

Microsoftova nabava

Vodič za program Sigurnost dobavljača i osiguranje privatnosti (SSPA)

Verzija 7

studeni 2020.

Uvod

Mi u Microsoftu smatramo da je privatnost temeljno pravo. U našoj misiji da osnažimo svakog pojedinca i organizaciju na planeti da postignu više, cilj nam je svakodnevno zaslužiti i zadržati povjerenje naših korisnika.

Snažne prakse glede privatnosti i sigurnosti ključne su za našu misiju, esencijalne za povjerenje korisnika, a u nekim jurisdikcijama i obavezne prema zakonu. Standardi izloženi u Microsoftovim pravilima o privatnosti i sigurnosti odražavaju naše vrijednosti kao tvrtke i oni se protežu do naših dobavljača (poput vaše tvrtke) koji obrađuju Microsoftove podatke u naše ime.

Program Sigurnost dobavljača i osiguranje privatnosti („**SSPA**“) jest Microsoftov korporacijski program za isporuku Microsoftovih osnovnih uputa za obradu podataka našim dobavljačima, u obliku Microsoftovih zahtjeva za zaštitu podataka dobavljača („**DPR**“), a koji su dostupni na [SSPA on Microsoft.com/Procurement](https://SSPA.onmicrosoft.com/Procurement). Imajte na umu da će dobavljači možda morati ispuniti dodatne zahtjeve na razini organizacije o kojima se odlučuje i koji se objavljuju izvan SSPA-a od strane Microsoftove grupe odgovorne za suradnju s dobavljačem.

Ključni SSPA izrazi definirani su u [DPR-u](#). Da biste saznali više o programu, pročitajte naša [Često postavljana pitanja](#) i kontaktirajte naš globalni tim tako da im pošaljete poruku na SSPAHelp@microsoft.com.

Pregled programa SSPA

SSPA je partnerstvo između Microsoftove nabave, korporacijskih vanjskih i pravnih poslova te korporacijske sigurnosti kako bi se osiguralo poštivanje principa privatnosti i sigurnosti od strane naših dobavljača.

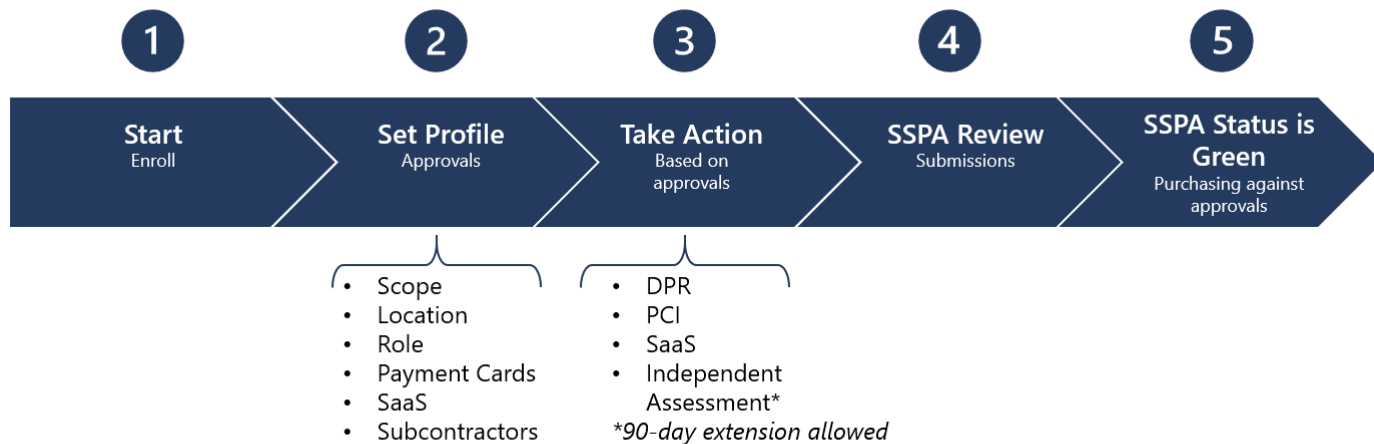
Opseg SSPA pokriva globalno sve dobavljače koji obrađuje osobne podatke ili Microsoftove povjerljive podatke u vezi s izvedbom tog dobavljača (npr. davanje usluga, softverske licence, usluge oblaka) prema odredbama svojeg ugovora s tvrtkom Microsoft (npr. uvjeti narudžbenice, glavni ugovor) („**Izvesti**“, „**Izvođenje**“ ili „**Izvedba**“).

SSPA dobavljaču omogućava odabir profila obrade podataka koji je usklađen s proizvodima i/ili uslugama za koje ste sklopili ugovor da ćete ih obaviti. Ti odabiri aktivirat će odgovarajuće zahtjeve da bi Microsoftu pružili osiguranje usklađenosti.

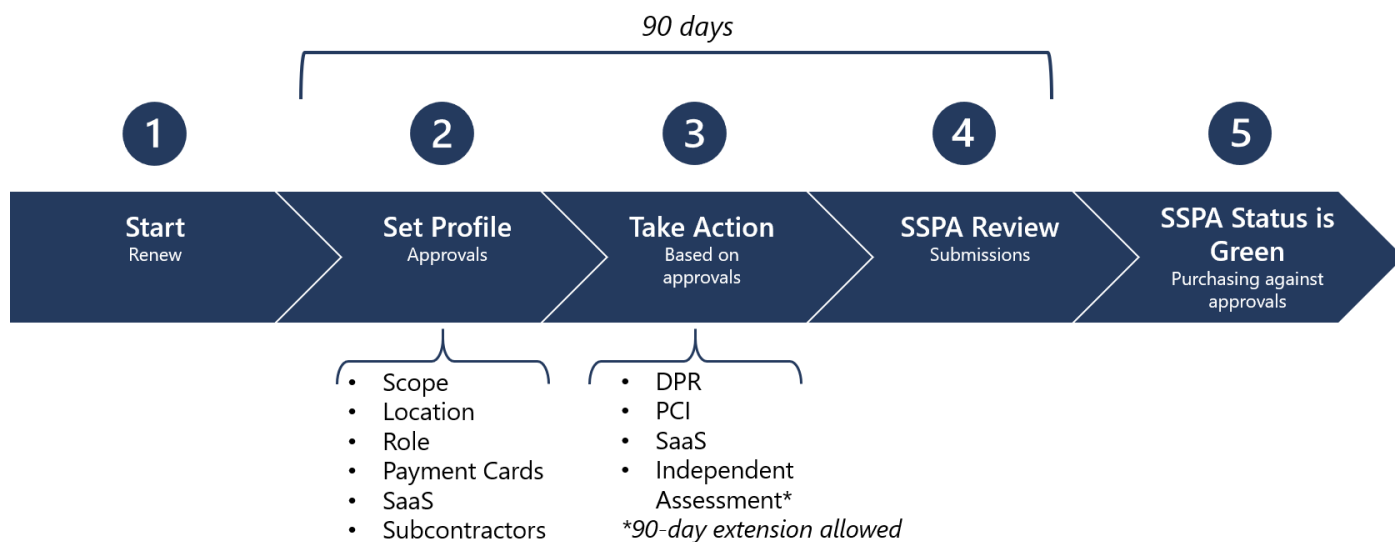
Svi prijavljeni dobavljači svake godine napraviti će samotestiranje usklađenosti s DPR-om. Vaš profil obrade podataka određuje hoće li biti izdan puni DPR ili se primjenjuje podskup zahtjeva. Dobavljači koji obrađuju podatke koje Microsoft smatra podacima višeg rizika također moraju udovoljiti dodatnim zahtjevima, kao što je pružiti neovisnu potvrdu usklađenosti.

Važno: aktivnosti usklađenosti utvrđuju SSPA status zelene boje (usklađen) ili crvene boje (neusklađen). Microsoftovi alati za kupnju potvrđuju je li SSPA status zelene boje (za svakog dobavljača u opsegu SSPA) prije nego što dopusti daljnje sudjelovanje.

Dijagram procesa programa SSPA - Novi dobavljač Pristupnica



Dijagram procesa programa SSPA - godišnja obnova dobavljača



Opseg programa SSPA

Pogledajte popis primjera u tablici u nastavku kako biste odredili obrađujete li vi (dobavljač) osobne podatke i/ili Microsoftove povjerljive podatke. Uzmite na znanje da su to samo primjeri, a ne cjelovit popis.

Napomena: vlasnik tvrtke koja posluje s Microsoftom može tražiti prijavu koja nije na ovom popisu u vezi s povjerljivom prirodom obrađenih podataka.

Osobni podaci prema vrsti podataka

Primjeri uključuju, ali bez ograničenja na sljedeće:

Osjetljivi podaci
Podaci u vezi djece
Genetički podaci, biometrijski podaci ili zdravstveni podaci
Rasno ili etničko podrijetlo
Politička, vjerska ili filozofska stajališta, mišljenja ili udruženja
Članstvo u sindikatima
Seksualni život ili seksualno opredjeljenje osobe
Imigracijski status (viza, radna dozvola itd.)
Službeni dokumenti (putovnica, vozačka dozvola, viza, OIB, JMBG)
Precizni podaci o lokaciji korisnika (unutar 300 metara)
Podaci o korisničkom sadržaju
Dokumenti, fotografije, videozapisi, glazba itd.
Recenzije i/ili ocjene unesene za proizvod ili uslugu
Odgovori u anketama
Povijest pregledavanja, interesi i favoriti
Pisanje, tipkanje i govorenje (glas/zvuk i/ili čavrljanje/bot za razgovor)
Podaci o vjerodajnicama (lozinke, podsjetnici za lozinke, korisničko ime, biometrijski podaci korišteni za identifikaciju)
Korisnički podaci povezani sa slučajem podrške

Snimljeni i generirani podaci
Neprecizni podaci o lokaciji
IP adresa
Preference i personalizacija uređaja
Upotreba usluga na web-mjestima, praćenje klikova na web-mjestima
Podaci s društvenih medija, odnosi društvenih grafikona
Podaci aktivnosti povezanih uređaja, kao što su monitori za fitnes
Kontaktne podaci, kao što su ime, adresa, broj telefona, e-adresa, datum rođenja, uzdržavane osobe i hitni kontakti
Procjena za prijevaru i rizik, pozadinska provjera
Pojedinosti o osiguranju, mirovini i olakšicama
Životopisi kandidata, bilješke s razgovora/povratne informacije
Podaci o računu
Podaci o instrumentima plaćanja
Broj kreditne kartice i datum isteka
Podaci o bankovnom usmjeravanju
Broj bankovnog računa
Kreditni zahtjevi ili iznosi kredita
Dokumenti o porezu i identifikatori
Podaci o investicijama ili troškovima
Korporacijske kartice
Pseudoanonimni podaci krajnjeg korisnika (EUPI) (identifikatori koje je izradio Microsoft kako bi prepoznao korisnike Microsoftovih proizvoda i usluga)
Globalno jedinstveni identifikator (GUID)
Korisnički ID putovnice ili jedinstveni identifikator (PUID)
Informacije o krajnjem korisniku koje se mogu prepoznati, a koje su kontrolni identifikacijski broj (EUII)
ID-jevi sesija
ID-jevi uređaja
Dijagnostički podaci
Podaci zapisnika

Microsoftovi povjerljivi podaci prema klasi podataka

Primjeri uključuju, ali bez ograničenja na sljedeće:

Strogo povjerljivo
Informacije u vezi ili povezane s razvojem, testiranjem ili proizvodnjom Microsoftovih proizvoda ili komponenti Microsoftovih proizvoda <i>Microsoftov softver, mrežne usluge, usluge ili hardver koji se komercijalno prodaje u bilo kojim kanalima naziva se „Microsoftov proizvod“</i>
Unaprijed objavljene marketinške informacije o Microsoftovom uređaju
Nenajavljeni Microsoftovi korporacijski financijski podaci podliježu pravilima programa SEC
Povjerljivo
Microsoftovi licencni ključevi proizvoda u ime Microsofta za distribuciju bilo kojom metodom
Informacije u vezi ili povezane s razvojem ili testiranjem Microsoftovih internih poslovnih aplikacija (LOB)
Microsoftov unaprijed objavljeni marketinški materijali za Microsoftov softver i usluge, kao što su Office, SQL, Azure itd.
Pisana, dizajnirana, elektronička ili pisana dokumentacija za sve Microsoftove usluge proizvode, kao što su uređaji (vodiči za postupak ili proceduru, konfiguracijski podaci itd.)

Važno: vlasnik tvrtke koja posluje s Microsoftom može zahtijevati sudjelovanje za podatke koji nisu uključeni u ovaj popis.

Profil za obradu podataka

Dobavljači Microsofta imaju punu kontrolu nad svojim profilom za obradu podataka SSPA.

To dobavljačima omogućava da odluče za koje dužnosti žele ispunjavati uvjete za obavljanje. Vodite računa o odabirima i razmotrite aktivnosti usklađenosti koje treba dovršiti kako biste postigli odobrenje. **Pogledajte odjeljak „Zahtjevi za osiguranje“ u nastavku i Dodatak A.**

Microsoftove poslovne grupe moći će se angažirati s dobavljačima čije aktivnosti obrade podataka odgovaraju odobrenjima koje je pribavio dobavljač.

Dobavljači će moći ažurirati svoj profil obrade podataka u bilo kojem trenutku tijekom godine **ako nema otvorenih zadataka**. Kada se napravi promjena, bit će izdana odgovarajuća aktivnost i potrebno ju je dovršiti prije nego se pribave odobrenja. Postojeća, dovršena odobrenja primjenjivat će se samo dok se ne dovrše novoizdani zahtjevi.

Ako novoizvršeni zadaci nisu dovršeni unutar dopuštenog roka od 90 dana, SSPA status promijenit će se u CRVENO, a postojat će rizik da će račun biti deaktiviran unutar sustava Microsoftove naplate računa.

Upozorenje: ako počnete ažurirati profil prije godišnje obnove, no odlučite ne učiniti bilo kakve promjene, sustav će svejedno izvršiti odgovarajuće zahtjeve koje će opet trebati dovršiti.

Odobrenja za obradu podataka	
1	Opseg obrade podataka <ul style="list-style-type: none">▪ Povjerljivo▪ Osobno, povjerljivo
2	Lokacija obrade podataka <ul style="list-style-type: none">▪ U Microsoftu ili kod korisnika▪ Kod dobavljača
3	Uloga obrade podataka <ul style="list-style-type: none">▪ Nadzornik (neovisan ili zajednički)▪ Obrađivač (obrađivač ili podobrađivač)
4	Obrada platnih kartica <ul style="list-style-type: none">▪ Da▪ Nije primjenjivo
5	Softver kao usluga <ul style="list-style-type: none">▪ Da▪ Nije primjenjivo
6	Korištenje podizvođača <ul style="list-style-type: none">▪ Da▪ Nije primjenjivo

Razmatranja odobrenja

Opseg obrade podataka

Povjerljivo

Odaberite ovo odobrenje ako će dobavljačeva izvedba uključivati obradu samo Microsoftovih povjerljivih podataka. Pogledajte definicije u DPR-u.

Ako odaberete ovo odobrenje, nećete ispunjavati uvjete za dužnosti obrade osobnih podataka.

Osobno, povjerljivo

Odaberite ovo odobrenje ako će dobavljačeva izvedba uključivati obradu osobnih podataka i Microsoftovih povjerljivih podataka. Pogledajte definicije u DPR-u.

Lokacija obrade

U Microsoftu ili kod korisnika

Odaberite ovo odobrenje ako će dobavljačeva izvedba uključivati dobavljačevu obradu podataka unutar Microsoftovog mrežnog okruženja gdje osoblje koristi *@microsoft.com* vjerodajnice za pristup ili unutar okruženja Microsoftovog klijenta.

Nemojte odabrati ovu mogućnost u ovim okolnostima:

- Dobavljač upravlja Microsoftovim objektom u inozemstvu (OF).
- Dobavljač Microsoftu pruža resurse i povremeno rade na Microsoftovoj mreži. Lokacija obrade za rad izvan mreže smatra se radom „kod dobavljača“.

Kod dobavljača

Ako se ne primjenjuje uvjet „U Microsoftu ili kod korisnika“ (opisan iznad), odaberite ovu opciju.

Uloga obrade podataka

Nadzornik (obuhvaća neovisne ili zajedničke nadzornike)

Odaberite ovo odobrenje ako **svi** aspekti izvedbe dobavljača ispunjavaju definicije uloge obrade podataka nadzornika (pogledajte DPR).

Ako odaberete ovo odobrenje, nećete ispunjavati uvjete za obradu osobnih podataka s oznakom „obrađivača“. Ako je dobavljač i obrađivač i nadzornik za Microsoft, nemojte odabrati „Nadzornik“, već radije odaberite „Obrađivač“.

Obrađivač (uključuje obrađivače i podobrađivače)

To je najuobičajenija uloga obrade kada dobavljači obrađuju podatke za Microsoft. Pregledajte definicije obrađivača i podobrađivača u DPR-u.

Obrada platnih kartica

Odaberite ovo odobrenje ako bilo koji dio podataka koje obrađuje dobavljač uključuje podatke koji podržavaju obradu kreditne kartice ili druge platne kartice u ime tvrtke Microsoft.

Odobrenje dopušta dobavljaču da se angažira na dužnostima obrade platnih kartica.

Softver kao usluga (SaaS)

Odaberite ovo odobrenje ako izvedba dobavljača obuhvaća proviziju usluge Microsoftu pomoću tehnologije temeljene na internetu koja pokriva pristup i upotrebu poslužitelja, umrežavanje pohrane i podatkovne centre. Dobavljač obrađuje podatke izvan Microsoftovih prostorija ili okruženja. Primjeri usluge u oblaku uključuju softver kao uslugu („SaaS“), platformu kao uslugu („PaaS“) i infrastrukturu kao uslugu („IaaS“).

Microsoft definira „SaaS“ kao isporuku softverskih funkcija putem mehanizama temeljenih na internetu, na temelju uobičajenog koda koji se koristi na od jednog do više modela na temelju plaćanja po upotrebi ili kao pretplatu na temelju podataka o upotrebi.

Korištenje podizvođača

Odaberite ovo odobrenje ako dobavljač koristi podizvođače za izvedbu. Pogledajte definicije u DPR-u.

Zahtjevi za osiguranje

Zahtjevi na temelju Odobrenja profila

Odobrenja koja je odabrao dobavljač u svojem profilu za obradu podataka pomaže SSPA-u u procjeni razine rizika za Microsoftovu suradnju s dobavljačem iz perspektive obrade podataka. Zahtjevi za usklađenost dobavljača sa SSPA-om razlikuju se ovisno o dobavljačevim odobrenjima u profilima dobavljača. U ovom odjeljku objašnjeni su različiti zahtjevi za SSPA.

Postoje kombinacije koje mogu podići ili smanjiti zahtjeve za usklađenost. Kombinacije su snimljene u Dodatku A i to je ono što možete očekivati za izvršavanje s portala za usklađenost za dobavljače nakon što dovršite svoj profil. Uvijek možete provjeriti kako scenarij odgovara okviru tako da zatražite reviziju SSPA tima.

Radnja: pronađite svoj profil za odobrenje u Dodatku A i pregledajte odgovarajuće zahtjeve za osiguranje i opcije neovisnog osiguranja, ako je primjenivo.

Važno: ako u svom profilu odabirete softver kao uslugu (SaaS), podizvođače, hostiranje web-mjesta ili platne kartice, potrebno je dodatno osiguranje.

Samopotvrđivanje usklađenosti s DPR-om

Svi dobavljači u programu SSPA moraju dovršiti samopotvrđivanje usklađenosti s DPR-om u roku od 90 dana od primanja zahtjeva. Ovaj zahtjev bit će pružen na godišnjoj razini no to može biti češće ako se profil obrade podatak ažurira sredinom godine. Računi dobavljača promijenit će se u SSPA status CRVENO (neusklađeno) ako se premaši rok od 90 dana. Nove narudžbenice u opsegu ne mogu se obraditi sve dok SSPA status ne postane zelen (usklađeno).

Novoprijavljeni dobavljači mogu ispuniti zahtjeve, prema odabiru odobrenja, kako bi se osigurao SSPA status zeleno (usklađeno) prije nego počnu dužnosti.

Kao što je navedeno, profil obrade podataka određuje hoće li biti izdan puni DPR ili se primjenjuje podskup zahtjeva. Ta odobrenja mogu se promijeniti tijekom godine, no svaki put kada se napravi izmjena, potrebno je ispuniti povezane zahtjeve da bi promjena stupila na snagu.

Važno: tim programa SSPA nema ovlasti za odobravanje produljenja zadatka.

Ovlašteni predstavnik dovršit će samopotvrđivanje, što će osigurati da ima dovoljno informacija od stručnjaka za temu da bi odgovorio na svaki zahtjev sa sigurnošću. Dodatno, dodavanjem svog imena

obrascu programa SSPA potvrđuje da je pročitala i razumije DPR. Dobavljači uvijek mogu dodati druge kontakte mrežnom alatu za pomoć u ispunjavanju zahtjeva.

Ovlašteni predstavnik (pogledajte definiciju) mora sljedeće:

1. utvrditi koji se zahtjevi primjenjuju
2. poslati odgovor na svaki primjenjivi zahtjev
3. potpisati i poslati atestiranje na Microsoftovom portalu za usklađenost za dobavljače.

Primjenjivost

Od dobavljača se očekuje da odgovore na sve primjenjive zahtjeve za DPR izdane prema profilu obrade podataka. Očekuje se da se, u sklopu izdanih zahtjeva, nekolicina neće prijaviti za pružanje proizvoda i usluga Microsoftu. Njih se može označiti s „ne primjenjuje se” s detaljnim komentaram SSPA revizora za provjeru.

Podnesene zahtjeve za DPR pregledava SSPA tim za bilo koji odabir „ne primjenjuje se”, „lokalni pravni sukob” ili „ugovorni konflikt”. Ocjenjivači provjeravaju aktivnosti na ispunjavanju dužnosti vezane uz račun dobavljača da bi potvrdili odabir „ne primjenjuje se”. SSPA tim može zatražiti objašnjenje za jedan odabir ili više njih. Lokalni pravni i ugovorni sukobi prihvaćaju se samo ako se pružaju reference za potporu i konflikt je jasan.

Zahtjev za neovisnu procjenu

Pregledajte odjeljak Zahtjevi prema odobrenjima u Dodatku A da biste vidjeli odobrenja za obradu podataka koja pokreću ovaj zahtjev.

Dobavljači imaju opciju promijeniti odobrenja tako da ažuriraju profil obrade podataka.

Da biste osigurali odobrenja koja zahtijevaju neovisnu potvrdu usklađenosti, dobavljači će trebati odabrati neovisnog procjenitelja da bi potvrdio usklađenost s DPR-om. Procjenitelj će pripremiti pismo sa savjetom za pružanje jamstava usklađenosti Microsoftu. Pismo mora biti bezuvjetno i svi problemi neusklađenosti moraju biti riješeni i ispravljani prije slanja pisma potvrde Microsoftovom Portalu usklađenosti dobavljača za procjenu SSPA tima. Procjenitelji nas mogu kontaktirati radi odobrenog predloška pisma sa savjetom putem e-adrese SSPAHelp@Microsoft.com.

Dodatak A obuhvaća prihvatljive alternative certifikacije ako odaberete da ne koristite neovisnog procjenitelja za potvrdu usklađenosti s DPR-om (kad je primjenjivo, na primjer za dobavljače SaaS-a, dobavljače hostiranja web-mjesta ili dobavljače s podizvođačima). Oslanja se na ISO 27701 (privatnost) i ISO 27001 (sigurnost) za davanje bliskog mapiranja zahtjeva za zaštitu podataka (DPR).

Važno: SOC 2 izvješća (s pokrivenog sigurnošću) neće se prihvaćati nakon **prosinca 2021**.

SSPA može ručno izvršiti neovisnu procjenu ako okolnosti izvan standardnih okidača zahtijevaju dodatnu dubinsku analizu. To bi mogao biti zahtjev od privatnosti ili sigurnosti odjela; provjera ispravljanja podataka incidenta s podacima.; zahtjev za izvršenje prava automatiziranog subjekta podataka.

Smjernice o tome kako pristupiti ovom zahtjevu:

1. Angažman mora izvesti procjenitelj s dostatnom tehničkom obukom i znanjem o temi da bi mogao zadovoljavajuće pristupiti procjeni usklađenosti.
2. Procjenitelji moraju biti povezani s udruženjima International Federation of Accountants ([IFAC](#)) ili American Institute of Certified Public Accountants ([AICPA](#)) ili moraju imati certifikate od drugih relevantnih organizacija za privatnost i sigurnost, kao što su International Association of Privacy Professionals ([IAPP](#)) ili Information Systems Audit and Control Association ([ISACA](#)).
3. Procjenitelj mora koristiti najnoviji DPR koji obuhvaća potrebne dokaze za podržavanje svakog zahtjeva. **Dobavljači će procjenitelju trebati pružiti najnovije odgovore na potvrđivanje DPR-a.**
4. U slučaju novoprijavljenog dobavljača, procjenitelj će testirati dizajn kontrola procesa. U svim drugim slučajevima, procjenitelj će testirati učinkovitost kontrola.
5. Opseg angažmana procjene ograničen je na Microsoftove osobne podatke ili Microsoftove povjerljive podatke u vezi s izvedbom dobavljača.
6. Opseg dužnosti ograničen je na sve aktivnosti obrade podataka izvršene prema broju računa dobavljača koji je primio zahtjev. Ako se dobavljač odluči istovremeno koristiti više računa dobavljača, **pismo potvrde mora uključiti popis računa dobavljača uključenih u procjenu i povezane adrese.**
7. Pismo poslano SSPA-u ne smije uključivati izjave u kojima dobavljač ne može ispuniti navedene zahtjeve za zaštitu podataka. Te probleme potrebno je riješiti prije slanja pisma.

SSPA je napravio popis preferiranih [dostupnih](#) procjenitelja. Te tvrtke su upoznate s provođenjem procjena za SSPA. Dobavljači trebaju platiti ovu procjenu; troškovi će ovisiti o razini i opsegu obrade podataka.

PCI DSS zahtjev za certifikaciju

Standard sigurnosti podataka industrije platnih kartica (PCI DSS) jest okvir za razvoj robusnih podatkovnih sigurnosnih procesa za plaćanje karticama koji obuhvaća prevenciju, otkrivanje i odgovarajuće reakciju na sigurnosne incidente. Okvir je razvilo Vijeće za PCI sigurnosne standarde, samoregulatorna industrijska organizacija. Svrha zahtjeva standarda PCI DSS jest prepoznati ranjivosti tehnologije i procesa koje predstavljaju rizik za sigurnost podataka vlasnika kartice koji obrađuju.

Microsoft mora biti u skladu s tim standardima. Ako dobavljač rukuje podacima platnih kartica u ime Microsofta, tražit ćemo dokaz vašeg poštivanja ovih standarda. Obratite se [Vijeću za PCI sigurnosne standarde](#) da biste shvatili zahtjeve koje je postavila PCI organizacija.

Ovisno o količini obrađenih transakcija, dobavljač će morati imati certifikat usklađenosti kvalificiranog procjenitelja sigurnosti ili može ispuniti [obrazac](#) za samoprocjenu.

Brendovi platnih kartica postavljaju pragove za vrstu procjene, tipično;

- Razina 1: Pošaljite PCI DSS^{certifikat} treće strane
- Razina 2 ili 3: Pošaljite PCI DSS upitnik samoprocjene (SAQ) koji je potpisao djelatnik dobavljača.

Program SSPA prihvaća obje vrste procjene. Pošaljite certifikaciju koja se primjenjuje i ispunjava zahtjeve za PCI.

Zahtjevi za SaaS

Dobavljači koji nude softver kao uslugu Microsoftu moraju poslati valjanu ISO 27001 certifikaciju s funkcionalnom pokrivenošću softverske usluge kojom upravlja dobavljač.

Imajte na umu da SSPA ne očekuje certifikaciju podatkovnog centra treće strane kao ranije – mi očekujemo ISO 27001 certifikaciju softverskih usluga koje se nude Microsoftu i koje su zabilježene u vašem ugovoru s Microsoftom.

Korištenje podizvođača

Microsoft smatra korištenje podugovarača visokorizičnim faktorom.

DPR zahtijeva da dobavljači obavijesti Microsoft kada koriste treću stranu za obradu podataka u opsegu. To je moguće učiniti kroz SSPA.

Incidenti s podacima

Ako dobavljač uoči incident s privatnošću ili sigurnošću podataka, dobavljači moraju obavijestiti Microsoft kao što je navedeno u DPR-u. Pogledajte primjenjive definicije u Dodatku B.

Pošaljite e-poruku na SSPAHelp@microsoft.com koristeći se sljedećim predloškom: [Prijavite incident s podacima](#). Obavezno navedite:

- Datum incidenta s podacima:
- Naziv dobavljača:
- Broj dobavljača:
- Obaviješteni Microsoftov kontakt:
- Povezana narudžbenica, ako je dostupna:
- Sažetak incidenta s podacima:

Dodatak A

Zahtjevi na temelju Odobrenja profila

#	Profil	Zahtjevi za osiguranje	Opcije neovisnog osiguranja
1	<p>Opseg: osobno, povjerljivo</p> <p>Lokacija obrade: u Microsoftu ili kod korisnika</p> <p>Uloga obrade: obrađivač ili nadzornik</p> <p>Klasa podataka: strogo povjerljivo ili povjerljivo</p> <p>Platne kartice: nije primjenjivo</p> <p>SaaS: nije primjenjivo</p> <p>Korištenje podizvođača: nije primjenjivo</p> <p>Hostiranje web-mjesta: nije primjenjivo</p>	Samopotvrđivanje usklađenosti s DPR-om	
2	<p>Opseg: povjerljivo</p> <p>Lokacija obrade: kod dobavljača</p> <p>Uloga obrade: obrađivač</p> <p>Klasa podataka: povjerljivo</p> <p>Platne kartice: nije primjenjivo</p> <p>SaaS: nije primjenjivo</p> <p>Korištenje podizvođača: nije primjenjivo</p> <p>Hostiranje web-mjesta: nije primjenjivo</p>	Samopotvrđivanje usklađenosti s DPR-om	
3	<p>Opseg: povjerljivo</p> <p>Lokacija obrade: kod dobavljača</p> <p>Uloga obrade: obrađivač</p> <p>Klasa podataka: strogo povjerljivo</p> <p>Platne kartice: nije primjenjivo</p> <p>SaaS: nije primjenjivo</p> <p>Korištenje podizvođača: nije primjenjivo</p> <p>Hostiranje web-mjesta: nije primjenjivo</p>	Samopotvrđivanje usklađenosti s DPR-om i Neovisno osiguranje usklađenosti	Opcije neovisnog osiguranja: <ol style="list-style-type: none">1. Dovođite neovisnu procjenu sukladno DPR-u ili2. pošaljite ISO 27001 ili3. pošaljite SOC2 Kriterij za povjerljivu sigurnost (prestaje s radom u prosincu 2021.)

#	Profil	Zahtjevi za osiguranje	Opcije neovisnog osiguranja
4	<p>Opseg: osobno, povjerljivo</p> <p>Lokacija obrade: kod dobavljača</p> <p>Uloga obrade: obrađivač</p> <p>Klasa podataka: Highly Confidential</p> <p>Platne kartice: nije primjenjivo</p> <p>SaaS: nije primjenjivo</p> <p>Korištenje podizvođača: nije primjenjivo</p> <p>Hostiranje web-mjesta: nije primjenjivo</p>	<p>Samopotvrđivanje usklađenosti s DPR-om</p> <p>i</p> <p>Neovisno osiguranje usklađenosti</p>	<p>Opcije neovisnog osiguranja:</p> <ol style="list-style-type: none"> 1. Dopržite neovisnu procjenu sukladno DPR-u ili 2. pošaljite ISO 27701 i ISO 27001
5	<p>Opseg: osobno, povjerljivo</p> <p>Lokacija obrade: kod dobavljača</p> <p>Uloga obrade: obrađivač</p> <p>Klasa podataka: povjerljivo</p> <p>Platne kartice: nije primjenjivo</p> <p>SaaS: nije primjenjivo</p> <p>Korištenje podizvođača: nije primjenjivo</p> <p>Hostiranje web-mjesta: nije primjenjivo</p>	<p>Samopotvrđivanje usklađenosti s DPR-om</p>	
6	<p>Opseg: osobno, povjerljivo</p> <p>Lokacija obrade: kod dobavljača</p> <p>Uloga obrade: nadzornik</p> <p>Klasa podataka: strogo povjerljivo ili povjerljivo</p> <p>Platne kartice: nije primjenjivo</p> <p>SaaS: nije primjenjivo</p> <p>Korištenje podizvođača: nije primjenjivo</p> <p>Hostiranje web-mjesta: nije primjenjivo</p>	<p>Samopotvrđivanje usklađenosti s DPR-om</p>	

#	Profil	Zahtjevi za osiguranje	Opcije neovisnog osiguranja
Učinak dodavanja SaaS-a, podizvođača, hostiranja web-mjesta			
7	<p>Opseg: osobno, povjerljivo</p> <p>Lokacija obrade: kod dobavljača</p> <p>Uloga obrade: obrađivač</p> <p>Klasa podataka: strogo povjerljivo ili povjerljivo</p> <p>Platne kartice: nije primjenjivo</p> <p>Podizvođači: DA ili</p> <p>SaaS: DA ili</p> <p>Hostiranje web-mjesta: DA</p>	<p>Samopotvrđivanje usklađenosti s DPR-om</p> <p>i</p> <p>Neovisno osiguranje usklađenosti</p>	<p>Opcije neovisnog osiguranja:</p> <ol style="list-style-type: none"> 1. Dopršite neovisnu procjenu sukladno DPR-u ili 2. pošaljite ISO 27701 i ISO 27001
8	<p>Opseg: osobno, povjerljivo</p> <p>Lokacija obrade: kod dobavljača</p> <p>Uloga obrade: nadzornik</p> <p>Klasa podataka: strogo povjerljivo ili povjerljivo</p> <p>Platne kartice: nije primjenjivo</p> <p>Podizvođači: DA ili</p> <p>SaaS: DA ili</p> <p>Hostiranje web-mjesta: DA</p>	<p>Samopotvrđivanje usklađenosti s DPR-om</p>	

#	Profil	Zahtjevi za osiguranje	Opcije neovisnog osiguranja
Dodatno osiguranje za platne kartice i SaaS			
9	Bilo koji od profila iznad i platne kartice	Prethodni zahtjevi koji se primjenjuju i osiguranje industrije platnih kartica	Pošaljite PCI DSS certifikaciju
10	Bilo koji od profila iznad i Softver kao usluga (SaaS)	Gore navedeni zahtjevi koji se primjenjuju i šalju vašu ugovorno obaveznu ISO 27001 certifikaciju pokrivaju funkcionalne usluge.	Pošaljite ISO 27001 certifikaciju s funkcionalnom pokrivenošću pruženih usluga.