Microsoftova nabava

Priročnik za program zagotavljanja varnosti in zasebnosti za dobavitelje (SSPA)

različica 7

november 2020

Uvod

V Microsoftu menimo, da je zasebnost temeljna pravica. Naše poslanstvo je vsakemu posamezniku ali organizaciji na tem planetu omogočiti, da doseže več; vsakodnevno si prizadevamo pridobiti in ohraniti zaupanje strank.

Strogi postopki glede zasebnosti in varnosti so ključni za naše poslanstvo ter nujni za ohranjanje zaupanja uporabnikov, v nekaterih sodnih pristojnostih pa jih terja zakonodaja. Standardi, opredeljeni v Microsoftovih pravilnikih o zasebnosti in varnosti, odražajo vrednote našega podjetja in se prenašajo na dobavitelje (kot je vaše podjetje), ki v našem imenu obdelujejo Microsoftove podatke.

Program zagotavljanja varnosti in zasebnosti za dobavitelje (»**SSPA**«) je Microsoftov interni program za zagotavljanje temeljnih navodil za obdelavo podatkov Microsoftovim dobaviteljem v obliki Microsoftovih zahtev za varstvo podatkov (»**ZVP**«), ki so na voljo v okviru SSPA na spletnem mestu Microsoft.com/Procurement. Upoštevajte, da bodo dobavitelji morda morali izpolniti dodatne zahteve na organizacijski ravni, ki jih Microsoftova skupina, odgovorna za interakcijo z dobaviteljem, določi in o njih obvesti zunaj programa SSPA.

Najpomembnejši izrazi za SSPA so definirani v ZVP. Če želite več informacij o programu, preberite naše odgovore na pogosta vprašanja in se obrnite na našo globalno skupino tako, da nam pišete na SSPAHelp@microsoft.com.

Pregled programa SSPA

SSPA je partnerstvo med Microsoftovimi oddelki za nabavo, notranje in zunanje pravne zadeve ter varnost v podjetju, katerega namen je zagotoviti, da naši dobavitelji spoštujejo načela varnosti in zasebnosti.

SSPA velja za vse Microsoftove dobavitelje, ki obdelujejo osebne podatke ali Microsoftove zaupne podatke v okviru dobaviteljevega izvajanja (npr. zagotavljanja storitev, licence za programsko opremo, oblačne storitve) na podlagi določil pogodbe z Microsoftom (npr. določila naročilnice, krovna pogodba) (»**izvesti**«, »**izvajati**« ali »**izvedba**«).

SSPA dobavitelju omogoča izbiro profilov obdelave podatkov, ki so usklajeni z blagom in/ali storitvami, ki jih pogodbeno izvajate. Ti izbori sprožijo ustrezne zahteve za zagotavljanje skladnosti Microsoftu.

Vsi včlanjeni dobavitelji bodo vsako leto opravili samopotrditev skladnosti z ZVP. Vaš profil za obdelavo podatkov določa, ali se izda celoten ZVP ali zgolj podnabor zahtev. Dobavitelji, ki obdelujejo podatke, ki jih Microsoft obravnava kot podatke z večjim tveganjem, bodo morda morali izpolniti dodatne zahteve, kot je zagotavljanje neodvisnega preverjanja skladnosti.

Pomembno: Dejavnosti zagotavljanja skladnosti so podlaga za določanje zelenega (skladno) ali rdečega (neskladno) stanja SSPA. Microsoftova orodja za nabavo preverijo, da je stanje v programu SSPA zeleno (za vsakega dobavitelja v obsegu SSPA), preden dovolijo nadaljevanje sodelovanja.

Diagram postopka za SSPA – Včlanitev novega dobavitelja

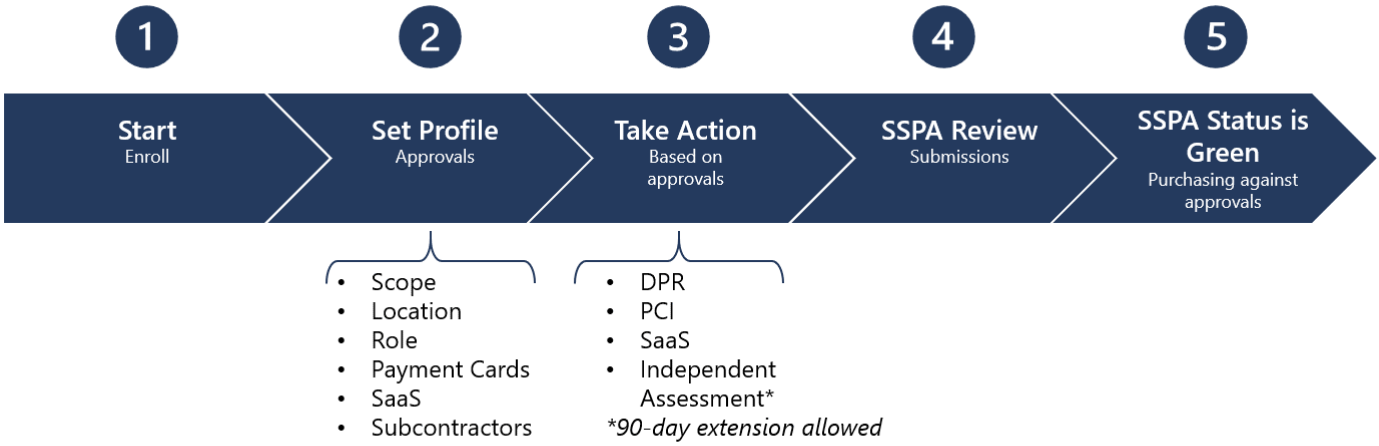
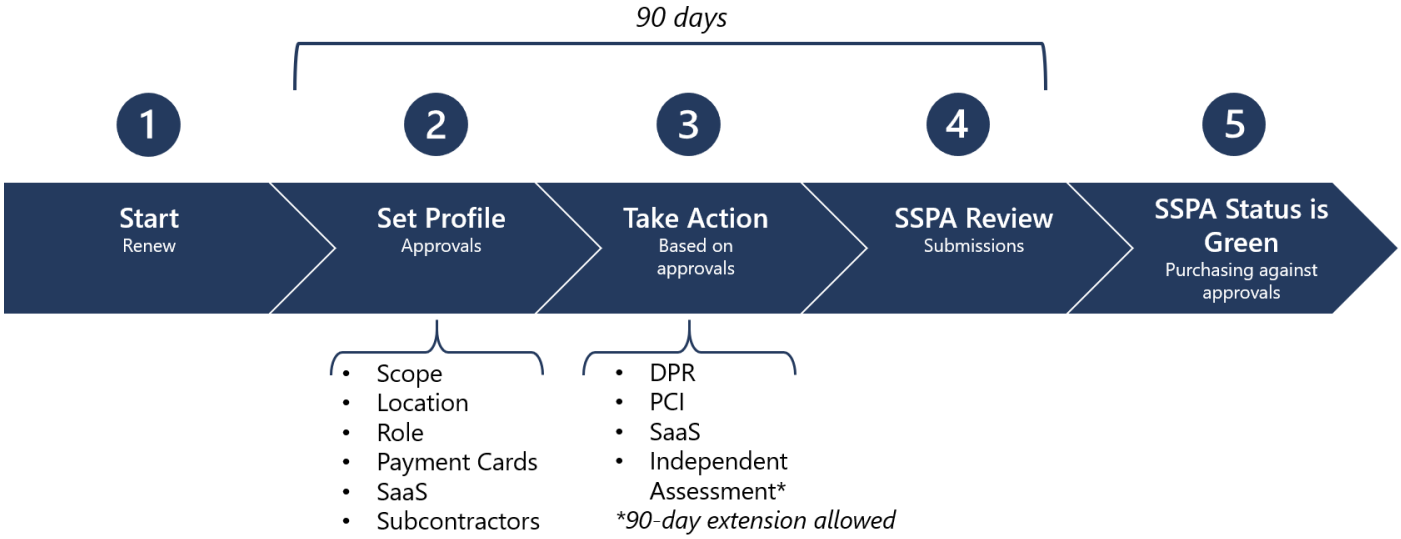


Diagram postopka za SSPA – Letno podaljšanje dobavitelja



Obseg programa SSPA

Za pomoč pri ugotavljanju, ali vaše podjetje (dobavitelj) obdeluje osebne podatke in/ali Microsoftove zaupne podatke, si oglejte seznam primerov v spodnjih tabelah. Upoštevajte, da so to primeri in ne izčrpen seznam.
Opomba: Microsoftov lastnik podjetja lahko zahteva včlanitev zunaj tega seznama glede na zaupno naravo obdelanih podatkov.

Osebni podatki glede na vrsto podatkov

Primeri med drugim vključujejo:

Občutljive podatke
podatke, povezane z otroki;
genetske, biometrične in zdravstvene podatke;
podatke o rasnem ali etničnem izvoru;
politične, verske ali filozofske poglede, mnenja ali pripadnosti;
članstvo v sindikatu;
spolno življenje ali spolno usmeritev fizične osebe;
status bivanja v državi (vizum, delovno dovoljenje itd.);
državne identifikatorje (potni list, vozniško dovoljenje, vizum, nacionalne identifikacijske številke, davčne številke);
natančne podatke o lokaciji uporabnika (do 300 m natančno);
Podatke o vsebini strank
dokumente, fotografije, videoposnetke, glasbo ipd.;
mnenja in/ali ocene, vnesene v izdelku ali storitvi;
odgovore na ankete;
zgodovino brskanja, zanimanja in priljubljena spletna mesta;
rokopisne vnose, tipkanje in glasovne vnose (glas/zvok in/ali klepet/bot);
podatke poverilnic (gesla, namigi za gesla, uporabniška imena, biometrični podatki, uporabljeni za identifikacijo);
podatke o stranki, povezane s prošnjo za podporo;

Zajete in generirane podatke
nenatančne podatke o lokaciji;
naslov IP;
nastavitve in prilagoditve naprav;
uporabo storitev za spletna mesta, sledenje klikov na spletnih straneh;
podatke iz družbenih omrežij, odnose z družbenega grafikona;
podatke o dejavnosti iz povezanih naprav, kot so merilniki telesne dejavnosti;
podatke za stik, kot so ime, naslov, telefonska številka, e-poštni naslov, datum rojstva, podatki za stik z vzdrževanimi družinskimi člani in za stik v sili;
ugotavljanje goljufij in presojo tveganj, preverjanje preteklosti
podrobnosti o zavarovanju, pokojnini in ugodnostih;
življenjepise kandidatov, opombe/povratne informacije o razgovorih;
Podatke o računu
podatke o plačilnih sredstvih;
številko in datum poteka kreditne kartice;
podatke za usmerjanje bančnih nakazil;
številko bančnega računa;
prošnje za kreditiranje ali kreditne linije;
davčne dokumente in identifikatorje;
podatke o naložbah ali stroških;
službene kartice;
Psevdoanonimizirane podatke o končnih uporabnikih (identifikatorji, ki jih Microsoft ustvari za prepoznavanje uporabnikov Microsoftovih izdelkov in storitev)
globalno enolične identifikatorje (GUID);
ID-je uporabnika potnega lista ali enolične identifikatorje (PUID);
zgoščene podatke končnega uporabnika, ki jih je mogoče prepoznati;
ID-je sej;
ID-je naprav;
diagnostične podatke;
dnevniške podatke.

Microsoftovi zaupni podatki glede na razred podatkov

Primeri med drugim vključujejo:

Zelo zaupno
informacije glede razvoja, testiranja ali proizvodnje Microsoftovih izdelkov ali delov Microsoftovih izdelkov oziroma povezane s tem. *Microsoftova strojna in programska oprema, spletne storitve ali storitve, ki so javno naprodaj prek katerega koli distribucijskega kanala, se obravnavajo kot »**Microsoftov izdelek**«;*
predizdajne trženjske informacije o Microsoftovih napravah;
neobjavljene finančne podatke družbe Microsoft, za katere veljajo pravila komisije za vrednostne papirje in borzo (SEC).
Zaupno
licenčne ključe za Microsoftove izdelke v imenu Microsofta za distribucijo na kakršen koli način;
informacije glede razvoja ali preskušanja Microsoftovih internih programov za vodenje poslovanja;
Microsoftovo predizdajno trženjsko gradivo za Microsoftovo programsko opremo in storitve, kot so Office, SQL, Azure itd.;
pisno, oblikovno, elektronsko ali tiskano dokumentacijo za vse Microsoftove storitve ali izdelke, kot so naprave (priročniki za procese in postopke, konfiguracijski podatki ipd.).

Pomembno: Microsoftove osebe, odgovorne za vaše podjetje, lahko zahtevajo sodelovanje za podatke, ki niso navedeni na tem seznamu.

Profil obdelave podatkov

Microsoftovi dobavitelji imajo popoln nadzor nad svojim profilom za obdelavo podatkov SSPA.

To dobaviteljem omogoča, da se odločijo, do katerih vrst sodelovanj želijo biti upravičeni. Bodite zelo pozorni na izbire in upoštevajte dejavnost za zagotavljanje skladnosti, ki jo je treba izvesti za doseganje odobritve. **Glejte spodnji razdelek »Zahteve glede zagotovil« in prilogo A**.

Microsoftove poslovne skupine bodo lahko ustvarile sodelovanja samo z dobavitelji, katerih dejavnost obdelave podatkov se ujema z odobritvami, ki jih je prejel dobavitelj.

Dobavitelji bodo lahko kadar koli med letom posodobili svoj profil za obdelavo podatkov, **če ni odprtih opravil**. Ko pride do spremembe, bo izdana ustrezna dejavnost, ki jo je treba opraviti, preden so izdane odobritve. Obstoječe opravljene odobritve bodo veljale, dokler niso izpolnjene novoizdane zahteve.

Če novosprožena opravila niso opravljena v dovoljenem 90-dnevnem obdobju, bo status v programu SSPA postal RDEČ in obstajala bo možnost, da bo račun deaktiviran iz Microsoftovih sistemov za plačilne obveznosti.

Opozorilo: Če posodobitev profila začnete pred letnim podaljšanjem, vendar se ne odločite za nobeno spremembo, bo sistem sprožil ustrezne zahteve, ki jih bo treba znova izpolniti.

Odobritve za obdelavo podatkov	
1	Obseg obdelave podatkov ▪ Zaupno ▪ Osebno, zaupno
2	Kraj obdelave podatkov ▪ Pri Microsoftu ali stranki ▪ Pri dobavitelju
3	Vloga pri obdelavi podatkov ▪ Upravljavec (skupni upravljavec ali neodvisni upravljavec) ▪ Obdelovalec (obdelovalec ali podobdelovalec)
4	Obdelava plačilnih kartic ▪ Da ▪ Ni ustrezno
5	Programska oprema kot storitev ▪ Da ▪ Ni ustrezno
6	Uporaba podizvajalcev ▪ Da ▪ Ni ustrezno

Dejavniki pri odobritvi

Obseg obdelave podatkov

Zaupno

To odobritev izberite, če bo v dobaviteljevo izvajanje vključena samo obdelava Microsoftovih zaupnih podatkov. Oglejte si definicije v ZVP.

Če izberete to odobritev, ne boste upravičeni do sodelovanj z obdelavo osebnih podatkov.

Osebno, zaupno

To odobritev izberite, če bo v dobaviteljevo izvajanje vključena obdelava osebnih podatkov in Microsoftovih zaupnih podatkov. Oglejte si definicije v ZVP.

_____

Kraj obdelave

Pri Microsoftu ali stranki

To odobritev izberite, če bo v dobaviteljevo izvajanje vključena dobaviteljeva obdelava podatkov v Microsoftovem omrežnem okolju, kjer osebje uporablja poverilnice za dostop z domeno *@microsoft.com*, ali v okolju Microsoftove stranke.

Te možnosti ne izberite v teh okoliščinah:

- Dobavitelj upravlja zunajteritorialni objekt, ki ga določi Microsoft.
- Dobavitelj zagotavlja sredstva Microsoftu in občasno dela v Microsoftovem omrežju in zunaj njega. Kraj obdelave za delo zunaj omrežja se obravnava kot »pri dobavitelju«.

Pri dobavitelju
Če ni izpolnjen pogoj »pri Microsoftu ali stranki« (kot je opisano zgoraj), izberite to možnost.

_____

Vloga pri obdelavi podatkov

Upravljavec (velja za skupne in neodvisne upravljavce)

To odobritev izberite, če **vsi** vidiki izvajanja ustrezajo upravljavčevi definiciji obdelave podatkov (glejte ZVP).

Če izberete to odobritev, ne boste upravičeni do obdelave osebnih podatkov v vlogi »obdelovalec«. Če je dobavitelj tako obdelovalec kot tudi upravljavec za Microsoft, ne izberite možnosti »Upravljavec«, temveč »Obdelovalec«.

Obdelovalec (velja za obdelovalce in podobdelovalce)

To je najpogostejša vloga obdelave, ko dobavitelji obdelujejo podatke v Microsoftovem imenu. Oglejte si definicije obdelovalca in podobdelovalca v ZVP.

_____

Obdelava plačilnih kartic

To odobritev izberite, če kateri koli del podatkov, ki jih obdeluje dobavitelj, vključuje podatke za podporo obdelave kreditnih ali drugih plačilnih kartic v Microsoftovem imenu.

Ta odobritev dobavitelju omogoča sodelovanje pri obdelavi plačilnih kartic.

_____

Programska oprema kot storitev (SaaS)

To odobritev izberite, če dobaviteljeva izvedba vključuje zagotavljanje storitve Microsoftu z uporabo internetne tehnologije, ki pokriva dostop do strežnika in njegovo uporabo, shranjevalna omrežja in podatkovna središča. Dobavitelj obdeluje podatke zunaj Microsoftovih prostorov ali okolja. Primeri oblačnih storitev so med drugim programska oprema kot storitev (»SaaS«), platforma kot storitev (»PaaS«) ali infrastruktura kot storitev (»IaaS«).

Microsoft definira »SaaS« kot zagotavljanje funkcij programske opreme prek internetnega mehanizma, ki temelji na skupni kodi, uporabljeni v modelu ena-na-mnogo s plačilom na podlagi uporabe oziroma naročnino na podlagi meritev uporabe.

Uporaba podizvajalcev

To odobritev izberite, če dobavitelj za izvajanje uporablja podizvajalce. Oglejte si definicije v ZVP.

Zahteve glede zagotovil

Zahteve na podlagi odobritev profilov

Odobritve, ki jih dobavitelj izbere v svojem profilu za obdelavo podatkov, programu SSPA pomagajo pri ocenjevanju stopnje tveganja za Microsoftovo sodelovanje z dobaviteljem z vidika obdelave podatkov. Zahteve glede dobaviteljeve skladnosti s SSPA se razlikujejo glede na odobritve in profile dobavitelja. V tem razdelku pojasnjujemo različne zahteve glede SSPA.

Obstajajo tudi kombinacije, ki lahko povišajo ali znižajo zahteve za zagotavljanje skladnosti. Kombinacije so navedene v prilogi A in lahko pričakujete, da bo ob dokončanju profila to treba izvesti v portalu za zagotavljanje skladnosti dobaviteljev. Kako primeren za to ogrodje je vaš način uporabe, lahko kadar koli preverite tako, da zahtevate pregled skupine za SSPA.

Ukrep: V prilogi A poiščite svoj profil odobritve ter preverite ustrezne zahteve glede zagotovil in morebitne možnosti za neodvisno zagotovilo.

Pomembno: Če v profilu izberete programsko opremo kot storitev (SaaS), podizvajalce, gostovanje spletnih mest ali plačilne kartice, so potrebna dodatna zagotovila.

Samopotrditev za ZVP

Vsi dobavitelji, včlanjeni v program SSPA, morajo v roku 90 dni po prejemu zahteve opraviti samopotrditev skladnosti z ZVP. Ta zahteva bo izdana vsakoletno, vendar je lahko pogostejša, če se profil za obdelavo podatkov spremeni sredi leta. Če je presežen 90-dnevni rok, bo status računa dobavitelja v programu SSPA postal RDEČ (ni skladno). Obdelava novih naročilnic v obsegu ne bo mogoča, dokler ni status v programu SSPA spet zelen (skladno).

Novovčlanjeni dobavitelji morajo pred začetkom sodelovanj skladno z izbori odobritev izpolniti zahteve za pridobitev zelenega (skladno) statusa SSPA.

Kot je že bilo navedeno, profil za obdelavo podatkov določa, ali se izda celoten ZVP ali pa velja zgolj podnabor. Te odobritve je mogoče spremeniti vse leto, vendar je treba pri vsaki spremembi izpolniti povezane zahteve, preden začne veljati sprememba.

Pomembno: Skupina za SSPA ni pooblaščena za odobritev podaljšanj roka za to opravilo.

Pooblaščeni zastopniki, ki opravijo samopotrditev, morajo zagotoviti, da imajo zadostne informacije strokovnjakov za ustrezno področje, da lahko z gotovostjo odgovorijo na vsako zahtevo. Poleg tega ta oseba s podpisom obrazca programa SSPA potrdi, da je prebrala in razumela ZVP. Dobavitelji lahko v spletno orodje vedno dodajo dodatne stike za pomoč pri izpolnjevanju zahtev.

Pooblaščeni zastopnik (glejte definicijo) mora:

1. ugotoviti, katere zahteve so primerne;
2. objaviti odgovor za vsako upoštevno zahtevo;
3. v Microsoftovem portalu za zagotavljanje skladnosti dobaviteljev podpisati in predložiti potrditev.

Veljavnost

Pričakujemo, da se dobavitelji odzovejo na vse upoštevne zahteve glede ZVP, izdane glede na profil za obdelavo podatkov. Pričakovano je, da v okviru izdanih zahtev nekatere morda ne bodo veljale za blago ali storitve, ki jih dobavitelj zagotavlja Microsoftu. Te lahko označite kot »ne velja« in dodate podroben komentar, ki ga bodo pregledovalci za SSPA preverili.

Predložitve za ZVP pregleda skupina za SSPA in se prepriča, ali kateri od izborov »ne velja«, je v »lokalnem pravnem navzkrižju« ali »pogodbenem navzkrižju« z izdanimi zahtevami. Pregledovalci preverijo dejavnost sodelovanja, povezano z računom dobavitelja, da potrdijo izbor »ne velja«. Skupina za SSPA lahko zahteva dodatno pojasnilo za eno ali več izbir. Lokalna pravna navzkrižja ali pogodbena navzkrižja so sprejeta samo, če so priložena ustrezna dokazila in je navzkrižje jasno.

Zahteva za neodvisno ocenjevanje

Za ogled odobritev za obdelavo podatkov, ki sprožijo to zahtevo, glejte razdelek »Zahteve glede na odobritve« v prilogi A.

Dobavitelji imajo možnost, da odobritve spremenijo tako, da posodobijo svoj profil za obdelavo podatkov.

Za pridobitev odobritev, za katere je potrebno neodvisno preverjanje skladnosti, bodo dobavitelji morali izbrati neodvisnega ocenjevalca, ki bo preveril izpolnjevanje zahtev ZVP. Ocenjevalec pripravi svetovalno pismo za Microsoft z zagotovili o skladnosti z zahtevami. To pismo mora biti brezpogojno in razrešene morajo biti vse težave z neskladnostjo ter morebitne posledice teh neskladnosti odpravljene, preden se pismo predloži v pregled skupini za SSPA na Microsoftovem portalu za zagotavljanje skladnosti dobaviteljev. Ocenjevalci, ki potrebujejo predlogo, odobreno za svetovalno pismo, nam lahko pišejo na SSPAHelp@Microsoft.com.

Priloga A vključuje sprejemljive alternative k pridobivanju potrdila, če se odločite, da ne želite uporabiti neodvisnega ocenjevalca za preverjanje skladnosti z ZVP (ko je primerno, na primer za dobavitelje storitev SaaS ali spletnega gostovanja oziroma dobavitelje s podizvajalci). Uporabljata se standarda ISO 27701 (zasebnost) in ISO 27001 (varnost), saj sta tesno usklajena z zahtevami za varstvo podatkov (ZVP).

Pomembno: Poročila SOC 2 (z varnostnim kritjem) ne bodo sprejeta po **decembru 2021**.

SSPA lahko ročno sproži neodvisno ocenjevanje, če poleg standardnih sprožiteljev obstajajo okoliščine, zaradi katerih je potreben dodaten skrbni pregled. To je lahko zahteva oddelka glede zasebnosti ali varnosti; preverjanje odpravljanja posledic dogodkov, povezanih s podatki; zahteva za samodejno uveljavljanje pravic osebe, na katero se nanašajo osebni podatki.

Nasveti, kako se lotiti te zahteve:

1. Postopek mora izvesti ocenjevalec, ki je zadostno tehnično usposobljen in dovolj pozna temo, da lahko primerno oceni skladnost z zahtevami.
2. Ocenjevalci morajo biti povezani z mednarodno zvezo računovodij (International Federation of Accountants oz. IFAC) ali ustanovo American Institute of Certified Public Accountants (AICPA) oziroma morajo imeti potrdila ustreznih organizacij za zagotavljanje zasebnosti in varnosti, kot sta International Association of Privacy Professionals (IAPP) in Information Systems Audit and Control Association (ISACA).
3. Ocenjevalec mora uporabiti najnovejše ZVP, kar vključuje dokazila, potrebna za podporo posameznim zahtevam. **Dobavitelji bodo morali ocenjevalcu predložiti svoje nazadnje odobrene odgovore za potrditev za ZVP.**
4. Če gre za novovčlanjenega dobavitelja, bo ocenjevalec preskusil zasnovo postopkovnih mehanizmov nadzora. V vseh drugih primerih bo ocenjevalec preskušal učinkovitost mehanizmov nadzora.
5. Obseg ocenjevalnega sodelovanja je omejen na Microsoftove osebne podatke ali Microsoftove zaupne podatke v povezavi z izvajanjem zadevnega dobavitelja.
6. Obseg sodelovanja je omejen na vso dejavnost obdelave podatkov v obsegu, izvedeno za številko dobaviteljevega računa, ki je prejela zahtevo. Če se dobavitelj odloči za ocenjevanje več računov dobaviteljev hkrati, mora **pismo o potrditvi vključevati seznam računov dobaviteljev, vključenih v ocenjevanje, in povezane naslove.**
7. Pismo, predloženo SSPA, ne sme vključevati morebitnih izjav, da dobavitelj ne more izpolniti pisnih zahtev za varstvo podatkov. Te težave je treba rešiti pred pošiljanjem pisma.

V programu SSPA je sestavljen seznam prednostnih ocenjevalcev. Ta podjetja imajo izkušnje z opravljanjem ocenjevanj SSPA. Od dobaviteljev se pričakuje, da bodo plačali to ocenjevanje; stroški se razlikujejo glede na obseg in zahtevnost obdelave podatkov, za katero je potrebno zagotavljanje skladnosti.

Zahteva glede potrdila PCI DSS

Standard za varnost podatkov Payment Card Industry Data Security Standard (PCI DSS) je ogrodje za razvoj zanesljive varnosti za podatke o plačilnih karticah, ki zajema preprečevanje in odkrivanje varnostnih incidentov ter ustrezno odzivanje nanje. To ogrodje je razvil svet za varnostne standarde PCI (PCI Security Standards Council), samoregulativna sektorska organizacija. Zahteve PCI DSS so namenjene odkrivanju ranljivosti v tehnologiji in procesih, ki ogrožajo varnost podatkov imetnika kartice, ki se obdelujejo.

Microsoft mora ravnati skladno s temi standardi. Če dobavitelj v Microsoftovem imenu obdeluje podatke za plačilo, potrebujemo dokazila o skladnosti s temi standardi. Za podrobno pojasnilo zahtev, ki jih določa organizacija PCI, se obrnite na svet za varnostne standarde PCI.

Odvisno od količine transakcij, ki jih obdeluje, bomo od dobavitelja zahtevali potrdilo o skladnosti od usposobljenega ocenjevalca varnosti ali obrazec s samooceno.

Blagovne znamke plačilnih kartic običajno določajo prag za vrsto ocenjevanja:

- Raven 1: potrebno je potrdilo zunanjega ocenjevalca za PCI DSS.
- Raven 2 ali 3: potreben je vprašalnik za samoocenjevanje za PCI DSS, ki ga podpiše član uprave dobavitelja.

Program SSPA sprejema obe vrsti ocenjevanj. Pošljite potrdilo, ki je ustrezno in izpolnjuje zahteve PCI.

Zahteva za SaaS

Dobavitelji, ki Microsoftu zagotavljajo programsko opremo kot storitev, morajo priskrbeti veljavno potrdilo za ISO 27001 za funkcionalno kritje storitve programske opreme, ki jo upravlja dobavitelj.

Upoštevajte, da SSPA ne pričakuje potrdila tretje osebe za podatkovno središče kot v preteklosti – pričakujemo potrdilo za ISO 27001 za storitve programske opreme, ki se zagotavljajo Microsoftu in so navedene v vaši pogodbi z Microsoftom.

Uporaba podizvajalcev

Microsoft uporabo podizvajalcev obravnava kot dejavnik velikega tveganja.

ZVP zahteva, da dobavitelji obvestijo Microsoft, ko za obdelavo podatkov v obsegu uporabljajo zunanje izvajalce. To je mogoče storiti prek SSPA.

Podatkovni dogodki

Če dobavitelj izve za dogodek, povezan z zasebnostjo ali varnostjo podatkov, mora obvestiti Microsoft, kot je podrobno opisano v ZVP. Glejte ustrezno definicijo v prilogi B.

Po e-pošti Microsoft obvestite na naslov SSPAHelp@microsoft.com s tem obrazcem: Prijava podatkovnega dogodka. Vključiti morate naslednje:

- Datum podatkovnega dogodka:
- Ime dobavitelja:
- Številka dobavitelja:
- Obveščena oseba za stik pri Microsoftu:
- Povezana naročilnica (če je primerno):
- Povzetek podatkovnega dogodka:

Priloga A

Zahteve na podlagi odobritev profilov

Št.	Profil	Zahteve glede zagotovil	Možnosti za neodvisno zagotovilo
1	**Obseg**: osebno, zaupno **Kraj obdelave:** pri Microsoftu ali stranki **Vloga pri obdelavi:** obdelovalec ali upravljavec **Razred podatkov:** zaupni **ali** strogo zaupni **Plačilne kartice:** ni relevantno **SaaS:** ni relevantno **Uporaba podizvajalcev:** ni relevantno **Gostovanje spletnega mesta:** ni relevantno	Samopotrditev skladnosti z ZVP	
2	**Obseg:** zaupno **Kraj obdelave:** pri dobavitelju **Vloga pri obdelavi:** obdelovalec **Razred podatkov:** zaupni **Plačilne kartice:** ni relevantno **SaaS:** ni relevantno **Uporaba podizvajalcev:** ni relevantno **Gostovanje spletnega mesta:** ni relevantno	Samopotrditev skladnosti z ZVP	
3	**Obseg**: zaupno **Kraj obdelave:** pri dobavitelju **Vloga pri obdelavi:** obdelovalec **Razred podatkov:** zelo zaupni **Plačilne kartice:** ni relevantno **SaaS:** ni relevantno **Uporaba podizvajalcev:** ni relevantno **Gostovanje spletnega mesta:** ni relevantno	Samopotrditev skladnosti z ZVP **in** neodvisno zagotovilo o skladnosti	Možnosti za neodvisno zagotovilo: 1. izvedba neodvisnega ocenjevanja skladnosti z ZVP **ali** 2. oddaja ISO 27001 **ali** 3. oddaja SOC 2 z merili zaupanja glede varnosti (ta možnost ne bo več na voljo po decembru 2021)

Št.	Profil	Zahteve glede zagotovil	Možnosti za neodvisno zagotovilo
4	**Obseg:** osebno, zaupno **Kraj obdelave:** pri dobavitelju **Vloga pri obdelavi:** obdelovalec **Razred podatkov:** zelo zaupni **Plačilne kartice:** ni relevantno **SaaS:** ni relevantno **Uporaba podizvajalcev:** ni relevantno **Gostovanje spletnega mesta:** ni relevantno	Samopotrditev skladnosti z ZVP **in** neodvisno zagotovilo o skladnosti	Možnosti za neodvisno zagotovilo: 1. izvedba neodvisnega ocenjevanja skladnosti z ZVP **ali** 2. oddaja ISO 27701 **in** ISO 27001
5	**Obseg:** osebno, zaupno **Kraj obdelave:** pri dobavitelju **Vloga pri obdelavi:** obdelovalec **Razred podatkov:** zaupni **Plačilne kartice:** ni relevantno **SaaS:** ni relevantno **Uporaba podizvajalcev:** ni relevantno **Gostovanje spletnega mesta:** ni relevantno	Samopotrditev skladnosti z ZVP	
6	**Obseg:** osebno, zaupno **Kraj obdelave:** pri dobavitelju **Vloga pri obdelavi:** upravljavec **Razred podatkov:** zelo zaupni ali zaupni **Plačilne kartice:** ni relevantno **SaaS:** ni relevantno **Uporaba podizvajalcev:** ni relevantno **Gostovanje spletnega mesta:** ni relevantno	Samopotrditev skladnosti z ZVP	

Št.	Profil	Zahteve glede zagotovil	Možnosti za neodvisno zagotovilo
Učinek dodajanja storitev SaaS, podizvajalcev, spletnega gostovanja			
7	**Obseg:** osebno, zaupno **Kraj obdelave:** pri dobavitelju **Vloga pri obdelavi:** obdelovalec **Razred podatkov:** zelo zaupni ali zaupni **Plačilne kartice:** ni relevantno **Podizvajalci:** DA ali **SaaS:** DA ali **Gostovanje spletnega mesta:** DA	Samopotrditev skladnosti z ZVP **in** neodvisno zagotovilo o skladnosti	Možnosti za neodvisno zagotovilo: 1. izvedba neodvisnega ocenjevanja skladnosti z ZVP **ali** 2. oddaja ISO 27701 **in** ISO 27001
8	**Obseg:** osebno, zaupno **Kraj obdelave:** pri dobavitelju **Vloga pri obdelavi:** upravljavec **Razred podatkov:** zelo zaupni **ali** zaupni **Plačilne kartice:** ni relevantno **Podizvajalci:** DA ali **SaaS:** DA ali **Gostovanje spletnega mesta:** DA	Samopotrditev skladnosti z ZVP	
Dodatna zagotovila za plačilne kartice in SaaS			
9	Kateri koli od zgornjih profilov in **plačilne kartice**	Upoštevne zgornje zahteve **in** zagotovilo PCI	Predložitev potrdil o skladnosti s standardi PCI DSS
10	Kateri koli od zgornjih profilov in **programska oprema kot storitev (Software as a Service oz. SaaS)**	Upoštevne zgornje zahteve **in** predložiti morate pogodbeno zahtevano potrdilo za ISO 27001 za funkcionalne storitve.	Oddati potrdilo za ISO 27001 s funkcionalnim kritjem storitev, ki se zagotavljajo.