# Microsoftovi zahtjevi za zaštitu podataka o dobavljačima

## Primjenjivost

Microsoftovi zahtjevi za zaštitu podataka o dobavljačima („**DPR**”) odnose se na svakog Microsoftovog dobavljača 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**”).

- U slučaju sukoba između ovdje sadržanih zahtjeva i zahtjeva navedenih u ugovorima između dobavljača i tvrtke Microsoft, DPR ima prednost, osim ako primjenjivi dobavljač navede u DPR obrascu atestiranja točnu proviziju u ugovoru koji je u sukobu s primjenjivim DPR odjeljkom (u tom slučaju prednost imaju uvjeti ugovora).
- U slučaju sukoba između ovdje sadržanih zahtjeva i bilo kakvih pravnih ili statutarnih zahtjeva, prednost imaju pravni ili statutarni zahtjevi.
- U slučaju kad se Microsoftov dobavljač ponaša kao nadzornik, u skladu s ovim DPR-om, primjenjuju se samo zahtjevi u odjeljku J „Sigurnost” i odjeljku A „Upravljanje” u skladu s aktivnostima obrade tog dobavljača kao nadzornika.
- U slučaju kad se Microsoftov dobavljač ponaša kao podobrađivač, kao što su Microsoftove usluge savjetovanja, u skladu s ovim DPR-om, primjenjuju se samo zahtjevi u odjeljku A „Upravljanje”, odjeljku E „Zadržavanje”, odjeljku F „Subjekti podataka”, odjeljku G „Otkrivanje”, odjeljku H „Kvaliteta”, odjeljku I „Nadzor i provođenje” i odjeljku J „Sigurnost” u skladu s aktivnostima obrade tog dobavljača.
- U slučaju da Microsoftov dobavljač ne obrađuje Microsoftove osobne podatke, već samo Microsoftove povjerljive podatke, u skladu s ovim DPR-om, primjenjuju se samo zahtjevi u odjeljku A Upravljanje, odjeljku E Zadržavanje i J Sigurnost u skladu s obradom Microsoftovih povjerljivih podataka tog dobavljača.

## Međunarodni prijenos podataka

Bez ograničavanje njegovih drugih obaveza, dobavljač neće obavljati međunarodni prijenos Microsoftovih osobnih podataka osim ako je tvrtka Microsoft osigurala prethodno pisano odobrenje i u svakom slučaju dobavljač mora poštivati zahtjeve za zaštitu podataka, uključujući standardne ugovorne uvjete, ili prema odluci Microsofta druge odgovarajuće međunarodne mehanizme prijenosa koje su odobrile odgovarajuće vlasti za zaštitu podataka ili Europska komisija, kako je primjenjivo i usvojila ili prihvatila tvrtka Microsoft, uključujući, ali bez ograničenja prijenose iz Švicarske, okvir Zaštite privatnosti Švicarska-SAD , kako je primjenjivo. Sve sljedeće Standardne ugovorne odredbe koje je prihvatila Europska komisija ili Europski nadzornik za zaštitu podataka i odobrila Europska komisija bit će be ugrađene i obvezujuće za dobavljača od dana njhovog prihvaćanja. Dobavljač će također osigurati da se toga pridržavaju i svi podobrađivači (kako je definirano u Standardnim ugovornim odredbama).

## Ključne definicije

Sljedeći izrazi koji se koriste u ovom DPR-u imaju sljedeća značenja. Popis primjera nakon „uključujući”, „kao što je”, „npr.”, „na primjer” ili slični koji se koriste u ovom DPR-u tumače se da uključuju „bez ograničenja” ili „ali bez ograničavanja na“, osim ako su označeni riječima kao što su „samo” ili „isključivo”.

„**Nadzornik**” označava privatnu ili pravnu osobu, javnu vlast, agenciju ili bilo koje tijelo koje samostalno ili skupno s drugima utvrđuje svrhu i značenje obrade osobnih podataka; gdje svrhu i značenje obrade određuje Europska unija („**EU**”) ili zakoni države članice, nadzornika (ili kriterij za nominiranje nadzornika) mogu odrediti ti zakoni.

„**Probijanje podataka**” označava kršenje sigurnosti koje vodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa Microsoftovim osobnim podacima ili Microsoftovim povjerljivim podacima koji su poslani, pohranjeni su ili su na drugi način obrađeni od strane dobavljača ili njegovih podizvođača ili (2) sigurnosna ranjivost povezana s dobavljačevim rukovanjem Microsoftovih osobnih podataka ili Microsoftovih povjerljivih podataka.

„**Subjekt podataka**” označava sve stvarne osobe koje se mogu identificirati, izravno ili neizravno, osobito putem reference na identifikator, kao što je ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili putem jednog ili više faktora specifičnih za fizički, psihološki, genetički, mentalni, ekonomski, kulturalni ili socijalni identitet te stvarne osobe.

„**Pravo Subjekta podataka**” označava pravo Subjekta podataka da pristupi, briše, uređuje, izvozi, ograniči ili se protivi obradi Microsoftovih osobnih podataka tog Subjekta podataka, ako je to potrebno prema zakonu.

„**Zakon**” označava sve primjenjive zakone, pravila, pravilnike, uredbe, odluke, naredbe, regulativne odluke, kodove, zakonske odredbe, odluke i zahtjeve bilo koje pravne vlasti (federalne, državne, lokalne ili međunarodne) koje imaju nadležnost. „**Nezakonito**” označava svako kršenje zakona.

„**Microsoftovi povjerljivi podaci**” jesu bilo koji podaci koji, ako su kompromitirani putem povjerljivosti ili integriteta, mogu dovesti do značajnih gubitaka reputacije ili financijskih gubitaka tvrtke Microsoft. To uključuje hardverske i softverske proizvode tvrtke Microsoft, interne aplikacije za obavljanje poslovne djelatnosti, marketinške materijale koji prethode izdavanju, licencne ključeve proizvoda i tehničku dokumentaciju vezano uz proizvode i usluge tvrtke Microsoft.

„**Microsoftovi osobni podaci**“ označavaju sve osobne podatke koje obrađuje tvrtka Microsoft ili netko u njezino ime.

„**Osobni podaci**” označavaju sve podatke povezane sa Subjektom podataka i sve druge podatke koji čine „osobne podatke” ili „osobne informacije” prema zakonu.

„**Obrada**” označava svaku operaciju ili skup operacija koje se izvode na bilo kojim Microsoftovim osobnim ili povjerljivim podacima, bilo putem automatiziranih radnji ili ne, kao što su prikupljanje, snimanje, organizacija, strukturiranje, pohrana, adaptacija ili izmjena, dohvat, konzultacija, upotreba, otkrivanje putem emitiranja, rasparčavanje ili na drugi način postavljanja dostupnosti, poravnavanje ili kombiniranje, ograničavanje, brisanje ili uništavanje. „Obrađivanje” i „Obrađeno” imat će odgovarajuće značenje.

„**Obrađivač**” označava privatnu ili pravnu osobu, javnu vlast, agenciju ili drugo tijelo koje obrađuje osobne podatke u ime nadzornika.

„**Podizvođač**” označava treću stranu kojoj dobavljač dodjeljuje svoje obaveze u vezi s ugovorom koji pokriva njihovu izvedbu, uključujući afilijaciju dobavljača koja nema ugovor izravno s tvrtkom Microsoft.

„**Podobrađivač**” označava treću stranu koju Microsoft unajmljuje za Izvedbu, gdje Izvedba obuhvaća obradu Microsoftovih osobnih podataka za koje je Microsoft obrađivač.

„**Standardne ugovorne odredbe**” označavaju (i) standardne ugovorne odredbe za prijenos osobnih podataka obrađivačima koji su u trećim državama koje ne osiguravaju adekvatnu razinu zaštite podataka, kako je opisano u Članku GDPR-a i odobreno od strane Europske komisije u odluci 2010/87/EC 5. veljače 2010.; (ii) sve sljedeće odredbe koje je usvojila Europska komisija u skladu s GDPR-om; (iii) sve sljedeće odredbe koje je usvojio Europski nadzornik za zaštitu podataka i odobrio u skladu s EUDPR-om; i (iv) sve odredbe koje je na drugi način odobrio Europski nadzornik za zaštitu podataka za podatkovne prijenose za Microsoftove entitete u skladu s EUDPR-om.

„**Zahtjevi za zaštitu privatnosti podataka**” označavaju GDPR, EUDPR, Lokalni EU/EEA zakoni za zaštitu podataka, Kalifornijski zakon o zaštiti privatnosti potrošača, Cal. Civ. Code § 1798.100 i sljedeći („*CCPA*”), Dokument o zaštiti podataka Ujedinjene Kraljevine iz 2018. i svi povezani ili sljedeći zakoni, odredbe i drugi pravni zahtjevi primjenjivi u Ujedinjenoj Kraljevini, te svi primjenjivi zakoni, odredbe i drugi pravni zahtjevi povezani s (a) privatnošću i sigurnošću podataka; ili (b) upotrebom, prikupljanjem, zadržavanjem, pohranom, sigurnošću, otkrivanjem, prijenosom, odlaganjem i drugim vrstama obrade osobnih podataka.

„**EUDPR**" označava Odredbu (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti stvarnih osoba u vezi s obradom osobnih podataka od strane institucija, tijela, ureda i agencija Unije te o slobodnom kretanju takvih podataka i stavljanju izvan snage Odredbe (EC) No. 45/2001 i Odluke br. 1247/2002/EC.

„**GDPR**" označava Odredbu (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti stvarnih osoba u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka i stavljanju izvan snage Odredbe 95/46/EC (Odredba o općoj zaštiti podataka).

„**Odredbe EU modela**" i „**Standardne ugovorne odredbe**" označavaju standardne ugovorne odredbe za prijenos osobnih podataka obrađivaču koji je u trećoj državi, kako je postavljeno u dodatku Odluke Europske komisije 2010/87/EU 5. veljače 2010. kako je postavljeno u Prilogu A Standardnih ugovornih odredbi i svim sljedećim Standardnim ugovornim odredbama.

„**Sve sljedeće Standardne ugovorne odredbe**" označavaju sve odredbe koje je prihvatila Europska komisija u skladu s Odredbom (EU) 2016/679 Europskog parlamenta i Vijeća 27. travnja 2016. o zaštiti stvarnih osoba u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka i stavljanju izvan snage Odredbe 95/46/EC (Odredba o općoj zaštiti podataka) i odredbe koje je prihvatio Europski nadzornik za zaštitu podataka i odobrila Europska komisija ili koje je na drugi način odobrio Europski nadzornik za zaštitu podataka za podatkovne prijenose za Microsoftove entitete u skladu s Odredbom (EU) 2018/1725 Europskog parlamenta i Vijeća 23. listopada 2018. o zaštiti stvarnih osoba u vezi s obradom osobnih podataka od strane institucija, tijela, ureda i agencija Unije te o slobodnom kretanju takvih podataka i stavljanju izvan snage Odredbe (EC) No. 45/2001 i Odluke br. 1247/2002/EC.

## Odgovor dobavljača

Dobavljači godišnje potvrđuju usklađenost s ovim zahtjevima o korištenju mrežnih usluga kojima upravlja tvrtka Microsoft. Pogledajte Vodič za program SSPA da biste razumjeli kako se upravlja usklađenošću.

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak A: Upravljanje** | |
| 1 | Svaki primjenjivi ugovor između Microsofta i dobavljača (npr. glavni ugovor, izjava o radu, narudžbenice i druge narudžbe) sadrži jezik zaštite podataka privatnosti i sigurnosti u odnosu na Microsoftove povjerljive i osobne podatke, kako je primjenjivo, uključujući zabrane prodaje Microsoftovih osobnih podataka i obradu Microsoftovih osobnih podataka izvan izravnog poslovnog odnosa između Microsofta i dobavljača.<br><br>Za tvrtke koje se ponašaju kao obrađivači ili podobrađivači u vezi s Izvedbom, u skladu s Microsoftovim osobnim podacima, ugovor mora uključivati temu i trajanje obrade, prirodu i svrhu obrade, vrstu Microsoftovih osobnih podataka i kategorije Subjekata podataka te obaveze i prava tvrtke Microsoft. | Dobavljač mora podnijeti primjenjivi ugovor između tvrtke Microsoft i dobavljača.<br><br>Za obrađivače i podobrađivače opisi obrade nalaze se u primjenjivom ugovoru (*npr.* izjava o radu, narudžbenice).<br><br>Napomena: tvrtke s narudžbenicama tijekom leta mogu dodati potreban opis aktivnosti obrade kasnije tijekom postupka kupnje. |
| 2 | Dodijeliti odgovornost i pouzdanost u skladu s DPR-om određenoj osobi ili grupi unutar tvrtke. | Naziv uloge osobe ili grupe zadužene za osiguranje usklađenosti s DPR-om Microsoftovog dobavljača.<br><br>Dokument opisuje ovlasti i odgovornosti ove osobe ili grupe koji pokazuje ulogu privatnosti i/ili sigurnosti. |
| 3 | Uspostavljanje, održavanje i obavljanje godišnje obuke o privatnosti i sigurnosti za zaposlenike koji će imati pristup Osobnim podacima koje obrađuje dobavljač u vezi s Izvedbom ili Microsoftovim povjerljivim podacima.<br><br>Ako vaša tvrtka nema pripremljen sadržaj, možete koristiti ovaj izvadak organizatora i prilagoditi ga svojoj tvrtki.<br><br>Napomena: od osoblja dobavljača može se tražiti da dovrše dodatnu obuku koju osiguravaju Microsoftovi odjeli. | Dostupni su godišnji zapisi o pohađanju i mogu se po zahtjevu dostaviti tvrtki Microsoft.<br><br>Sadržaj o obuci obuhvaća principe o privatnosti i sigurnosti.<br><br>Dokumentacija o usklađenosti uz zahtjeve za obuku uključivat će dokaze o obuci povezane s pravnim zahtjevima o privatnosti, sigurnosnim obavezama i usklađenosti s primjenjivim ugovornim zahtjevima i obavezama. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak A: Upravljanje (nast.)** | |
| 4 | Obrađivati Microsoftove osobne podatke samo u skladu s Microsoftovim dokumentiranim uputama, uključujući scenarije imajući na umu prijenose Microsoftovih osobnih podataka trećoj zemlji ili međunarodnoj organizaciji, osim ako se to traži zakonom; u takvom slučaju obrađivač ili podobrađivač (dobavljač) će obavijestiti nadzornika (Microsoft) o tom pravnom zahtjevu prije obrade, osim ako zakon zabranjuje takve podatke na važnom temelju javnog interesa. | Dobavljač sakuplja i održava sve Microsoftove dokumentirane upute (npr. ugovor, izjavu o radu ili dokumentaciju narudžbe) elektroničkim putem na lako dostupnoj lokaciji zaposlenicima dobavljača i ugovornim stranama koje sudjeluju u Izvedbi. |
| | **Odjeljak B: Obavijest** | |
| 5 | Dobavljač mora koristiti Microsoftovu Izjavu o zaštiti privatnosti kad prikuplja osobne podatke u ime tvrtke Microsoft.<br><br>Obavijest o privatnosti mora biti jasna i dostupna Subjektima podataka kako bi im pomogla da odluče žele li dobavljaču dati svoje osobne podatke.<br><br>Napomena: tamo gdje je vaša tvrtka nadzornik aktivnosti obrade, objavit ćete svoju vlastitu obavijest o privatnosti. | Dobavljač koristi fwdlink za aktualnu objavljenu Microsoftovu Izjavu o zaštiti privatnosti.<br><br>Izjava o zaštiti privatnosti objavljuje se u bilo kojem kontekstu gdje će se prikupljati korisnički osobni podaci.<br><br>Ako je primjenjivo, dostupna je izvanmrežna verzija te se nudi prije prikupljanja podataka.<br><br>Bilo koje izvanmrežne Izjave o zaštiti privatnosti koje se koriste jesu najnovije objavljene verzije i ispravno su datirane.<br>Za usluge Microsoftovih zaposlenika koristi se Microsoftova Obavijest o privatnosti podataka. |
| 6 | Prilikom prikupljanja Microsoftovih osobnih podataka putem glasovnog poziva uživo ili snimljenog glasovnog poziva, dobavljači moraju biti pripremljeni na razgovor sa Subjektima podataka o primjenjivima načinima prikupljanja, rukovanju, korištenju i zadržavanju podataka. | Skripta za glasovne snimke uključuje kako se obrađuju Microsoftovi osobni podaci i uključuje<br>▪ prikupljanje,<br>▪ upotrebu i<br>▪ zadržavanje. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak C: Izbor i pristanak** | |
| 7 | Kad se dobavljač oslanja na pristanak kao zakonski temelj za obradu podataka, dobavljač mora nabaviti i dokumentirati pristanak Subjekta podataka za sve svoje aktivnosti obrade (uključujući sve nove i ažurirane aktivnosti obrade) prije prikupljanja osobnih podataka tog Subjekta podataka. | Dobavljač može demonstrirati kako Subjekt podataka daje pristanak za aktivnost obrade te da opseg pristanaka pokriva sve aktivnosti obrade dobavljača u skladu s osobnim podacima tog Subjekta podataka.<br><br>Dobavljač može demonstrirati kako Subjekt podataka povlači pristanak za aktivnost obrade.<br><br>Dobavljač može demonstrirati kako se provjeravaju preference prije pokretanja nove aktivnosti obrade.<br><br>Dobavljač nadzire učinkovitost upravljanja preferencama kako bi osigurao vremenski okvir za promjenu preferenci i to je najrestriktivniji lokalni pravni zahtjev koji se primjenjuje.<br><br>Napomena: dokaz može biti snimka zaslona interakcije s korisnikom; eksperimentiranje s uslugom ili mogućnost pregleda tehničke dokumentacije. |
| 8 | Kolačići su male tekstualne datoteke koje na uređaju pohranjuju web-mjesta i/ili aplikacije koje sadrže podatke koji se koriste za prepoznavanje Subjekta podataka ili uređaja.<br><br>Dobavljači koji izrađuju i upravljaju Microsoftovim web-mjestima i/ili aplikacijama moraju Subjektima podataka ponuditi transparentnu obavijest i odabir u vezi upotrebe kolačića. Osim ako je posebno zatraženo da se to ne radi od strane ugovorne poslovne jedinice, dobavljači trebaju koristiti Standardni banner koji je napravio 1ES za upravljanje kontrolama za odabir.<br><br>Dobavljači koji izrađuju i upravljaju Microsoftovim web-mjestima i/ili aplikacijama moraju osigurati da je upotreba kolačića u skladu s obavezama u Izjavi o zaštiti privatnosti tvrtke Microsoft i lokalnim zakonskim zahtjevima, kao što su pravila koja je postavila Europska unija.<br><br>Napomena: Microsoftovi poslovni sponzori moraju registrirati Microsoftova web-mjesta na internonm portalu Web Compliance (http://aka.ms/wcp) kako bi im se inventar kolačića katalogizirao i kako bi se njime upravljalo. | Svrha svakog kolačića mora biti dokumentirana i mora obavještavati o vrsti implementiranog kolačića.<br>▪ Dugotrajni kolačići ne smiju se koristiti kad su dostatni kolačići sesije.<br>▪ Kad se koriste dugotrajni kolačići, oni ne smiju imati datum isteka koji je dulji od 2 godine nakon što je korisnik posjetio web-mjesto.<br><br>Provjerite usklađenost sa zakonima EU koji su primjenjivi, kao što je:<br>▪ upotreba pravila o naslovima, „Privatnost i kolačići” za izjavu o privatnosti.<br>▪ osigurati korisnikov pristanak prije upotrebe kolačića u svrhu koja nije ključna, kao što je oglašavanje<br>▪ pristanak mora isteći ili ga je potrebno ponovo dobiti na najviše svakih 6 mjeseci. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak D: Prikupljanje** | |
| 9 | Dobavljač mora nadgledati prikupljanje Microsoftovih osobnih i/ili povjerljivih podataka kako bi se osiguralo da se prikupe samo podaci potrebni za izvođenje. | Dobavljač može pružiti dokumentaciju koja pokazuje da se Microsoftovi osobni i/ili povjerljivi podaci prikupljaju kako je potrebno za izvedbu.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 10 | Ako dobavljač prikuplja osobne podatke od treće strane u ime Microsofta, dobavljač mora potvrditi da su pravila i prakse treće strane u vezi zaštite podataka u skladu s dobavljačevim ugovorom s Microsoftom te da ispunjavaju DPR zahtjeve. | Dobavljač može pružiti dokumentaciju da je provedena dubinska analiza pravila i načina zaštite podataka treće strane.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 11 | Prije prikupljanja Microsoftovih osobnih podataka putem instalacije ili korištenja softvera koji se može pokrenuti na računalu Subjekta podataka, potrebno je dokumentirati potrebu prikupljanja tih podataka u sporazumu dobavljača s tvrtkom Microsoft koji je na snazi. | Microsoftov ugovor za upotrebu softvera za izvođenje na uređaju Subjekta podataka naveden je u izvršenom ugovoru. |
| 12 | Prije prikupljanja osjetljivih Microsoftovih osobnih podataka (podataka koji otkrivaju rasno ili etničko podrijetlo, politička stajališta, vjerska ili filozofska vjerovanja ili članstvo u sindikatu, genetičke podatke, biometrijske podatke, podatke u vezi zdravlja ili podatke u vezi seksualnog života ili seksualne orijentacije osobe), potrebitost prikupljanja takvih Microsoftovih osobnih podataka potrebno je dokumentirati u pravovaljanom ugovoru dobavljača s tvrtkom Microsoft. | Potrebitost prikupljanja osjetljivih Microsoftovih osobnih podataka navedena je u izvršenom ugovoru s tvrtkom Microsoft. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak E: Zadržavanje** | |
| 13 | Osigurati da se Microsoftovi osobni i povjerljivi podaci zadržavaju u vremenu koje ne traju dulje od potrebnog za izvođenje, osim ako je zadržavanje Microsoftovih osobnih i/ili povjerljivih podataka zakonski uvjetovano. | Dobavljač radi u skladu s pravilima dokumentiranog zadržavanja ili zahtjevima zadržavanja koje određuje Microsoft u ugovoru (npr. izjavi o radu, narudžbenici).<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 14 | Osigurati da se, prema isključivom nahođenju Microsofta, Microsoftovi osobni i povjerljivi podaci u posjedu dobavljača ili pod njegovim nadzorom vrate Microsoftu ili da se unište nakon dovršetka izvedbe ili po Microsoftovom zahtjevu.<br><br>Unutar aplikacija, procesi moraju osigurati da kad se podaci uklone iz aplikacije eksplicitno od strane korisnika ili na temelju drugih okidača poput starosti podataka, da su ti podaci sigurno izbrisani.<br><br>Kad je potrebno uništiti Microsoftove osobne ili povjerljive podatke, dobavljač mora spaliti, samljeti ili izrezati fizička sredstva koja sadrže Microsoftove osobne i/ili povjerljive podatke, tako da podatke nije moguće pročitati niti rekonstruirati. | Zadržati zapise o odbacivanju Microsoftovih osobnih i osjetljivih podataka za (npr. o vraćanju tvrtki Microsoft radi uništavanja).<br><br>Ako je potrebno uništavanje ili ga Microsoft zahtijeva, dobavljač mora dati certifikat o uništenju koji je potpisao djelatnik dobavljača. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak F: Subjekti podataka** | |
| | Subjekti podataka imaju pravo pristupiti, izbrisati, urediti, izvesti, zabraniti i žaliti se protiv obrade svojih osobnih podataka („**Prava Subjekta podataka**"). Kad Subjekt podataka zatraži ispunjavanje svojih prava prema zakonima u vezi svojih Microsoftovih osobnih podataka, dobavljač mora omogućiti tvrtki Microsoft da učini nešto od sljedećeg ili da izvede ove radnje u ime tvrtke Microsoft: | |
| 15 | Asistirati tvrtki Microsoft putem odgovarajućih tehničkih i organizacijskih mjera, gdje je moguće, da bi ispunio svoje obaveze u reagiraju na zahtjeve Subjekata podataka koji traže izvršiti svoja Prava Subjekata podataka bez odgađanja.<br><br>Osim ako je Microsoft drugačije odredio, dobavljač će sve Subjekte podataka koji ga kontaktiraju uputiti izravno Microsoftu da ispune svoja Prava subjekata podataka. | Dobavljač mora održavati dokaze o dokumentiranim postupcima i procedurama kako bi podržao izvršavanje DSR-a.<br><br>Dobavljač će zadržati dokumentirane dokaze testiranja. Dokazi će biti dostupni po zahtjevu tvrtki Microsoft. |
| 16 | Kad odgovara izravno Subjektu podataka ili kad dobavljač osigura samoposlužni mrežni mehanizam, dobavljač ima postupke i procedure za identificiranje Subjekta podataka koji podnosi zahtjev. | Dobavljač ima dokumentiranu metodu koja se koristi za identificiranje Microsoftovih Subjekata podataka.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 17 | Ako tvrtka Microsoft traži da se lociraju Microsoftovo osobni podaci o Subjektu podataka koji nisu dostupni putem samoposlužnog mrežnog mehanizma, dobavljač će uložiti sve razumne napore da locira zatražene podatke i sačuva dovoljno zapisa koji pokazuju da je uložen razuman trud u pretraživanje. | Dobavljač će zadržati dokumentirane dokaze o procedurama kako bi utvrdio zadržavaju li se Microsoftovi osobni podaci i pružit će dokumentaciju tvrtki Microsoft po zahtjevu.<br><br>Dobavljač zadržava zapis koji pokazuje koji su koraci poduzeti da se udovoljio zahtjevima Prava Subjekta podataka.<br>Dokumentacija uključuje:<br>▪ datum i vrijeme zahtjeva<br>▪ radnje koje su poduzete kako bi se odgovorilo na zahtjev i zapis kad je tvrtka Microsoft obaviještena.<br>Dobavljač će pružiti dokaze o čuvanju zapisa tvrtki Microsoft po zahtjevu. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak F: Subjekti podataka (nast.)** | |
| 18 | Dobavljač će Subjektu podataka reći sve korake koje je potrebno poduzeti da bi dobili pristup ili na drugi način ostvarili svoja prava vis-à-vis njihovih Microsoftovih osobnih podataka. | Dobavljač će zadržati dokumentirane dokaze o komunikaciji i postupcima za pristup Microsoftovim osobnim podacima. Dobavljač će zadržati dokumentirane dokaze i pružiti ih tvrtki Microsoft po zahtjevu. |
| 19 | Zabilježiti datum i vrijeme zahtjeva Prava Subjekta podataka i radnji koje je poduzeo dobavljač kao odgovor na takve zahtjeve<br><br>Ako se njihov zahtjev odbije, prema uputama Microsofta, ponudite Subjektu podataka pisano objašnjenje.<br><br>Daje zapise o zahtjevima Subjekta podataka tvrtki Microsoft po zahtjevu. | Dobavljač održava zapise o zahtjevima za pristup i dokumentira promjene Microsoftovih osobnih podataka.<br><br>Instance dokumenata kada se zahtjevi odbiju i zadržavabhe dokaza Microsoftovog pregleda i odobrenja.<br><br>Dobavljač će pružiti dokaze o čuvanju zapisa zahtjeva i odbijanja pristupa Microsoftovim osobnim podacima. |
| 20 | Dobavljač mora omogućiti tvrtki Microsoft ili dobiti kopiju zatraženih Microsoftovih osobnih podataka za autentificiranog Subjekta podataka u odgovarajućem tiskanom, elektroničkom ili verbalnom formatu. | Dobavljač daje Microsoftove osobne podatke Subjektu podataka u formatu koji je razumljiv te u obliku koji odgovara Subjektu podataka i dobavljaču. |
| 21 | Dobavljač mora poduzeti razumne mjere opreza kako bi se osiguralo da se izdani Microsoftovi osobni podaci ne koriste za identifikaciju druge osobe. | Dobavljač mora održavati dokumentirane dokaze postupaka povezanih s mjerama opreza kako bi se izbjegla identifikacija Subjekta podataka koja nije u skladu s uvjetima ugovora. Dobavljač će pružiti dokaze tvrtki Microsoft po zahtjevu. |
| 22 | Ako se Subjekt podataka i dobavljač ne slažu o tome jesu li Microsoftovi osobni podaci potpuni i točni, dobavljač mora eskalirati problem tvrtki Microsoft i surađivati s tvrtkom Microsoft ako je potrebno za rješavanje problema. | Dobavljač dokumentira slučajeve neslaganja i eskalira problem tvrtki Microsoft.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak G: Otkrivanje trećim stranama** | |
| | Ako dobavljač namjerava koristiti podizvođača za obradu Microsoftovih osobnih ili povjerljivih podataka, dobavljač mora sljedeće: | |
| 23 | Dobiti Microsoftovo izričito pisano odobrenje prije unajmljivanja podizvođača usluga ili unošenja bilo kakvih izmjena u vezi dodavanja ili zamjene podizvođača.<br><br>Napomena: navedite svoje prihvaćanje ove obaveze čak i ako trenutačno nemate podizvođače, ali ih u budućnosti možete imati. | Potvrdite da Microsoftove osobne podatke obrađuju samo tvrtke koje su poznate Microsoftu kako se zahtijeva primjenjivim ugovorom (npr. izjava o radu, dodatak, narudžbenica) ili kako je snimljeno u bazi podataka SSPA-a. |
| 24 | Dokumentirati prirodu i opseg Microsoftovih osobnih i povjerljivih podataka koje obrađuje podizvođač, osiguravajući da su prikupljeni podaci potrebni za izvođenje. | Dobavljač održava dokumentaciju koja s odnosi na Microsoftove osobne i povjerljive podatke koji su otkriveni ili preneseni podizvođačima.<br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 25 | Kad je Microsoft nadzornik Microsoftovih osobnih podataka, osigurati da podizvođač koristi Microsoftove osobne podatke u skladu s navedenim preferencama kontakta za Subjekt podataka. | Pokazati kako podizvođači koriste preference Microsoftovih Subjekata podataka.<br>Ponuditi pomoćnu dokumentaciju (npr. snimke zaslona, SLA, SOW itd.) koja obuhvaća vremenski okvir za podizvođača da ispoštuje promjene preferenci. |
| 26 | Ograničiti podizvođačevu obradu Microsoftovih osobnih podataka na svrhe nužne za ispunjavanje ugovora dobavljača s tvrtkom Microsoft. | Dobavljač može pružiti dokumentaciju koja pokazuje da se Microsoftovi osobni podaci daju podizvođaču kako je potrebno za izvedbu.<br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak G: Otkrivanje trećim stranama (nast.)** | |
| 27 | Pregledati žalbe za indikacije bilo kakve neovlaštene ili nezakonite obrade Microsoftovih osobnih podataka. | Dobavljač može demonstrirati sustave i postupke koji su tu su da rješavaju žalbe koje se odnose na podizvođačevo neovlašteno korištenje ili otkrivanje Microsoftovih osobnih podataka.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 28 | Odmah obavijestiti tvrtku Microsoft ako saznate da je podizvođač obradio Microsoftove osobne ili povjerljive podatke u bilo koje druge svrhe osim onih povezanih s izvedbom. | Dobavljač je podizvođaču dao upute i načine za prijavljivanje zloupotrebe Microsoftovih podataka.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 29 | Odmah poduzeti postupke za umanjenje bilo koje stvarne ili potencijalne štete uzrokovane podizvođačevom neovlaštenom ili nezakonitom obradom Microsoftovih osobnih i privatnih podataka. | Dobavljač mora održavati dokumentirane dokaze plana i postupka te pružiti dokaz dokumentacije tvrtki Microsoft po zahtjevu. |
| | **Odjeljak H: Kvaliteta** | |
| 30 | Dobavljač mora zadržati integritet svih Microsoftovih osobnih podataka te osigurati da ostanu točni, potpuni i relevantni za navedene svrhe zbog kojih su obrađeni. | Dobavljač može demonstrirati da postoje postupci za validaciju Microsoftovih osobnih podataka kad se prikupljaju, izrađuju i ažuriraju.<br><br>Dobavljač može demonstrirati da postoje postupci za nadzor i uzorkovanje da bi se potvrdila točnost i ispravnost u svakom trenutku, ako je to potrebno.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | Odjeljak I: Nadzor i provođenje | |
| 31 | Dobavljač ima plan odgovora na incident koji zahtijeva da dobavljač obavijesti tvrtku Microsoft bez odlaganja čim postane svjestan probijanja podataka.<br><br>Dobavljač mora, po zahtjevu ili uputama tvrtke Microsoft, surađivati s Microsoftom u svakoj istrazi, ublažavanju ili rješavanju Incidenta, uključujući davanje Microsoftu podataka, informacija, pristupa osoblju dobavljača ili potrebnom hardveru za provođenje forenzičkog pregleda. | Dobavljač ima plan za odgovor na incident koji uključuje korak za obavještavanje korisnika (Microsoft) kako je opisano u ovom odjeljku.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 32 | Ne smije izdati nikakve objave za medije niti bilo koju drugu objavu za javnost koje su povezane s probijanjem podataka. | Dobavljač pristaje ispuniti ovaj zahtjev ako dođe do događaja. |
| 33 | Implementirati plan ispravljanja i nadzirati rješavanje svakog probijanja podataka kako bi se osiguralo pravovremeno poduzimanje odgovarajućih radnji. | Dobavljač ima dokumentirane postupke koje će poduzeti kao odgovor na probijanje podataka i rješavanje problema.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |
| 34 | Kad je Microsoft nadzornik Microsoftovih osobnih podataka, ustanoviti službeni žalbeni postupak za reakciju na sve žalbe u vezi sa zaštitom podataka koje se odnose na Microsoft osobne podatke. | Dobavljač ima načine za primanje žalbi u vezi Microsoftovih osobnih podataka te ima dokumentirani postupak za žalbe kako bi ih riješio.<br><br>Dobavljač će pružiti dokumentirane dokaze tvrtki Microsoft po zahtjevu. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak J: Sigurnost** | |
| | Dobavljač mora postaviti, implementirati i održavati program o sigurnosti podataka koji sadrži pravila i postupke kako bi zaštitio i očuvao sigurnost Microsoftovih osobnih i povjerljivih podataka u skladu s dobrim praksama industrije i kako se to zahtijeva zakonom.<br>Sigurnosni program dobavljača mora udovoljavati standardima koji se nalaze niže, zahtjevi 35-53. | Prihvatljiva zamjena za odjeljak J jest valjano izvješće ISO 27001 ili SOC 2 sa sigurnošću.<br><br>Napomena: morat ćete podnijeti dokumentaciju koja opisuje opseg ovih certifikata/izvješća. |
| 35 | Obaviti godišnju procjenu sigurnosti mreže koja obuhvaća:<br>▪ pregled velikih izmjena okruženja, kao što su nova komponenta sustava, mrežna topologija, pravilo vatrozida,<br>▪ obavljanje skeniranja ranjivosti i<br>▪ održavanje zapisnika promjena. | Dobavljač ima dokumentiranu procjenu mreže, zapisnike o izmjenama i rezultate skeniranja.<br><br>Potrebni zapisnici o izmjenama moraju pratiti izmjene, dati podatke o razlogu izmjene i uključivati ime i titulu dodijeljene osobe koja je to odobrila. |
| 36 | Dobavljač mora definirati, komunicirati i implementirati pravilo za mobilne uređaje koje štiti i ograničava upotrebu Microsoftovih osobnih ili povjerljivih podataka kojima se pristupa ili se koriste na mobilnom uređaju. | Dobavljač demonstrira upotrebu pravila za mobilne uređaje gdje rukovanje Microsoftovim osobnim ili povjerljivim podacima zahtijeva upotrebu mobilnog uređaja. |
| 37 | Sva sredstva koja se koriste za podržavanje izvedbe moraju biti na broju i imati identificiranog vlasnika. Dobavljač je odgovoran za održavanje inventara tih informacijskih sredstava; uspostavljajući prihvatljivu i ovlaštenu upotrebu sredstava; i nudeći odgovarajuću razinu zaštite za sredstva tijekom njihovog vijeka trajanja. | Inventar uređaja korištenih za podržavanje performansi. Inventar tih sredstava mora sadržavati:<br>▪ lokaciju uređaja<br>▪ klasifikaciju podataka na sredstvu<br>▪ zapis obnove sredstva nakon dovršetka posla ili poslovnog ugovora i<br>▪ zapis o odlaganju medija za pohranu podataka kad više nije potreban. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | Odjeljak J: Sigurnost (nast.) | |
| 38 | Uspostaviti i održati postupke za upravljanje pravima pristupa kako bi se spriječio neovlašteni pristup bilo kojim Microsoftovim osobnim ili povjerljivim podacima pod kontrolom dobavljača. | Dobavljač pokazuje da je implementirao plan pristupa upravljanja pravima koji obuhvaća:<br>▪ pristup postupcima kontrole<br>▪ postupci identifikacije<br>▪ postupci za zaključavanje nakon neuspješnih pokušaja<br>▪ robusni parametri za odabir vjerodajnica za autentifikaciju i<br>▪ deaktivacija korisničkih računa po završetku zadatka u roku od 48 sati kontrole lozinke, uključujući:<br>○ 1) ponovno postavljanje lozinke koliko je često potrebno, ali ne dulje od svakih 70 dana<br>○ ili 2) prilikom primjene upotrebe biometrijskih prijava (samo za neprivilegirane korisničke račune): lozinka se mijenja svakih 365 dana, automatski tjerajući korisnike (uključujući administratore) da promijene lozinke za korisničke račune nakon isteka, osiguravajući da su konfigurirane kontrole protiv lažiranja pošiljatelja.<br><br>Dobavljač pokazuje da je uspostavio postupak za pregled pristupa korisnika Microsoftovim osobnim i povjerljivim podacima, primjenjujući princip najmanje privilegije. Postupak uključuje:<br>▪ jasno definirane korisničke uloge<br>▪ postupci za pregled i opravdanje odobrenja pristupa ulogama i<br>▪ testiranje da korisnici unutar uloga s pristupom Microsoftovim podacima imaju dokumentirano opravdanje za tu grupu/ulogu. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak J: Sigurnost (nast.)** | |
| 39 | Definirati i implementirati postupke upravljanja zakrpama koji daju prioritet sigurnosnim zakrpama za sustave koji se koriste za obradu Microsoftovih osobnih ili povjerljivih podataka. Ovi postupci uključuju:<br>▪ definirani pristup riziku radi davanja prioriteta sigurnosnim zakrpama<br>▪ mogućnost rukovanja i implementiranja hitnih zakrpa<br>▪ primjenjivost za operativni sustav i serverski softver, kao što su poslužitelj aplikacija i softver baze podataka<br>▪ dokumentiranje rizika koji zakrpa smanjuje i praćenje svih izuzetaka i<br>▪ zahtjevi za prekid korištenja softvera koji autorska tvrtka više ne podržava. | Dobavljač može demonstrirati implementirani postupak upravljanja zakrpama koji udovoljava ovom zahtjevu i pokriva barem sljedeće.<br>▪ Određivanje ozbiljnosti za informiranje postavljanja prioriteta. (Definicije ozbiljnosti dokumentirane su.)<br>▪ Dokumentirani postupak za implementiranje hitnih zakrpa.<br>▪ Provjerite da se ne koriste operativni sustavi koji više nemaju podršku autorske tvrtke.<br>▪ Zapisi upravljanja zakrpama koji prate odobrenja i izuzetke. |
| 40 | Instalirati antivirusni softver i softver protiv zlonamjernih programa na opremu povezanu s mrežom koja se koristi za obradu Microsoftovih osobnih i povjerljivih podataka, uključujući poslužitelje, računala za produkciju i obuku kako bi se zaštitili od potencijalno opasnih virusa i zlonamjernog softvera.<br><br>Ažurirati definicije zlonamjernih programa svakodnevno ili kako je naveo dobavljač antivirusnog softvera i softvera protiv zlonamjernih programa. Napomena: to se odnosi na sve operativne sustave, uključujući Linux. | Postoje zapisi da je aktivan antivirusni softver i softver protiv zlonamjernih programa.<br><br>Napomena: ovaj zahtjev primjenjuje se na sve operativne sustave. |
| 41 | Dobavljači koji razvijaju softver za Microsoft u postupak izrade moraju inkorporirati principe sigurnosti po dizajnu. | Dobavljačevi dokumenti s tehničkim specifikacijama uključuju točke provjere za provjeru sigurnosti u svojim razvojnim ciklusima. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak J: Sigurnost (nast.)** | |
| 42 | Implementiranje programa Prevencija gubitka podataka („**DLP**") za sprječavanje ometanja, gubitka i druge neovlaštene aktivnosti.Podatke je potrebno ispravno klasificirati, označiti i zaštititi te dobavljač mora nadzirati informacijske sustave koji se koriste tamo gdje se obrađuju Microsoftovi osobni ili povjerljivi podaci kako ne bi došlo do ometanja, gubitka i druge neovlaštene aktivnosti. Program DLP minimalno zahtijeva sljedeće:<br>▪ upotrebu sustava Intrusion Detection Systems („**IDS**") na poslužitelju, mreži i u oblaku prema industrijskim standardima ako zadržavate Microsoftove osobne ili povjerljive podatke<br>▪ implementaciju naprednih sustava Intrusion Protection Systems („**IPS**") konfiguriranih za nadziranje i aktivno zaustavljanje gubitka podataka<br>▪ u slučaju probijanja sustava, zahtijeva analizu sustava kako bi se osiguralo rješavanje i svih zaostalih ranjivosti<br>▪ opisivanje potrebnih postupaka za nadzor alata za otkrivanje kompromitacije sustava<br>▪ uspostavljanje odgovora na incident i izvođenje postupka upravljanja kad se otkrije događaj probijanja podataka i<br>▪ zahtijeva komunikaciju (za sve zaposlenike dobavljača i podizvođače koji više nisu dio Izvedbe dobavljača) u vezi neovlaštenog preuzimanja i upotrebe Microsoftovih osobnih ili povjerljivih podataka. | Dokumentirani DLP program primijenjen s postupcima na mjestu kako bi se spriječilo ometanje, gubitak i druga neovlaštena aktivnost (i minimalno sve stavke navedene u ovom odjeljku). |
| 43 | Odmah prenijeti rezultate istrage odgovora na incident višem menadžmentu i tvrtki Microsoft. | Sustavi i postupci tu su da prenesu rezultate istrage odgovora na incident tvrtki Microsoft. |
| 44 | Administratori sustava, radno osoblje, menadžment i treće strane moraju proći godišnju obuku o sigurnosti. | Uspostaviti program obuke o sigurnosti koji obuhvaća sljedeće:<br>▪ godišnja obuka o reagiranju na incident i<br>▪ simulirani događaji i automatizirani mehanizmi za omogućavanje učinkovitog reagiranja na krizne situacije.<br>▪ Svijest o sprječavanju incidenata, kao što su rizici povezani s preuzimanjem zlonamjernog softvera. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak J: Sigurnost (nast.)** | |
| 45 | Dobavljač mora osigurati da se postupcima planiranja sigurnosnog kopiranja zaštite Microsoftovi osobni i povjerljivi podaci od neovlaštenog korištenja, pristupa, otkrivanja, izmjene i uništenja. | Dobavljač može pokazati dokumentirane postupke odgovora i obnove s pojedinostima o tome kako će organizacija upravljati negativnim događajem i očuvati sigurnost svojih podataka na unaprijed utvrđenoj razini temeljnoj na ciljevima kontinuiteta sigurnosti podataka koje je odobrilo vodstvo.<br><br>Dobavljač može pokazati da ima definirane i implementirane postupke za povremeno sigurnosno kopiranje, sigurnu pohranu i učinkovitu obnovu kritičnih podataka. |
| 46 | Uspostaviti i testirati poslovni kontinuitet i planove o obnovi u slučaju katastrofe. | Plan o obnovi nakon katastrofe mora sadržavati sljedeće.<br>▪ Definirani kriteriji za utvrđivanje je li sustav kritičan za rad dobavljačevog poslovanja.<br>▪ Popis kritičnih sustava na temelju definiranih kriterija koji se moraju ciljati za obnovu u slučaju katastrofe.<br>▪ Definirani postupak obnove nakon katastrofe za svaki kritičan sustav koji osigurava inženjera koji ne zna da sustav može oporaviti aplikaciju u manje od 72 sata.<br>▪ Godišnje (ili češće) testiranje i pregled planova za obnovu nakon katastrofe kako bi se osiguralo ispunjavanje ciljeva obnove. |
| 47 | Potvrdite identitet pojedinca prije nego što mu odobrite pristup Microsoftovim osobnim ili povjerljivim podacima i osigurajte da je pristup ograničen na određeni opseg aktivnosti pojedinca koji je dopušten za podržavanje Izvedbe. | Osigurati da su svi korisnički ID-jevi jedinstveni i da svaki ima metodu autentifikacije industrijskog standarda, kao što je Azure Active Directory.<br><br>Povišen pristup (administrativni ili druge vrste poboljšanih privilegija) mora zahtijevati upotrebu drugog faktora, kao što je autentifikator na temelju pametne kartice ili telefona.<br><br>Dokumentirani sigurnosni program o informacijama koji pokriva postupak kako bi se osiguralo da pristup zaposlenika dobavljača i podizvođača Microsoftovim osobnim ili povjerljivim podacima nije veći ili dulji od onoga što je potrebno za podršku Izvedbe. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak J: Sigurnost (nast.)** | |
| 48 | Dobavljač mora zaštititi sve obrađene podatke u vezi s Izvedbom u tranzitu između mreža putem šifriranja koristeći Transport Layer Security („**TLS**") ili Internet Protocol Security („**IPsec**").<br><br>Ove su metode opisane u NIST 800-52 i NIST 800-57; može se koristiti i ekvivalentni industrijski standard.<br><br>Dobavljač mora odbiti isporuku Microsoftovih osobnih ili povjerljivih podataka koje se prenose nešifriranim putovima. | Postupak izrade, primjene i zamjene TLS-a ili drugih certifikata mora biti definiran i primjenjivati se. |
| 49 | Svi uređaji dobavljača (prijenosna računala, radne stanice itd.) koji će pristupati ili rukovati Microsoftovim osobnim ili povjerljivim podacima moraju koristiti enkripciju na temelju diska. | Šifriranje svih uređaja da udovoljava Bitlockeru ili drugom rješenju šifriranja diska industrijskog ekvivalenta za sve klijentske uređaje koji se koriste za rukovanje Microsoftovim osobnim ili povjerljivim podacima. |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | **Odjeljak J: Sigurnost (nast.)** | |
| 50 | Moraju postojati sustavi i postupci (koji koriste aktualne industrijske standarde, poput onih opisanih u standardu NIST 800-111 kako bi se šifrirali u mirovanju (kad su pohranjeni) bilo koji i svi Microsoftovi osobni i/ili povjerljivi podaci, uključujući bilo što ili sve od sljedećeg:<br>▪ podatke vjerodajnica (npr. korisničko ime/lozinke)<br>▪ podatke o instrumentima plaćanja (npr. brojevi kreditnih kartica ili bankovnih računa)<br>▪ osobni podaci povezani s imigracijom<br>▪ podaci medicinskog profila (npr. brojevi medicinskog zapisa ili biometrijski markeri ili identifikatori, kao što su DNK, otisci prsta, mrežnica i dužica oka, glasovni uzorci, uzorci lica i mjere ruke, koji se koriste u svrhu autentifikacije)<br>▪ podaci o službenom identifikacijskom broju (npr. OIB ili broj vozačke dozvole)<br>▪ podaci koji pripadaju Microsoftovim korisnicima (e.g., SharePoint, O365 dokumenti, korisnici OneDrivea)<br>▪ materijal povezan s nenajavljenim Microsoftovim proizvodima<br>▪ datum rođenja<br>▪ podaci o profilu djeteta<br>▪ geografski podaci u stvarnom vremenu<br>▪ fizička privatna adresa (koja nije poslovna)<br>▪ privatni brojevi telefona (koji nisu poslovni)<br>▪ vjeroispovijest<br>▪ politička stajališta<br>▪ seksualna orijentacija/preferenca<br>▪ odgovori na sigurnosno pitanje (npr. 2fa, poništavanje lozinke)<br>▪ majčino djevojačko prezime. | Provjerite da su Microsoftovi osobni i povjerljivi podaci navedeni u ovom retku šifrirani u mirovanju. |
| 51 | Kad se obrađuju kreditne kartice u ime Microsofta, treba se pridržavati primjenjivih standarda za rukovanje kreditnim karticama izdavača kartice. | Pokazati usklađenost pružanjem godišnje certifikacije Payment Card Industry Data Services Standard („**PCI-DSS**”).<br><br>*Poslati SSPA-u certifikate PCI DSS.* |

| # | Microsoftovi zahtjevi za zaštitu podataka o dobavljačima | Dokaz o usklađenosti |
|---|---|---|
| | Odjeljak J: Sigurnost (nast.) | |
| 52 | Dobavljač mora pohraniti Microsoftove fizičke uređaje u okruženju s kontroliranim pristupom. | Sustavi i postupci tu su za upravljanje fizičkim pristupom digitalnim, tiskanim, arhivskim i sigurnosnim kopijama Microsoftovih podataka.<br>Potrebno je slijediti lanac nadležnosti za premještaje i uništavanje fizičkih medija koji sadrže Microsoftove podatke. |
| 53 | Učiniti anonimnim sve Microsoftove osobne podatke koji se koriste u okruženju za razvoj ili testiranje. | Microsoftovi osobni podaci ne smiju se koristiti u okruženjima za razvoj ili testiranje; ako ne postoji alternativa, moraju se na odgovarajući način učiniti anonimnima kako bi se spriječila identifikacija Subjekata podataka ili zloupotreba osobnih podataka.<br><br>Napomena: anonimni podaci razlikuju se od pseudoanonimnih podataka. Anonimni podaci jesu podaci koji se ne povezuju s identificiranom fizičkom osobom ili koja se može identificirati, gdje subjekt osobnih podataka više nije prepoznatljiv. |