személyre szabások
Webhelyek szolgáltatásainak használata, webhely-kattintások követése
Közösség média adatok, szociális gráf kapcsolatok
Csatolt eszközöktől származó tevékenységadatok, pl. edzésprogramok
Kapcsolattartási adatok, mint név, cím, telefonszám, e-mail cím, születés ideje, függőségi és segélyhívási kapcsolattartók
Csalás- és kockázatelemzés, háttérellenőrzés
Biztosítás, nyugdíj, juttatás adatai
Jelentkezők önéletrajza, interjú feljegyzések/visszajelzés
Metadata and telemetry
Fiókadatok
Fizetőeszköz adatok
Hitelkártya száma és lejárata
Bankazonosító adatok
Bankszámlaszám
Hiteligénylések vagy hitelelőzmények
Adózási dokumentumok és azonosítók
Befektetési vagy költségadatok
Vállalati kártyák
Végfelhasználók álnevesített adatai (EUPI) (A Microsoft által a Microsoft termékek és szolgáltatások felhasználóinak azonosítására létrehozott azonosítók)
Globális egyedi azonosító (GUID)
Útlevél felhasználói azonosító vagy egyedi azonosító (PUID)
Hasított végfelhasználói azonosító adatok (EUII)
Munkamenet-azonosítók
Eszközazonosítók
Diagnosztikai adatok
Naplóadatok

Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

Microsoft bizalmas adatok adatosztály szerint

Például, de nem kizárólagosan:

Szigorúan bizalmas
A Microsoft termékek vagy a Microsoft termékek elemeinek fejlesztésével, tesztelésével vagy gyártásával kapcsolatos, vagy arra vonatkozó adatok. *A bármely csatornán kereskedelmi forgalomban lévő Microsoft szoftverek, online szolgáltatások vagy hardverelemek mindegyike „**Microsoft termék**".*
Microsoft eszközök bevezetés előtti marketing információi
A SEC szabályok hatálya alá tartozó be nem jelentett Microsoft vállalati pénzügyi adatok
Bizalmas
A Microsoft termékek a Microsoft nevében bármely módon megosztott licenckulcsai
A Microsoft belső üzletági (LOB) alkalmazásainak fejlesztésével vagy tesztelésével kapcsolatos vagy arra vonatkozó információ
A Microsoft szoftverek és szolgáltatások, például az Office, SQL, Azure stb. kiadás előtti marketinganyagai
A Microsoft szolgáltatások és termékek, például eszközök (eljárás- vagy folyamat-útmutatók, konfigurációs adatok stb.) írott, terv-, elektronikus vagy nyomtatott dokumentációja.

Fontos: Egy Microsoft vállalkozás tulajdonosa kérheti a részvételét a listán kívüli adatokra is.

Adatfeldolgozói profil

A Microsoft szállítók ellenőrzik a saját SSPA adatfeldolgozói profiljukat.

Ez lehetővé teszi a szállítók számára, hogy eldöntsék, milyen tevékenységek végrehajtására kívánnak jogosulttá válni. Gondosan ügyeljen a választására és vegye fontolóra a megfelelőségi tevékenységeket, amelyeket a jóváhagyás beszerzéséhez teljesítenie kell. **Lásd a „Biztosítási követelmények" szakaszt lentebb, valamint az A függeléket.**

A Microsoft üzleti csoportok csak olyan szállítókkal működhetnek együtt, ahol az adatfeldolgozási tevékenység megfelel a szállító által beszerzett jóváhagyásoknak.

A szállítók az év során bármikor frissíthetik az adatfeldolgozói profiljukat, **amennyiben nincsenek nyitott ügyleteik**. Módosítás esetén a megfelelő tevékenység előírásra kerül, és azt a jóváhagyás megszerzése előtt teljesíteni kell. A meglévő, már teljesített jóváhagyások maradnak érvényben addig, míg az újonnan előírt követelmények teljesítve nem lesznek.

Ha az újonnan végrehajtandó feladatok nem teljesülnek a rendelkezésre álló 90 napos időkeretben, az SSPA állapot vörösre (nem megfelelő) vált, és a partner inaktiválásra kerülhet a Microsoft szállítói számlázás rendszerében.

Adatfeldolgozói jóváhagyások	
1	Adatfeldolgozás hatálya ▪ Bizalmas ▪ Személyes, bizalmas
2	Adatfeldolgozás helye ▪ Microsoft vagy ügyfél ▪ Szállító
3	Adatfeldolgozói szerep ▪ Adatkezelő (független vagy társkezelő) ▪ Feldolgozó ▪ Megbízott adatfeldolgozó (Microsoft által kijelölt)
4	Pénzforgalmi kártya feldolgozás ▪ Igen ▪ Nem érvényes
5	Szoftver, mint szolgáltatás ▪ Igen ▪ Nem érvényes
6	Alvállalkozók bevonása ▪ Igen ▪ Nem érvényes

Jóváhagyási szempontok

Adatfeldolgozás hatálya

Bizalmas

Válassza ezt a jóváhagyást, ha a szállító teljesítésébe kizárólag Microsoft bizalmas adatok feldolgozása tartozik.

Ha ezt a jóváhagyást választja, nem lesz jogosul személyes adatok feldolgozásával járó feladatokra.

Személyes, bizalmas

Válassza ezt a jóváhagyást, ha a szállító teljesítésébe személyes adatok és Microsoft bizalmas adatok feldolgozása tartozik.

Feldolgozás helye

Microsoft vagy ügyfél

Válassza ezt a jóváhagyást, ha a szállító a teljesítés során az adatfeldolgozást a Microsoft hálózati környezetében végzi, ahol az alkalmazottak *@microsoft.com* hozzáférési hitelesítő adatokat használnak, vagy a Microsoft egy ügyfelének környezetében.

A következő esetekben ne válassza ezt a lehetőséget:

- A szállító egy kijelölt Microsoft offshore létesítményt (OF) kezel.
- A szállító erőforrásokat biztosít a Microsoft számára, és időnként a Microsoft hálózatában, máskor azon kívül dolgozik. A hálózaton kívüli munkavégzés során a feldolgozás helye a „szállító".

Szállító
Ha a „Microsoft vagy ügyfél" feltétel (a fentiek szerint) nem érvényes, válassza ezt a lehetőséget.

_____

Adatfeldolgozói szerep

Adatkezelő (független és közös adatkezelők)

Válassza ezt a jóváhagyást, ha a szállító teljesítésének **minden** vonatkozása megfelel az Adatkezelő adatfeldolgozói szerepkör definíciójának (lásd DPR).

Ha ezt a jóváhagyást választja, nem lesz jogosul személyes adatok feldolgozására „Feldolgozó" szerepkörrel. Ha a szállító egyszerre Feldolgozó és Adatkezelő is a Microsoftnál, ne az Adatkezelő, inkább a Feldolgozó szerepkört válassza ki.

Feldolgozó

Ez a leggyakoribb feldolgozói szerepkör, amikor a szállítók a Microsoft nevében adatokat dolgoznak fel. Kérjük, olvassa el a Feldolgozó definícióját a DPR-ben.

Megbízott adatfeldolgozó

A megbízott adatfeldolgozó olyan harmadik fél, akivel a Microsoft teljesítést végeztet, ahol a teljesítés magában foglalja olyan Microsoft személyes adatok kezelését, amelyek feldolgozója a Microsoft. A szállítók nem sorolhatják be magukat a Microsoft megbízott adatfeldolgozójaként, mivel ehhez a belső adatvédelmi csoportok előzetes jóváhagyása szükséges. A szállító csak abban az esetben lehet megbízott adatfeldolgozó, ha a Microsoft az adatfeldolgozó, és a szállító minősített nagyvállalati személyes adattípusokat dolgoz fel. A megbízott adatfeldolgozókra kiegészítő szerződés és megfelelőségi követelmények vonatkoznak, beleértve az adatvédelmi függeléket és egy független felmérést is (lásd lentebb).

Pénzforgalmi kártya feldolgozás

Válassza ezt a jóváhagyást, ha a szállító által végzett adatfeldolgozás bármely részébe beletartozik a Microsoft nevében hitelkártya vagy más pénzforgalmi kártya feldolgozását támogató adatok feldolgozása.

Az a jóváhagyás lehetővé teszi a szállítónak, hogy részt vegyen pénzforgalmi kártya feldolgozással járó megbízásokban.

_____

Szoftver

A Microsoft beszerzés minden szoftveres vásárlás esetén a vevőket egy felvételi folyamaton vezeti át, amely számos ellenőrzésből áll, amelybe beletartozik az SSPA osztályozás is annak meghatározására, hogy a szoftvert biztosító szállító az SSPA-felügyelet hatálya alá tartozik-e. (A Microsoft vásárlók további részleteket a belső ProcureWeb szoftver és felhőszolgáltatás oldalon bemutatott kivonatban találnak). Ha SSPA szükséges, előfordulhat, hogy a szállítóknak azonosítaniuk kell, hogy a „Szoftver, mint szolgáltatás" (SaaS) profilválasztás alkalmazandó-e. Az SSPA-regisztrált szállítók ezt megtehetik, amikor az adatfeldolgozási profiljukat a Microsoft megfelelőségi portálján kitöltik.

SSPA-megfelelőségi okokból a SaaS kibővített értelmezését alkalmazzuk, amelybe beletartozik a platform, mint szolgáltatás (PaaS) és az infrastruktúra, mint szolgáltatás (IaaS) is. (A SaaS-ra vonatkozó további információért olvassa el ezt a magyarázatot.)

Szoftver, mint szolgáltatás (SaaS)

A Szoftver, mint szolgáltatás (SaaS) lehetővé teszi a felhasználók számára, hogy interneten keresztül csatlakozzanak és használjanak felhőalapú alkalmazásokat.

A Microsoft definíciója szerint a **szoftver, mint szolgáltatás (SaaS)** egy egy-a-többhöz modellben alkalmazott, közös kódra épülő szoftver, használatalapú, vagy használati metrikákra épülő előfizetéses számlázással. A felhőszolgáltató fejleszti és tartja karban a felhőalapú szoftvert, automatikus szoftverfrissítéseket biztosít, és az ügyfelei számára az interneten keresztül teszi elérhetővé a szoftverét egy-a-többhöz, használatalapú fizetéses modellben. A szoftverszállítás és -licencelés ilyen módja a szoftverhez előfizetésen keresztüli online hozzáférést biztosít ahelyett, hogy a megvásárolt szoftvert miden egyes számítógépre telepíteni kellene.

Megjegyzés: A legtöbb SaaS szolgáltatónak hozzá kell adnia az Alvállalkozói jóváhagyást a Microsoft szállítói megfelelőségi portálon, ha a személyes adatot vagy a Microsoft bizalmas adatot külső partner platformján tárolja.

Alvállalkozók bevonása

Válassza ezt a jóváhagyást, ha a szállító a teljesítéshez alvállalkozó(ka)t vesz igénybe (definíciókat lásd a DPR-ben).

A szabadúszók is ide értendők (lásd DPR).

Biztosítási követelmények

Követelmények a profilban szereplő jóváhagyások alapján

Az adatfeldolgozási profiljában kiválasztott jóváhagyások segítenek az SSPA-nak a Microsofttal való teljes együttműködéséhez kapcsolódó kockázati szint felmérésében. Az SSPA-megfelelőségi követelmények az adatfeldolgozási profiltól és a hozzá kapcsolódó jóváhagyásoktól függően változnak. Ez a szakasz a különböző SSPA-követelményeket mutatja be.

Vannak olyan kombinációk is, amelyek fokozhatják vagy csökkenthetik a megfelelőségi követelményeket. A kombinációkat az A függelék tartalmazza, és a profilja kitöltésekor ennek előírására számíthat a Microsoft megfelelőségi portálon. Bármikor ellenőrizheti, hogy az Ön esete hogyan illeszkedik a keretrendszerbe, ha felülvizsgálatot kér az SSPA csoporttól.

Művelet: Keresse meg a jóváhagyási profilját az A függelékben, és tekintse át a megfelelő biztosítási követelményeket és független biztosítási opciókat, ha vannak.

Fontos: Ha a profilja szoftver, mint szolgáltatás (SaaS), alvállalkozók, web tárhely szolgáltatás vagy pénzforgalmi kártyák opciót tartalmaz, további biztosítás szükséges.

DPR önbevallás

Minden SSPA-regisztrált felhasználónak el kell végeznie a DPR-megfelelőségi önbevallást az igénytől számított 90 napon belül. Az igény évente várható, de ennél gyakoribb is lehet, ha év közben módosítja az adatfeldolgozási profilját. A szolgáltató partnerek SSPA állapota vörösre (nem megfelelő) vált, ha a 90 napos határidőt túllépik. Új hatókörön belüli megrendeléseket nem lehet feldolgozni, amíg az SSPA-állapot zöldre (megfelelő) nem vált.

Az újonnan regisztrált szállítóknak az előírt követelményeket teljesíteniük kell ahhoz, hogy az SSPA állapotuk zöld (megfelelő) legyen, és csak ezt követően kezdődhet meg az együttműködés.

Fontos: Az SSPA csapat nem jogosult ennek a feladatnak a meghosszabbítására.

Az önbevallást végző jogosult képviselőknek gondoskodniuk kell arról, hogy elegendő információt szerezzenek be a téma szakértőitől ahhoz, hogy magabiztosan meg tudják válaszolni az egyes követelményeket. Ezen felül, nevük feltüntetésével az SSPA adatlapon igazolják, hogy elolvasták és megértették az adatvédelmi követelményeket (DPR). A szállítók további kapcsolattartókat is felvehetnek az online eszközeikbe, hogy segítsenek a követelmények teljesítésében.

A jogosult képviselő (definíciót lásd a DPR-ben) feladata:

1. Meghatározni, hogy mely követelmények érvényesek.
2. Megválaszolni minden alkalmazandó követelményt.
3. Aláírni és beküldeni az önbevallást a Microsoft szállítói megfelelőségi portálon.

Alkalmazhatóság

A szállítóktól elvárt, hogy megválaszolják az összes, az adatfeldolgozási profil alapján előírt alkalmazandó DPR-követelményt. Számítani lehet arra, hogy az előírtak közül esetleg néhány nem alkalmazandó azokra a termékekre vagy szolgáltatásokra, amelyeket a szállító a Microsoft számára biztosít. Ezeket „nem érvényes" jelzéssel és részletes magyarázattal lehet ellátni, amelyet az SSPA-felülvizsgálók ellenőriznek.

Az SSPA csapat minden benyújtott DPR-ben megvizsgálja a „nem érvényes", „helyi jogszabályokba ütközik" vagy „szerződéses ellentét" jelzéseket az előírt követelményeknél. Az SSPA csapat kérheti egy vagy több választás magyarázatát. A helyi jogszabályokba ütközik és szerződéses ellentét csak abban az esetben elfogadható, ha van ezt igazoló hivatkozás, és az ellentét egyértelmű.

Független felmérési követelmény

Nézze meg az A függelék Követelmények jóváhagyások szerint szakaszában, hogy mely jóváhagyások váltják ki ezt a követelményt.

A szállítók az adateldolgozási profiljuk frissítésével módosíthatják a jóváhagyásokat. Viszont, ha a szállító adatfeldolgozói szerepköre Megbízott adateldolgozó, a szállító ezt a jóváhagyást nem módosíthatja, és évente el kell végeztetnie a független felmérést.

A megfelelőség független igazolását igénylő jóváhagyások biztosítására a szállítóknak választaniuk kell egy független felmérőt, aki ellenőrzi a DPR-nak való megfelelőségüket. A felmérőnek egy tanácsadói levelet kell elkészíteniük, amelyben megfelelőségi igazolást biztosítanak a Microsoft számára. Ennek a levélnek nem minősítettnek kell lennie, én minden meg nem felelőségi problémát fel kell oldani és orvosolni kell a megerősítő levél Microsoft szállítói megfelelőségi portálon SSPA csoport általi felülvizsgálatra való benyújtása előtt. A felmérők letölthetnek egy jóváhagyott tanácsadói levél sablont, amely az „Ajánlott felmérők" PDF melléklete, és elérhető itt.

Az **A függelék** tartalmazza az elfogadott tanúsítási alternatívákat, ha úgy dönt, hogy nem vesz igénybe független felmérőt a DPR-megfelelőség igazolására (ahol alkalmazandó, például SaaS szolgáltatók, web tárhely szolgáltatók, vagy alvállalkozókat igénybe vevő szállítók esetén). Az ISO 27701 (adatvédelem) és ISO 27001 (biztonság) elfogadható, mint a DPR. közeli megfeleltetése.

Ha a szállító az Amerikai Egyesült Államokban egészségügyi szolgáltató vagy fedett entitás, az adatvédelmi és biztonsági területekre elfogadjuk a HITRUST jelentést.

Az SSPA manuálisan is végrehajthat egy független felmérést, ha a normál kiváltókon kívüli körülmények további kellő gondosság alkalmazását igénylik. Ilyen lehet például a részleg adatvédelmi vagy biztonsági szakembereinek kérése, adatvédelmi incidens elhárításának ellenőrzése, vagy automatizált adatalanyi joggyakorlásra vonatkozó követelmény.

Útmutató a követelmény megközelítéséhez:

1. A feladatot a megfelelőség kielégítő felméréséhez megfelelő technikai képzettséggel és szakértelemmel rendelkező felmérőnek kell végrehajtania.

2. A felmérőnek az International Federation of Accountants (IFAC) vagy az American Institute of Certified Public Accountants (AICPA)társvállalatának kell lennie, vagy más releváns adatvédelmi és biztonsági szervezet tanúsítványával kell rendelkeznie, mint például az International Association of Privacy Professionals (IAPP) vagy az Information Systems Audit and Control Association (ISACA).
3. A felmérőnek a legfrissebb DPR alapján kell dolgoznia, amelyben megtalálható az egyes követelmények támogatásához szüksége bizonyíték. **A szállítóknak a legfrissebb jóváhagyott DPR bevallásukban foglalt válaszokat kell a felmérő rendelkezésére bocsátaniuk.**
4. Újonnan regisztrált szállítók esetében a felmérő teszteli a folyamatvezérlők tervezését. A felmérő minden esetben teszteli a vezérlők hatékonyságát.
5. A felmérési megbízás hatóköre az adott szállító teljesítéséhez kapcsolódó személyes adatokra és/vagy Microsoft bizalmas adatokra korlátozódik
6. A megbízás hatóköre azon szállító partner azonosítószáma alatt végrehajtott adatfeldolgozási tevékenységekre korlátozódik, amely az igény címzettje. Ha a szállító egyszerre több szállító partnert is választ, **a tanúsító levélben pontosan fel kell tüntetni a felmérésben részt vevő szállító partnerek listáját, és azok címeit**.
7. Az SSPA számára küldött levélben nem szerepelhetnek olyan nyilatkozatok, amely szerint a szállító nem felel meg a leírt adatvédelmi követelményeknek. Ezeket a problémákat a levél beküldése előtt javítani kell.

Az SSPA az ajánlott felmérők listáját elérhetővé tette. Ezek a vállalatok gyakorlattal rendelkeznek az SSPA felmérések végzésében. A szállítóknak ezekért a felmérésekért fizetniük kell; a költség az adatfeldolgozás nagyságától és terjedelmétől függően változik.

PCI DSS tanúsítási követelmény

A pénzforgalmi kártyák üzletági adatbiztonsági normája (PCI DSS) keretrendszert biztosít a robusztus pénzforgalmi kártya adatbiztonsági megoldások fejlesztéséhez, amely tartalmazza a biztonsági incidensek megelőzését, észlelését, valamint az azokra való megfelelő reagálást. A keretrendszert a PCI biztonsági szabványügyi bizottsága, egy önszabályozó iparági szervezet dolgozta ki. A PCI DSS követelmények célja a technológiai és eljárásbeli gyenge pontok azonosítása, amelyek kockáztatják a kártyatulajdonos feldolgozás alatt álló adatainak biztonságát.

A Microsoftnak meg kell felelnie ezeknek a normáknak. Ha egy szállító a Microsoft nevében pénzforgalmi kártya adatokat kezel, attól megköveteljük az ezen normáknak való megfelelőség bizonyítását. Tájékozódjon a PCI biztonsági szabványügyi bizottságnál a PCI szervezet által felállított követelmények jobb megértéséhez.

A feldolgozott tranzakciók mennyiségének függvényében egy szállítónak vagy minősített biztonsági felmérővel kell igazoltatnia a megfelelőségét, vagy kitölthet egy önfelmérő adatlapot.

A pénzforgalmi kártya márkák határozzák meg a felmérés típusának küszöbértékét, általában a következőképpen:

- 1. szint: Külső felmérőtől származó PCI AOC tanúsítvány

- 2. vagy 3. szint: PCI DSS önfelmérő kérdőív (SAQ), amelyet a szállító tisztviselője ír alá

Küldje be azt a tanúsítványt, amelyik érvényes, és megfelel a PCI követelményeinek.

Szoftver, mint szolgáltatás követelmény

Azoktól a szolgáltatóktól, akik megfelelnek az adatfeldolgozási profilon szereplő SaaS definíciónak, kérhetünk érvényes ISO 27001 tanúsítványt, ha ez szerepel a Microsoft felhőszolgáltatási szerződésében.

Az SSPA felülvizsgálók ellenőrzik, hogy a beküldés megfelel.e a szerződéses kötelezettségeknek.

Kérjük, ne küldjön be adatközpont tanúsítványt! Az elvárás az ISO 27001 tanúsítvány, amely a Microsofttal kötött szerződésében szereplő szoftver szolgáltatás(ok)ra vonatkozik.

Alvállalkozók bevonása

A Microsoft az alvállalkozók bevonását magas kockázati tényezőnek tekinti. Azoknak a szállítóknak, akik személyes és Microsoft bizalmas adatok feldolgozásába alvállalkozókat vonnak be, meg kell nevezniük az alvállalkozóikat. Ezen kívül a szállítónak meg kell jelölnie azokat az országokat is, ahol az egyes alvállalkozók az adatokat feldolgozzák.

Adatvédelmi incidensek

Ha egy szállítónak adatvédelmi vagy biztonsági incidens jut a tudomására, a szállítónak a DPR szerinti, abban meghatározott módon tájékoztatnia kell a Microsoftot.

Az adatvédelmi incidenst a SupplierWeb oldalon vagy emailben a SuppIR@microsoft.com címen jelezze

Ne felejtse el a következőket megadni:

- Adatvédelmi incidens dátuma:
- Szállító neve:
- Szállító száma:
- Értesített Microsoft kapcsolattartó(k):
- Érintett PO, ha alkalmazandó/elérhető:
- Az adatvédelmi incidens összefoglalása:

A függelék

Követelmények a profilban szereplő jóváhagyások alapján

#	Profil	Biztosítási követelmények	Független biztosítási opciók
1	**Hatókör:** Személyes, bizalmas **Feldolgozás helye:** Microsoft vagy ügyfél **Adatfeldolgozói szerep:** Feldolgozó vagy Adatkezelő **Adatosztály:** Bizalmas **vagy** Szigorúan bizalmas **Pénzforgalmi kártyák:** Nem érvényes **SaaS:** Nem érvényes **Alvállalkozók bevonása:** Nem érvényes **Web tárhely szolgáltatás:** Nem érvényes	A DPR-megfelelőség önbevallása	
2	**Hatókör:** Bizalmas **Feldolgozás helye:** Szállító **Adatfeldolgozói szerep:** N. é. **Adatosztály:** Bizalmas **Pénzforgalmi kártyák:** Nem érvényes **SaaS:** Nem érvényes **Alvállalkozók bevonása:** Nem érvényes **Web tárhely szolgáltatás:** Nem érvényes	A DPR-megfelelőség önbevallása	
3	**Hatókör:** Bizalmas **Feldolgozás helye:** Szállító **Adatfeldolgozói szerep:** Feldolgozó **Adatosztály:** Szigorúan bizalmas **Pénzforgalmi kártyák:** Nem érvényes **SaaS:** Nem érvényes **Alvállalkozók bevonása:** Nem érvényes **Web tárhely szolgáltatás:** Nem érvényes	A DPR-megfelelőség önbevallása **és** Független megfelelőségi biztosíték	Független biztosítási opciók: 1. A DPR-megfelelőség független felmérettetése, **vagy** 2. ISO 27001 beküldése

#	Profil	Biztosítási követelmények	Független biztosítási opciók
4	**Hatókör:** Személyes, bizalmas **Feldolgozás helye:** Szállító **Adatfeldolgozói szerep:** Feldolgozó **Adatosztály:** Szigorúan bizalmas **Pénzforgalmi kártyák:** Nem érvényes **SaaS:** Nem érvényes **Alvállalkozók bevonása:** Nem érvényes **Web tárhely szolgáltatás:** Nem érvényes	A DPR-megfelelőség önbevallása **és** Független megfelelőségi biztosíték	Független biztosítási opciók: 1. A DPR-megfelelőség független felmérettetése, 2. A DPR A-I megfelelőség független felmérettetése és ISO 27001, **vagy** 3. ISO 27701 **és** ISO 27001 beküldése
5	**Hatókör:** Személyes, bizalmas **Feldolgozás helye:** Szállító **Adatfeldolgozói szerep:** Feldolgozó **Adatosztály:** Bizalmas **Pénzforgalmi kártyák:** Nem érvényes **SaaS:** Nem érvényes **Alvállalkozók bevonása:** Nem érvényes **Web tárhely szolgáltatás:** Nem érvényes	A DPR-megfelelőség önbevallása	
6	**Hatókör:** Személyes, bizalmas **Feldolgozás helye:** Szállító **Adatfeldolgozói szerep:** Adatkezelő **Adatosztály:** Szigorúan bizalmas vagy Bizalmas **Pénzforgalmi kártyák:** Nem érvényes **SaaS:** Nem érvényes **Alvállalkozók bevonása:** Nem érvényes **Web tárhely szolgáltatás:** Nem érvényes	A DPR-megfelelőség önbevallása	

#	Profil	Biztosítási követelmények	Független biztosítási opciók
7	**Hatókör:** Személyes, bizalmas **Feldolgozás helye:** Bármely **Adatfeldolgozói szerep:** Megbízott adatfeldolgozó (ez egy Microsoft által kijelölt szerepkör - a profilban a „Megbízott adatfeldolgozói jóváhagyás: Igen“ látható) **Adatosztály:** Szigorúan bizalmas vagy Bizalmas **Pénzforgalmi kártyák:** Nem érvényes **SaaS:** Nem érvényes **Alvállalkozók bevonása:** Nem érvényes **Web tárhely szolgáltatás:** Nem érvényes	A DPR-megfelelőség önbevallása **és** Független megfelelőségi biztosíték	Független biztosítási opciók: 1. A DPR-megfelelőség független felmérettetése, 2. A DPR A-I megfelelőség független felmérettetése és ISO 27001, **vagy** 3. ISO 27701 **és** ISO 27001 beküldése

#	Profil	Biztosítási követelmények	Független biztosítási opciók
A SaaS, Alvállalkozók, Web tárhely szolgáltatás hozzáadásának hatása			
8	**Hatókör:** Személyes, bizalmas **Feldolgozás helye:** Szállító **Adatfeldolgozói szerep:** Feldolgozó **Adatosztály:** Szigorúan bizalmas vagy Bizalmas **Pénzforgalmi kártyák:** Nem érvényes **Alvállalkozók:** IGEN vagy **SaaS:** IGEN vagy **Web tárhely szolgáltatás:** IGEN	A DPR-megfelelőség önbevallása **és** Független megfelelőségi biztosíték	Független biztosítási opciók: 1. A DPR-megfelelőség független felmérettetése, 2. A DPR A-I megfelelőség független felmérettetése és ISO 27001, **vagy** 3. ISO 27701 **és** ISO 27001 beküldése
9	**Hatókör:** Személyes, bizalmas **Feldolgozás helye:** Szállító **Adatfeldolgozói szerep:** Adatkezelő **Adatosztály:** Szigorúan bizalmas vagy Bizalmas **Pénzforgalmi kártyák:** Nem érvényes **Alvállalkozók:** IGEN vagy **SaaS:** IGEN vagy **Web tárhely szolgáltatás:** IGEN	A DPR-megfelelőség önbevallása	

#	Profil	Biztosítási követelmények	Független biztosítási opciók
Kiegészítő biztosítás pénzforgalmi kártyák és SaaS esetén			
10	A fent profilok bármelyike és **Pénzforgalmi kártyák**	A fenti vonatkozó követelmények **és** a pénzforgalmi kártyákra vonatkozó iparági biztosítás	PCI DSS tanúsítvány beküldése
11	A fenti profilok bármelyike és **Szoftver, mint szolgáltatás (SaaS)**	A fenti vonatkozó követelmények **és** küldje be a szerződésben megkövetelt ISO 27001 tanúsítványt a funkcionális szolgáltatások vonatkozásában.	ISO 27001 tanúsítvány beküldése a nyújtott szolgáltatás(ok) funkcionális lefedésével.