

Набавка корпорације Microsoft

Водич за програм уверења о безбедности и приватности добављача (Supplier Security & Privacy Assurance, SSPA)

Верзија 8

јуни 2022.

Увод

У корпорацији Microsoft, верујемо да приватност спада у основна права. У оквиру наше мисије да сваком појединцу и организацији на планети омогућимо да постиже више, свакодневно се трудимо да задобијемо и задржимо поверење својих клијената.

Стриктне праксе приватности и безбедности пресудне су за нашу мисију, суштински важне за поверење које нам клијенти указују и, у неколико јурисдикција, прописане законом. Стандарди садржани у смерницама о приватности и безбедности корпорације Microsoft одражавају наше вредности као компаније, те важе и за наше добављаче (као што је ваша компанија) који Обрађују Microsoft податке у наше име.

Програм уверења о безбедности и приватности добављача (Supplier Security and Privacy Assurance Program, **SSPA**) представља корпоративни програм корпорације Microsoft помоћу којег се основна упутства о обради података корпорације Microsoft преносе нашим добављачима, у облику Захтева за заштиту података добављача (Data Protection Requirements, **DPР**), доступних у одељку [SSPA на сајту Microsoft.com/Procurement](https://www.microsoft.com/Procurement). Имајте на уму да ће добављачи можда морати да испуне додатне захтеве на нивоу организације о којима, ван SSPA, одлучује и које саопштава Microsoft група одговорна за ангажовања са добављачима.

Кључни појмови програма SSPA дефинисани су у документу [DPР](#). Да бисте сазнали више о програму, прочитајте наша [Често постављана питања](#) и обратите се нашем глобалном тиму путем адресе SSPAHelp@microsoft.com.

Преглед програма SSPA

SSPA је партнерство између одељења Microsoft набавке, Корпоративних, спољних и правних послова и Корпоративне безбедности, којим се осигурава да наши добављачи поштују принципе приватности и безбедности.

Опсег програма SSPA односи се на све добављаче широм света који обрађују Личне податке и/или Microsoft Поверљиве податке у вези с извршењем посла тог добављача (нпр. пружањем услуга, лиценцама за софтвер, услугама у облаку) на основу услова свог уговора са корпорацијом Microsoft (нпр. услови поруџбенице, главног уговора) („**Извршити**,” „**Извршава**,” или „**Извршење посла**“).

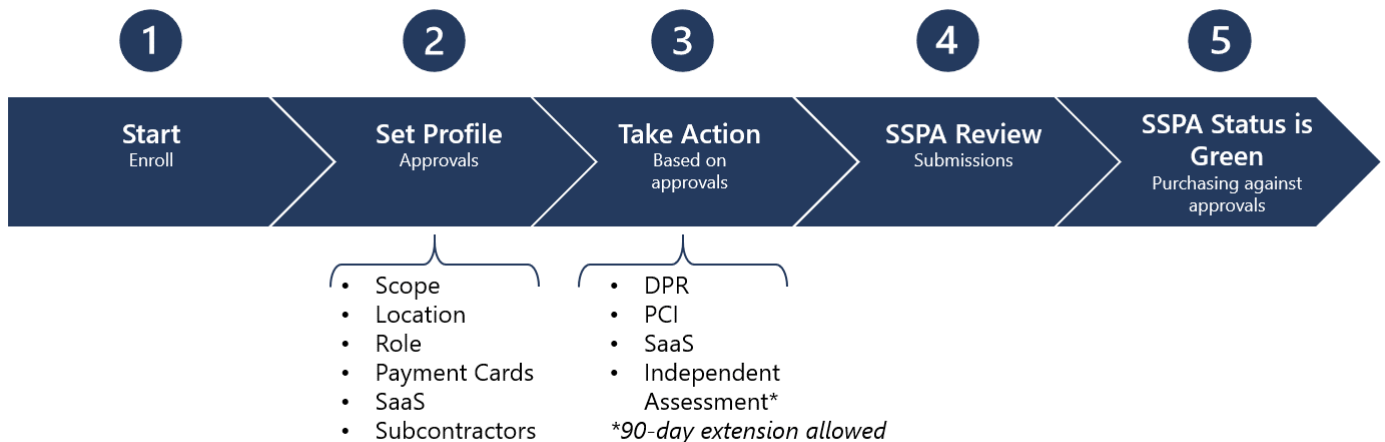
SSPA омогућава добављачу да на профилу обраде података изабере опције које су у складу са робом и/или услугама које, на основу уговора, извршавате. Ове опције подразумевају испуњавање одговарајућих захтева како бисте корпорацији Microsoft гарантовали усаглашеност.

Сви регистровани добављачи морају на годишњем нивоу да спроведу самостално атестирање усаглашености са програмом DPР. На основу вашег профила обраде података одређује се да ли се издаје комплетан DPР или се примењује само подскуп захтева. Добављачи који обрађују податке које Microsoft сматра подацима вишег ризика можда ће морати да испуне

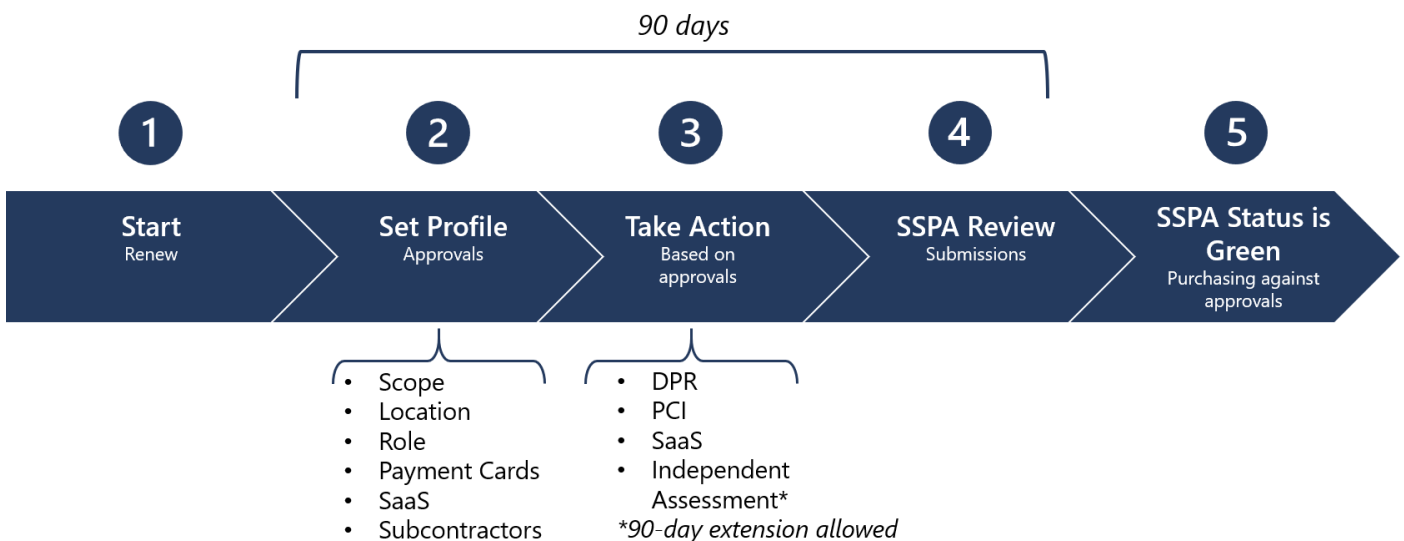
и додатне захтеве, као што је достављање независне верификације усаглашености. Од добављача који се налазе на списку објављених Мицрософтових подобрађивача (Subprocessor) такође ће се захтевати да доставе независну верификацију усаглашености.

Важно: На основу активности везаних за усаглашеност одређује се да ли ће SSPA статус бити зелен (усаглашено) или црвен (неусаглашено). Microsoft алатке за куповину потврђују да је SSPA статус зелен (за сваког добављача за којег важи SSPA) пре него што се дозволи да ангажман пређе у следећу фазу.

Дијаграм SSPA процеса – Регистрација новог добављача



Дијаграм SSPA процеса – Годишња обнова статуса добављача



Опсег програма SSPA

Да бисте утврдили да ли ви (добављач) Обрађујете личне податке и/или Microsoft поверљиве податке, погледајте листу примера у табелама у наставку. Имајте на уму да су ово примери, а не комплетна листа.

Напомена: Власник Microsoft предузећа може да затражи регистрацију која није обухваћена овом листом услед поверљиве природе података који се обрађују.

Лични подаци по типу података

Примери укључују, али нису ограничени на:

Осетљиви подаци
Подаци везани за децу
Генетски, биометријски или медицински подаци
Расно или етничко порекло
Политичка, религијска или филозофска убеђења, мишљења или припадност
Чланство у радничким синдикатима
Сексуални живот или сексуална оријентација физичког лица
Имиграциони статус (виза, дозвола за рад итд.)
Званична средства за идентификацију (пасош, возачка дозвола, виза, бројеви социјалног осигурања, матични бројеви)
Подаци о прецизној локацији корисника (у кругу од 300 метара)
Број личних банковних рачуна
Број и датум истека кредитних картица
Подаци о садржају корисника
Документи, фотографије, видео записи, музика итд.
Рецензије и/или оцене унете у оквиру производа или услуге
Одговори на анкете
Историја прегледања, интересовања и омиљени садржаји
Писање пером, куцање и изговорени текст (глас/звук и/или ћаскање/робот)
Подаци о акредитивима (лозинке, подсећања о лозинкама, корисничко име, биометријски подаци који се користе за идентификацију)
Подаци о кориснику повезани са предметом за тражење подршке

Снимљени и генерисани подаци
Непрецизни подаци о локацији
IP адреса
Жељене опције и персонализација уређаја
Употреба услуга за веб сајтове, праћење кликова на веб страницама
Подаци о друштвеним медијима, односи на друштвеним графиконима
Подаци о активностима са повезаних уређаја као што су уређаји за праћење фитнес активности
Контакт подаци као што су име, адреса, број телефона, адреса е-поште, датум рођења, контакти за издржавана лица и контакти за хитне случајеве
Процена могућности преваре и ризика, провера прошлости
Детаљи о осигурању, пензији и бенефицијама
Радне биографије кандидата, белешке/повратне информације са интервјуа
Metadata and telemetry
Подаци о налогу
Подаци о платним средствима
Број и датум истека кредитних картица
Информације за рутирање банке
Број банковног рачуна
Захтеви за кредит или кредитна линија
Порески документи и идентификатори
Подаци о инвестицијама и трошковима
Корпоративне картице
Псеудонимизоване информације о крајњим корисницима (EUPI) (Идентификатори које је креирао Microsoft за идентификацију корисника Microsoft производа и услуга)
Глобално јединствени идентификатор (GUID)
ИД корисника пасоша или јединствени идентификатор (PUID)
Хеширане информације за идентификацију крајњих корисника (EUII)
ID-ови сесија
ID-ови уређаја
Дијагностички подаци
Подаци о евиденцијама

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 поверљиви подаци по класи података

Примери укључују, али нису ограничени на:

Изузетно поверљиво
Информације које се тичу развоја, тестирања или производње Microsoft производа или компоненти Microsoft производа, или које се односе на њих <i>Microsoft софтвер, услуге на мрежи, услуге или хардвер који се комерцијално продају путем било ког канала сматрају се "Microsoft производом"</i>
Маркетиншке информације о прелиминарним верзијама Microsoft уређаја
Необјављени Microsoft корпоративни финансијски подаци који подлежу SEC правилима
Поверљиво
Лиценцни кључеви Microsoft производа у име корпорације Microsoft који се дистрибуирају на било који начин
Информације које се тичу развоја или тестирања интерних Microsoft апликација за област пословања (Line of Business, LOB) или које су везане за њих
Microsoft прелиминарни маркетиншки материјал за Microsoft софтвер и услуге као што су Office, SQL, Azure итд.
Писана, дизајнерска, електронска или штампана документација за Microsoft услуге или производе, као што су уређаји (водичи за процесе или процедуре, конфигурациони подаци итд.)

Важно: Власник Microsoft предузећа може да тражи укључивање података који нису наведени на овој листи.

Профил обраде података

Microsoft добављачи имају пуну контролу над својим SSPA профилем обраде података.

Ово добављачима омогућава да се одлуче за ангажмане за чије ће се извршавање квалификовати. Добро обратите пажњу приликом избора и размотрите

активности везане за усаглашеност које морате да обавите како бисте добили одобрење.

Погледајте одељак “Захтеви за пружање уверења ” у наставку као и Додатак А.

Microsoft пословне групе моћи ће да склапају ангажмане са добављачима само када се активности обраде података подударају са одобрењима која је добављач добио.

Добављачи могу да ажурирају профил обраде података било када током године **ако немају отворених задатака**. Када се унесе промена, издаје се одговарајућа активност, која се мора довршити пре добијања одобрења. Постојећа, завршена одобрења важе док се не испуне новоиздати захтеви.

Уколико се новоизвршени задаци не доврше у року од дозвољених 90 дана SSPA статус поново постаје црвен (неусаглашено) и постоји ризик да Microsoft систем дуговања деактивира налог.

Одобрења за обраду података

1	Опсег обраде података <ul style="list-style-type: none">ПоверљивоЛични, поверљиви
2	Локација обраде података <ul style="list-style-type: none">У корпорацији Microsoft или код КлијентаКод Добављача
3	Улога у обради података <ul style="list-style-type: none">Контролор (Независни или Заједнички контролор)ОбрађивачПодобрађивач (Одређује корпорација Microsoft)
4	Обрада платних картица <ul style="list-style-type: none">ДаНије примењиво
5	Софтвер као услуга <ul style="list-style-type: none">ДаНије примењиво
6	Ангажовање Подизвођача <ul style="list-style-type: none">ДаНије примењиво

Разматрања о одобрењу

Опсег обраде података

Поверљиво

Изаберите ово одобрење ако Извршење посла добављача обухвата Обраду искључиво Microsoft поверљивих података.

Ако изаберете ово одобрење, не испуњавајте услове за ангажмане обраде Личних података.

Лични, Поверљиви

Изаберите ово одобрење ако Извршење посла добављача обухвата Обраду Личних података и Microsoft поверљивих података.

Локација обраде

У корпорацији Microsoft или код Клијента

Изаберите ово одобрење ако Извршење посла добављача подразумева да ће добављач Обрађивати податке у мрежном окружењу корпорације Microsoft где особље користи @microsoft.com акредитиве за приступ или у окружењу клијента корпорације Microsoft.

Немојте бирати ову опцију у следећим околностима:

- Добављач управља офшор објектом (OF) који је одредио Microsoft.
- Добављач обезбеђује ресурсе корпорацији Microsoft и повремено ради на Microsoft мрежи и ван ње. Локација обраде за извршење посла сматра се локацијом “код добављача.”

Код Добављача

Изаберите ову опцију ако услов “У корпорацији Microsoft или код Клијента” (као што је описано изнад) не важи.

Улога у обради података

Контролор (обухвата независне и заједничке контролоре)

Изаберите ово одобрење ако **сви** аспекти Извршења посла добављача одговарају дефиницији улоге Контролора у обради података (погледајте DPR).

Ако изаберете ово одобрење, не испуњавате услове за обраду Личних података на основу улоге ‘Обрађивач’. Ако је добављач истовремено и Обрађивач и Контролор за Microsoft, не бирајте ‘Контролор’ већ изаберите Процесор.

Обрађивач

Ово је најчешћа улога у обради коју имају добављачи када обрађују податке у име корпорације Microsoft. Прегледајте дефиницију Обрађивача у документу DPR.

Подобрађивач

Подобрађивач је трећа страна коју Microsoft ангажује за Извршавање, при чему Извршавање посла укључује Образу Microsoft Личних података за које је Microsoft Обрађивач. Добављачи се не могу сами идентификовати као Подобрађивачи јер је за то потребно претходно одобрење интерних тимова за приватност. Добављачи могу бити Подобрађивачи само када је Microsoft Обрађивач података а добављач обрађује квалификоване типове Личних података предузећа. Подобрађивачи ће морати да испуне додатне захтеве за уговор и усаглашеност, укључујући Додатак о заштити података и Независну процену (погледајте у наставку).

Обрада платних картица

Изаберите ово одобрење ако било који део података које добављач Обрађује обухвата податке

потребне за обраду кредитних или других платних картица у име корпорације Microsoft. Ово одобрење добављачу омогућава да учествује у ангажманима обраде платних картица.

Софтвер

Одељење Набавке корпорације Microsoft усмерава Купце кроз процес пријема за све куповине софтвера, што укључује различите провере укључујући SSPA тријажу да би се одлучило да ли је добављач који испоручује софтвер у оквиру за управљање SSPA. (Microsoft Купци могу погледати кораке наведене на интерној страници [НабавкаВеб Софтвера и Услуге у облаку](#) за више детаља). Ако је потребан SSPA, добављачи ће можда морати да идентификују да се примењује опција профила 'Софтвер као услуга' (Software as a Service, SaaS). За добављаче регистроване као SSPA, ово се може урадити приликом попуњавања профила за обраду података на Microsoft порталу за усаглашеност добављача.

У сврху усаглашености са SSPA, SaaS посматрајте широко како бисте такође укључили платформу као услугу (PaaS), и инфраструктуру као услугу (IaaS). (Да бисте сазнали више о SaaS, погледајте ово [објашњење](#).)

Софтвер као услуга (SaaS)

Софтвер као услуга (Software as a Service, SaaS) омогућава корисницима да се повежу и користе апликације на бази облака преко Интернета.

Microsoft дефинише **Софтвер као услугу (SaaS)** као софтвер заснован на заједничком коду који се користи у моделу један-према-више по принципу плаћања по употреби или претплате засноване на метрици употребе. Провајдер услуга у облаку развија и одржава софтвер базиран на облаку, обезбеђује аутоматска ажурирања софтвера и чини софтвер доступним својим клијентима путем интернета по принципу један-према-више, колико трошиш, толико платиш. Овај метод испоруке и лиценцирања софтвера омогућава приступ софтверу на мрежи путем претплате, а не куповине и инсталирања на сваком појединачном рачунару.

Напомена: Већина добављача SaaS-а ће морати да дода одобрење Подизвођача на Microsoft порталу за усаглашеност добављача ако се Подаци о личности или Поверљиви подаци корпорације Microsoft хостују на платформи треће стране.

Ангажовање подизвођача

Изаберите ово одобрење ако добављач ангажује Подизвођаче у Извршењу посла (прегледајте дефиниције у документу DPR).

Ово такође укључује слободњаке (види DPR).

Захтеви за уверења

Захтеви засновани на одобрењима профила

Одобрења која добављач изабере на профили обраде података омогућавају SSPA тиму да процени ниво ризика у погледу ангажовања добављача корпорације Microsoft. Захтеви везани за усаглашеност добављача програмом SSPA разликују се у зависности од одобрења добављача на њиховим профилима. Овај одељак објашњава различите SSPA захтеве.

Постоје и комбинације које захтевају усаглашеност са већим или мањим бројем услова. Комбинације су наведене у Додатку А и њихово извршење можете да очекујете на Microsoft порталу за усаглашеност добављача (Supplier Compliance Portal) када попуните профил. Увек можете да проверите како се ваш сценарио уклапа у овај оквир тиме што ћете захтевати преглед SSPA тима.

Радња: Пронађите свој профил одобрења у Додатку А и прегледајте одговарајуће захтеве за уверења, као и опције за независна уверења, ако су примењиве.

Важно: Ако ваш профил укључује софтвер као услугу (SaaS), подизвођаче, хостинг веб локација, или платне картице, потребно је додатно уверење.

Самостално атестирање за DPR

Сви добављачи регистровани у програму SSPA морају да спроведу самостално атестирање усаглашености за програмом DPR у року од 90 дана од добијања захтева. Овај захтев се добија једном годишње, али то може да буде и чешће ако се профил обраде података ажурира средином године. Налози добављача ће добити SSPA статус Црвен (неусаглашено) ако се прекорачи период од 90 дана. Нове поруџбенице унутар опсега не могу се обрађивати док SSPA статус не постане Зелен (усаглашено).

Новорегистровани добављачи морају испунити издате захтеве да би добили SSPA статус Зелен (усаглашено) пре него што ангажмани могу да почну.

Важно: SSPA тим нема овлашћење да одобри продужења рока за овај задатак.

Овлашћени представници који спроводе самостално атестирање треба да осигурају да имају довољно информација од стручњака за предметну област како би са сигурношћу одговорили на сваки захтев. Поред тога, додавањем свог имена у SSPA образац потврђују да су прочитали и разумели DPR. Добављачи могу да додају друге контакте у онлајн алат да помогну у испуњавању захтева.

Овлашћени представник (погледајте DPR за дефиницију), треба да:

1. Одреди који се захтеви примењују.
2. Постави одговор на сваки применљив захтев.
3. Потпише и пошаље писмо о уверавању на порталу за усклађеност са стандардима Microsoft добављача (Supplier Compliance Portal).

Примењивост

Од добављача се очекује да испуне све примењиве DPR захтеве издате за профил обраде података. Очекује се да се, у оквиру издатих захтева, неки можда неће односити на робу или услуге које добављач пружа корпорацији Microsoft. Они се могу означити као 'није примењиво' са детаљним коментаром који SSPA рецензенти могу да потврде.

SSPA тим прегледа поднеске DPR у потрази за ознакама 'није примењиво', 'сукоб са локалним правним прописима' или 'сукоб са уговорима' у односу на издате захтеве. SSPA тим може да затражи појашњење једне или више изабраних опција. Локални правни и уговорни сукоби прихватају се само ако су дате пратеће референце и ако је сукоб јасан.

Захтеви за независну процену

Погледајте одељак Захтеви по одобрењима у Додатку А да бисте видели одобрења за обраду података која покрећу овај захтев.

Добављачи имају опцију да промене одобрења ажурирањем свог профила обраде података. Међутим, ако добављач има улогу "Подобрађивача" у обради података, добављач не може да промени ово одобрење и од њега ће се захтевати да сваке године обави независну процену (Independent Assessment).

Да би обезбедили одобрења која захтевају независну верификацију усаглашености, добављачи ће морати да одаберу независног процењивача како би се потврдила усаглашеност у односу на документ DPR. Процењивач треба да припреми саветодавно писмо којим ће корпорацији Microsoft пружити гаранцију о усаглашености. Ово писмо мора да буде неквалификовано, а сви проблеми који нису у складу са захтевима морају бити решени и отклоњени пре него што се писмо потврде пошаље на Microsoft портал за усаглашеност добављача како би га прегледао SSPA тим. Процењивачи могу да преузму одобрени шаблон саветодавног писма, који је приложен уз документ "Преферирани процењивачи" у PDF формату [овде](#).

Додатак А садржи прихватљиве алтернативе сертификацији ако одаберете да не користите независног процењивача за потврђивање усаглашености са документом DPR (када је то примењиво, на пример за SaaS добављаче, добављаче хостинга веб сајтова или добављачима са Подизвођачима). Користе се стандарди ISO 27701 (приватност) и ISO 27001 (безбедност) јер су уско везани са Захтевима за заштиту података (DPR).

Када је Добављач пружалац здравствених услуга у Сједињеним Државама или покривено лице прихватићемо извештај HITRUST ради заштите приватности и безбедности.

SSPA може да обави независну процену ручно ако околности изван стандардних покретача захтевају додатну дужну пажњу. Примери укључују захтев одељења за приватност или безбедност; валидација санирања инцидента са подацима; или захтев за аутоматизовану примену права лица на која се подаци односе.

Смернице о томе како да приступите овом захтеву:

1. Ангажман мора да изврши процењивач са довољно техничке обуке и познавања материје како би усаглашеност била процењена на одговарајући начин.
2. Процењивачи морају бити повезани са Међународном федерацијом рачуновођа (IFAC) или Америчким институтом сертифицираних јавних рачуновођа (AICPA), или морају поседовати сертификате других релевантних организација за заштиту приватности и безбедности, као што су Међународно удружење стручњака за приватност (IAPP) или Удружење за ревизију и контролу информационих система (ISACA).
3. Процењивач мора користити најновији DPR који укључује доказе потребне за подупирање сваког захтева. **Добављачи ће процењивачу морати да доставе најскорије одобрене одговоре који се односе на атестирање усаглашености са DPR.**
4. У случају новорегистрованог добављача, процењивач ће тестирати дизајн контрола процеса. У свим осталим случајевима, процењивач ће тестирати ефикасност контрола.
5. Обим ангажовања у процени ограничен је на Податке о личности и/или Поверљиве податке корпорације Microsoft у вези са Извршењем посла тог добављача.
6. Обим ангажовања је ограничен на све активности обраде података које су у опсегу извршења посла и које се извршавају према броју налога добављача за који је примљен захтев. Ако добављач изабере више налога добављача у исто време, **писмо о атестирању мора да садржи листу налога добављача наведених у процени, као и повезане адресе.**
7. Писмо које се доставља SSPA тиму не сме да садржи ниједну изјаву за коју добављач не може да испуни Захтеве за заштиту података на начин на који су описани. Такви проблеми се морају решити пре него што се писмо достави.

SSPA је саставио листу [препоручених процењивача](#). Ове компаније су упознате са поступком обављања SSPA процена. Од добављача се очекује да плате ову процену; трошкови варирају у зависности од размера и обима обраде података.

Захтев за PCI DSS сертификацију

Стандард безбедности података индустрије платних картица (Payment Card Industry Data Security Standard, PCI DSS) је оквир за развој робусне безбедности података о платним картицама која укључује превенцију, откривање и одговарајућу реакцију на безбедносне инциденте. Оквир је развио PCI Савет за стандарде безбедности, саморегулаторна индустријска организација. Сврха PCI DSS захтева је да идентификује пропусте у технологији и процесима који представљају ризик по податке о власницима картица који се обрађују.

Microsoft је дужан да се придржава ових стандарда. Ако добављач обрађује информације о платним картицама у име корпорације Microsoft, захтевамо доказе о придржавању ових стандарда. Консултујте се са [PCI саветом за стандарде безбедности](#) да бисте разумели захтеве које поставља PCI организација.

У зависности од обима обрађених трансакција, добављач ће морати да ангажује Квалификованог процењивача безбедности који ће потврдити његову усаглашеност или ће

моћи да попуни [образац](#) за самосталну процену.

Брендови платних картица постављају прагове за тип процене, обично:

- Ниво 1: Доставите PCI AOC сертификат треће стране
- Ниво 2 или 3: Доставите PCI DSS упитник за самооцењивање (Self-Assessment Questionnaire, SAQ) који је потписао службеник добављача.

Пошаљите сертификат који се примењује и испуњава PCI захтеве.

Софтвер као захтев за услугу

Од добављача који испуњавају SaaS дефиницију која се налази у Профилу за обраду података, може се тражити да обезбеде важећи ISO 27001 сертификат ако се то захтева по уговору с корпорацијом Microsoft о услугама у облаку.

SSPA рецензенти ће потврдити да ваш поднесак испуњава уговорну обавезу.

Немојте слати сертификат центра података. Очекујемо ISO 27001 сертификат који се примењује на софтверске услуге наведене у вашем уговору с корпорацијом Microsoft.

Ангажовање подизвођача

Microsoft сматра ангажовање подизвођача фактором високог ризика. Добављачи који користе подизвођаче који ће обрађивати Податке о личности и/или Microsoft поверљиве податке морају обелоданити те подизвођаче. Поред тога, добављач такође треба да открије земље у којима ће те податке о личности обрађивати сваки подизвођач.

Инциденти са подацима

Ако добављач сазна за инцидент везан за приватност или безбедност података, мора о томе да обавести Microsoft на начин наведен у документу DPR.

Пријавите инцидент у вези са подацима користећи линк [SupplierWeb](#) или пошаљите е-поруку на адресу SupplR@microsoft.com

Обавезно наведите:

- Датум инцидента са подацима:
- Име добављача:
- Број добављача:
- Обавештене Microsoft контакте:
- Повезану поруџбеницу, ако је примењива/доступна:
- Сажетак инцидента с подацима:

Додатак А

Захтеви засновани на одобрењима профила

#	Профил	Захтеви за уверења	Опције за независна уверења
1	<p>Опсег: Лични, поверљиви</p> <p>Локација обраде: У корпорацији Microsoft или код Клијента</p> <p>Улога у обради: Обрађивач или Контролор</p> <p>Класа података: Поверљиви или Строго поверљиви</p> <p>Платне картице: Није примењиво</p> <p>SaaS: Није примењиво</p> <p>Ангажовање подизвођача: Није примењиво</p> <p>Хостовање веб сајтова: Није примењиво</p>	Самостално атестирање усаглашености са програмом DPR	
2	<p>Опсег: Поверљиви</p> <p>Локација обраде: Код Добављача</p> <p>Улога у обради: Није примењиво</p> <p>Класа података: Поверљиви</p> <p>Платне картице: Није примењиво</p> <p>SaaS: Није примењиво</p> <p>Ангажовање подизвођача: Није примењиво</p> <p>Хостовање веб сајтова: Није примењиво</p>	Самостално атестирање усаглашености са програмом DPR	
3	<p>Опсег: Поверљиви</p> <p>Локација обраде: Код Добављача</p> <p>Улога у обради: Обрађивач</p> <p>Класа података: Строго поверљиви</p> <p>Платне картице: Није примењиво</p> <p>SaaS: Није примењиво</p> <p>Ангажовање подизвођача: Није примењиво</p> <p>Хостовање веб сајтова: Није примењиво</p>	Самостално атестирање усаглашености са програмом DPR и Независно уверење о усаглашености	Опције независног уверења: 1. обавите независну процену у односу на DPR, или 2. Доставите ISO 27001

#	Профил	Захтеви за уверења	Опције за независна уверења
4	<p>Опсег: Лични, поверљиви</p> <p>Локација обраде: Код Добављача</p> <p>Улога у обради: Обрађивач</p> <p>Класа података: Строго поверљиви</p> <p>Платне картице: Није примењиво</p> <p>SaaS: Није примењиво</p> <p>Ангажовање подизвођача: Није примењиво</p> <p>Хостовање веб сајтова: Није примењиво</p>	<p>Самостално атестирање усаглашености са програмом DPR</p> <p>и</p> <p>Независно уверење о усаглашености</p>	<p>Опције независног уверења:</p> <ol style="list-style-type: none"> 1. обавите независну процену у односу на DPR, 2. независну процену у односу на одељак A-I DPR-а и ISO 27001, <p>или</p> <ol style="list-style-type: none"> 3. доставите ISO 27701 и ISO 27001
5	<p>Опсег: Лични, поверљиви</p> <p>Локација обраде: Код Добављача</p> <p>Улога у обради: Обрађивач</p> <p>Класа података: Поверљиви</p> <p>Платне картице: Није примењиво</p> <p>SaaS: Није примењиво</p> <p>Ангажовање подизвођача: Није примењиво</p> <p>Хостовање веб сајтова: Није примењиво</p>	<p>Самостално атестирање усаглашености са програмом DPR</p>	
6	<p>Опсег: Лични, поверљиви</p> <p>Локација обраде: Код Добављача</p> <p>Улога у обради: Контролор</p> <p>Класа података: Строго поверљиви или поверљиви</p> <p>Платне картице: Није примењиво</p> <p>SaaS: Није примењиво</p> <p>Ангажовање подизвођача: Није примењиво</p> <p>Хостовање веб сајтова: Није примењиво</p>	<p>Самостално атестирање усаглашености са програмом DPR</p>	

#	Профил	Захтеви за уверења	Опције за независна уверења
7	<p>Опсег: Лични, поверљиви</p> <p>Локација обраде: Свака</p> <p>Улога у обради: Подобрађивач (Ову улогу утврђује Microsoft – у профилу стоји: “Подобрађивач одобрен: Да”)</p> <p>Класа података: Строго поверљиви или поверљиви</p> <p>Платне картице: Није примењиво</p> <p>SaaS: Није примењиво</p> <p>Ангажовање подизвођача: Није примењиво</p> <p>Хостовање веб сајтова: Није примењиво</p>	<p>Самостално атестирање усаглашености са програмом DPR</p> <p>и</p> <p>Независно уверење о усаглашености</p>	<p>Опције независног уверења:</p> <ol style="list-style-type: none"> 1. обавите независну процену у односу на DPR, 2. независну процену у односу на одељак A-I DPR-а и ISO 27001, или 3. доставите ISO 27701 и ISO 27001

#	Профил	Захтеви за уверења	Опције за независна уверења
Утицај додавања опција SaaS, Подизвођачи, Хостовање веб сајтова			
8	<p>Опсег: Лични, поверљиви</p> <p>Локација обраде: Код Додављача</p> <p>Улога у обради: Обрађивач</p> <p>Класа података: Строго поверљиви или поверљиви</p> <p>Платне картице: Није примењиво</p> <p>Подизвођачи: ДА или</p> <p>SaaS: ДА или</p> <p>Хостовање веб сајтова: ДА</p>	<p>Самостално атестирање усаглашености са програмом DPR</p> <p>и</p> <p>Независно уверење о усаглашености</p>	<p>Опције независног уверења:</p> <ol style="list-style-type: none"> обавите независну процену у односу на DPR, независну процену у односу на одељак А-1 DPR-а и ISO 27001, <p>или</p> <ol style="list-style-type: none"> доставите ISO 27701 и ISO 27001
9	<p>Опсег: Лични, поверљиви</p> <p>Локација обраде: Код Додављача</p> <p>Улога у обради: Контролор</p> <p>Класа података: Строго поверљиви или поверљиви</p> <p>Платне картице: Није примењиво</p> <p>Подизвођачи: ДА или</p> <p>SaaS: ДА или</p> <p>Хостовање веб сајтова: ДА</p>	<p>Самостално атестирање усаглашености са програмом DPR</p>	

#	Профил	Захтеви за уверења	Опције за независна уверења
Додатна уверења за Платне картице и SaaS			
10	Било који од горенаведених профила и Платне картице	Горенаведени захтеви који се примењују и гаранција индустрије платних картица	Доставите сертификат PCI DSS
11	Било који од горенаведених профила и Софтвер као услуга (SaaS)	Горенаведени захтеви који се примењују и достављање сертификата ISO 27001 на који сте уговором обавезани и који покрива функционалне услуге.	Доставите ISO 27001 сертификат са функционалном покривеношћу услуга које пружате.