Microsoftove zahteve za varstvo podatkov za dobavitelje

Ustreznost

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

- Ob navzkrižju med zahtevami v tem dokumentu in zahtevami, navedenimi v pogodbah med dobaviteljem in Microsoftom, se uporabljajo ZVP, razen če upoštevni dobavitelj v obrazcu s potrditvijo o skladnosti z ZVP navede pravilno določilo pogodbe, ki je v navzkrižju z upoštevnim razdelkom ZVP (v tem primeru imajo prednost določila pogodbe).
- Ob navzkrižju med zahtevami v tem dokumentu in morebitnimi pravnimi ali zakonskimi zahtevami se uporabljajo pravne ali zakonske zahteve.
- Če ima Microsoftov dobavitelj vlogo upravljavca na podlagi teh ZVP, veljajo za dobaviteljeve dejavnosti obdelave samo zahteve v razdelku J (Varnost) in razdelku A (Upravljanje).
- Če Microsoftov dobavitelj v okviru teh ZVP ne obdeluje Microsoftovih osebnih podatkov, temveč samo Microsoftove zaupne podatke, veljajo za dobaviteljevo obdelavo Microsoftovih zaupnih podatkov samo zahteve v razdelkih A (Upravljanje), E (Hranjenje) in J (Varnost).

Mednarodni prenos podatkov

Dobavitelj brez omejevanja svojih drugih obveznosti ne bo izvedel mednarodnega prenosa Microsoftovih osebnih podatkov, razen če ima Microsoftovo prejšnje pisno soglasje, in bo v vseh primerih ravnal skladno z zahtevami za varstvo podatkov v morebitnih standardnih pogodbenih določilih, zavezujočih pravilih podjetja ali drugih shemah, ki jih je odobril kateri koli urad za varstvo podatkov, Evropski odbor za varstvo podatkov ali Evropska komisija ter jih je Microsoft sprejel oziroma se strinja z njimi, med drugim tudi vključno z dogovorom EU in ZDA ter Švice in ZDA o okviru t. i. varnostnega ščita ter splošno uredbo EU o varstvu podatkov. Dobavitelj se strinja, da bo Microsoft obvestil, če ugotovi, da ne more več izpolnjevati svojih obveznosti, da zagotovi isto raven zaščite, kot jo zahtevajo načela varnostnega ščita. Dobavitelj prav tako zagotavlja, da bodo tako ravnali tudi morebitni in vsi njegovi nasledniki (kot je to opredeljeno v klavzuli 1(d) standardnih pogodbenih klavzul iz leta 2010, objavljenih kot priloga odločitvi Evropske komisije C(2010)593).

Pomembne definicije

Naslednji pojmi, opredeljeni v teh ZVP, imajo naslednje pomene. Seznami primerov po besedah »vključno z«, »kot je/so«, »npr.«, »na primer« ali podobnih, ki se uporabljajo po celotnih teh ZVP, se razlagajo, kot da vključujejo »brez omejitve« ali »vendar ne omejeno na«, razen če je drugače določeno z besedami, kot sta »samo« ali »izključno«.

»**Microsoftovi osebni podatki**« pomeni vse osebne podatke, ki jih obdela Microsoft ali se obdelajo v njegovem imenu.

»**Microsoftovi zaupni podatki**« so vsi podatki, ki bi lahko povzročili znatno škodo Microsoftovemu ugledu ali finančno izgubo zanj, če bi bila ogrožena njihova zaupnost ali celovitost. To vključuje Microsoftove izdelke strojne in programske opreme, interno poslovno programsko opremo, predizdajno trženjsko gradivo, licenčne ključe za izdelke in tehnično dokumentacijo, povezano z Microsoftovimi izdelki in storitvami.

»**Obdelava**« pomeni vsak avtomatiziran ali neavtomatiziran postopek ali niz postopkov, ki se izvajajo na morebitnih Microsoftovih osebnih ali zaupnih podatkih, kot so zbiranje, beleženje, urejanje, strukturiranje, shranjevanje,

prilagajanje ali spreminjanje, pridobivanje, posvetovanje, uporaba, razkritje s prenosom, širjenje ali drugo razpolaganje, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje. Pojma »obdelava« in »obdelano« imata ustrezne pomene.

»**Obdelovalec**« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki v imenu upravljavca obdeluje osebne podatke.

»**Osebni podatki**« pomeni vse podatke, ki se nanašajo na določeno ali določljivo fizično osebo (»**oseba, na katero se nanašajo osebni podatki**«); določljiva fizična oseba je oseba, ki jo je mogoče neposredno ali posredno identificirati, zlasti s sklicevanjem na identifikator, kot so ime, identifikacijska številka, lokacijski podatki ali spletni identifikator, oziroma na enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, ekonomsko, kulturno ali družbeno identiteto te fizične osebe.

»**Podatkovni vdor**« pomeni ogrozitev varnosti, ki ima za posledico nenamerno ali nezakonito uničenje, izgubo, spreminjanje ali nepooblaščeno razkritje osebnih podatkov ali Microsoftovih zaupnih podatkov, ki se prenašajo, shranjujejo ali drugače obdelujejo, oziroma dostop do njih.

»**Pravica osebe, na katero se nanašajo osebni podatki**« pomeni pravico osebe, na katero se nanašajo osebni podatki, do dostopa do njenih Microsoftovih osebnih podatkov, njihovega izbrisa, urejanja, izvoza ali omejevanja in ugovora obdelavi, če to zahteva zakonodaja.

»**Upravljavec**« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samostojno ali skupaj z drugimi določa namene in načine obdelave osebnih podatkov; če namene in načine obdelave določajo Evropska unija (»**EU**«) ali zakoni držav članic, lahko upravljavca (ali merila za imenovanje upravljavca) določajo ti zakoni.

»**Zakonodaja**« pomeni vse upoštevne zakone, pravila, zakonike, odredbe, odločbe, naloge, predpise, razsodbe, kodekse, uveljavitve, resolucije in zahteve katerega koli pristojnega državnega organa (zveznega, državnega, lokalnega ali mednarodnega). »**Nezakonito**« pomeni vsako kršitev zakona.

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek A: Upravljanje		
1	Vsaka upoštevna pogodba med Microsoftom in dobaviteljem (npr. krovna pogodba, delovni nalog, naročilnice in druga naročila) vsebuje besedilo o varstvu zasebnosti in varnosti podatkov, ki se nanaša na Microsoftove zaupne in osebne podatke, kjer je primerno. Za podjetja, ki delujejo kot obdelovalci, mora pogodba vsebovati predmet in trajanje obdelave, način in namen obdelave, vrsto Microsoftovih osebnih podatkov in kategorij oseb, na katere se nanašajo osebni podatki, ter Microsoftove pravice in obveznosti.	Dobavitelj mora predložiti upoštevno pogodbo med Microsoftom in dobaviteljem. Za obdelovalce so opisi obdelave vključeni v upoštevni pogodbi (*npr.* delovnem nalogu, naročilnicah). Opomba: Podjetja s sprotnimi naročilnicami lahko potrebne opise dejavnosti obdelave dodajo pozneje v postopku nakupovanja.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
2	Dobavitelj mora imenovati osebo ali skupino v podjetju, ki ima obveznost in odgovornost za zagotavljanje skladnosti z ZVP.	Ime osebe ali skupine, zadolžene za zagotavljanje skladnosti z ZVP za Microsoftovega dobavitelja. Dokument, ki opisuje avtoriteto in odgovornost te osebe ali skupine, ki dokazuje vlogo na področju zasebnosti in/ali varnosti.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
3	Vzpostaviti, vzdrževati in izvajati letna usposabljanja glede zasebnosti za zaposlene, ki bodo imeli dostop do Microsoftovih osebnih ali zaupnih podatkov. Če vaše podjetje nima pripravljene vsebine, lahko uporabite ta osnutek in ga prilagodite za svoje podjetje.	Na voljo so letne evidence prisotnosti. Izobraževalna vsebina vključuje načela glede zasebnosti in varnosti.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
4	Obdelati Microsoftove osebne podatke samo v skladu z Microsoftovimi dokumentiranimi navodili, vključno z navodili glede prenosov Microsoftovih osebnih podatkov v tretjo državo ali mednarodno organizacijo, razen če to zahteva zakonodaja. V tem primeru obdelovalec (dobavitelj) pred obdelavo upravljavca (Microsoft) obvesti o tej pravni zahtevi, razen če zakonodaja na podlagi pomembnega javnega interesa prepoveduje tako obveščanje.	Dokumentirana dokazila o navodilih, kot so določena v pogodbi (npr. delovni nalog ali naročilnica) oziroma evidentirana v elektronskem sistemu, uporabljenem za zagotavljanje storitev.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek B: Obvestilo		
5	Dobavitelj mora pri zbiranju osebnih podatkov v Microsoftovem imenu uporabiti Microsoftovo izjavo o zasebnosti. Obvestilo o zasebnosti mora biti očitno in na voljo osebam, na katere se nanašajo osebni podatki, tako da se lahko določijo, ali želijo dobavitelju razkriti svoje osebne podatke. Opomba: Če je vaše podjetje upravljavec dejavnosti obdelave, morate objaviti svoje obvestilo o zasebnosti. *Za dostop do pravilnih Microsoftovih obvestil se obrnite na SSPAHelp@microsoft.com.*	Dobavitelj uporablja povezavo za posredovanje do Microsoftove trenutne objavljene izjave o zasebnosti. Izjava o zasebnosti je objavljena v vsakem kontekstu, kjer se bodo zbirali osebni podatki uporabnika. Če je primerno, je na voljo nespletna različica, in sicer pred zbiranjem podatkov. Morebitne uporabljene nespletne izjave o zasebnosti so najnovejša objavljena različica in ustrezno opremljene z datumom. Za Microsoftove storitve za zaposlene se uporablja Microsoftovo obvestilo o varstvu podatkov.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
6	Dobavitelji morajo biti pri zbiranju Microsoftovih osebnih podatkov prek glasovnega klica v živo ali posnetega klica pripravljeni osebam, na katere se nanašajo osebni podatki, pojasniti upoštevne postopke zbiranja podatkov, ravnanja z njimi, njihove uporabe in hranjenja.	Skript za glasovne posnetke vključuje, kako se obdelujejo Microsoftovi osebni podatki, ter ▪ zbiranje, ▪ uporabo in ▪ hranjenje.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek C: Izbira in soglasje		
7	Kjer dobavitelj uporablja soglasje kot pravno podlago za obdelavo podatkov, mora pred zbiranjem osebnih podatkov osebe, na katero se nanašajo osebni podatki, pridobiti in zabeležiti njeno soglasje za vse svoje dejavnosti obdelave (vključno z morebitnimi novimi in posodobljenimi dejavnostmi obdelave).	Dobavitelj lahko dokaže, kako da oseba, na katero se nanašajo osebni podatki, soglasje za dejavnost obdelave in da obseg soglasja pokriva dobaviteljeve dejavnosti obdelave osebnih podatkov osebe, na katero se nanašajo osebni podatki. Dobavitelj lahko dokaže, kako oseba, na katero se nanašajo osebni podatki, umakne soglasje za dejavnost obdelave. Dobavitelj lahko dokaže, kako se pred začetkom nove dejavnosti obdelave preverjajo prednostne nastavitve. Dobavitelj spremlja učinkovitost upravljanja prednostnih nastavitev, da zagotovi, da je časovni okvir za upoštevanje spremembe prednostne nastavitve najbolj omejujoča veljavna lokalna pravna zahteva. Opomba: Dokazila so lahko posnetki zaslona interakcij z uporabniki, preskušanje storitve ali priložnost za ogled tehnične dokumentacije.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek C: Izbira in soglasje (nadaljevanje)		
8	Piškotki so majhne besedilne datoteke, ki jih spletna mesta in/ali aplikacije shranijo v napravah in vsebujejo podatke, uporabljene za prepoznavanje osebe, na katero se nanašajo osebni podatki, ali naprave. Dobavitelji, ki ustvarjajo in upravljajo Microsoftova spletna mesta in/ali aplikacije, morajo osebam, na katere se nanašajo osebni podatki, zagotoviti pregledno obvestilo in izbiro glede uporabe piškotkov. Dobavitelji, ki ustvarjajo in upravljajo Microsoftova spletna mesta in/ali aplikacije, morajo poskrbeti, da je uporaba piškotkov usklajena z zavezami v Microsoftovi izjavi o zasebnosti in lokalnimi pravnimi zahtevami, na primer s pravili, ki jih je določila EU.	Namen vsakega piškotka mora biti dokumentiran in opisovati vrsto uporabljenega piškotka. ▪ Če zadostujejo sejni piškotki, ni dovoljeno uporabiti trajnih piškotkov. ▪ Če se uporabljajo trajni piškotki, morajo imeti datum poteka, ki ne presega 2 let po uporabnikovem obisku spletnega mesta. Za uporabnike v EU datum poteka za trajne piškotke ne sme presegati 13 mesecev. Potrditev skladnosti z upoštevnimi zakoni EU, kot sta ▪ uporaba dogovora glede označevanja – »Zasebnost in piškotki« – za izjavo o zasebnosti; in ▪ zagotavljanje pozitivnega soglasja uporabnika pred uporabo piškotkov za »nenujne« namene, kot je oglaševanje.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek D: Prevzem		
9	Dobavitelj mora spremljati zbiranje Microsoftovih osebnih in/ali zaupnih podatkov, da se zagotovi zbiranje samo tistih podatkov, ki so potrebni za izvajanje.	Dobavitelj lahko priskrbi dokumentacijo, ki prikazuje, da so zbrani Microsoftovi osebni in/ali zaupni podatki potrebni za izvajanje.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
10	Če dobavitelj v Microsoftovem imenu zbira osebne podatke od tretjih oseb, mora potrditi, da so pravilniki in postopki za varovanje podatkov pri teh tretjih osebah skladni z dobaviteljevo pogodbo z Microsoftom in ZVP.	Dobavitelj lahko priskrbi dokumentacijo, da je bil izveden skrbni pregled pravilnikov in postopkov za varstvo podatkov pri tretji osebi.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
11	Pred zbiranjem Microsoftovih osebnih podatkov z namestitvijo ali uporabo izvedljive programske opreme v računalniku osebe, na katero se nanašajo osebni podatki, je treba potrebo za zbiranje teh podatkov dokumentirati v dobaviteljevi pogodbi, sklenjeni z Microsoftom.	Microsoftovo soglasje k uporabi izvedljive programske opreme v napravi osebe, na katero se nanašajo osebni podatki, je navedeno v sklenjeni pogodbi.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
12	Pred zbiranjem občutljivih Microsoftovih osebnih podatkov (podatkov, ki razkrivajo rasno ali etnično poreklo, politična mnenja, verske ali filozofske poglede ali pripadnost v sindikatu, genetske podatke, biometrične podatke, podatke o zdravju ali spolnem življenju ali usmeritvi fizične osebe) je treba potrebo za zbiranje Microsoftovih osebnih podatkov dokumentirati v dobaviteljevi pogodbi, sklenjeni z Microsoftom.	V pogodbi, sklenjeni z Microsoftom, je navedena nujnost zbiranja občutljivih Microsoftovih osebnih podatkov.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek E: Hranjenje		
13	Poskrbeti, da se Microsoftovi osebni in zaupni podatki hranijo samo tako dolgo, kot je potrebno za izvajanje, razen če nadaljnje hranjenje Microsoftovih osebnih in/ali zaupnih podatkov zahteva zakonodaja.	Dobavitelj mora ravnati skladno z dokumentiranimi pravilniki za hranjenje podatkov ali zahtevami za hranjenje, ki jih Microsoft določi v pogodbi (npr. v delovnem nalogu ali naročilnici).	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*
14	Poskrbeti, da se vsi Microsoftovi osebni ali zaupni podatki, ki jih ima dobavitelj ali so pod njegovim nadzorom, po Microsoftovi izključni presoji vrnejo Microsoftu ali uničijo takrat, ko je izvajanje opravljeno, ali na Microsoftovo zahtevo. V programih morajo biti uveljavljeni postopki zagotavljanja, da so podatki, ki jih iz programa izrecno odstranijo uporabniki ali so odstranjeni na podlagi drugih sprožilnikov, kot je starost podatkov, varno izbrisani. Ko je potrebno uničenje Microsoftovih osebnih ali zaupnih podatkov, mora dobavitelj zažgati, zdrobiti ali razrezati fizična sredstva, ki vsebujejo Microsoftove osebne in/ali zaupne podatke, da podatkov ni več mogoče prebrati ali znova sestaviti.	Imeti evidence o predaji Microsoftovih osebnih in zaupnih podatkov (to lahko vključuje vračilo Microsoftu v uničenje). Če je potrebno uničenje ali ga zahteva Microsoft, mora priskrbeti potrdilo o uničenju, ki ga podpiše član dobaviteljeve uprave.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek F: Osebe, na katere se nanašajo osebni podatki		
	Osebe, na katere se nanašajo osebni podatki, imajo pravico do dostopa do svojih osebnih podatkov, njihovega izbrisa, urejanja, izvažanja in omejevanja ter pravico nasprotovati njihovi obdelavi (»**pravice oseb, na katere se nanašajo osebni podatki**«). Ko želi oseba, na katero se nanašajo osebni podatki, uveljaviti svoje zakonske pravice glede Microsoftovih osebnih podatkov, mora dobavitelj:		
15	Kolikor je mogoče, Microsoftu z ustreznimi tehničnimi in organizacijskimi ukrepi pomagati izpolniti obveznosti, da se odzove na zahteve oseb, na katere se nanašajo osebni podatki, za uveljavitev njenih pravic.	Vpeljani so postopki in procesi za podporo uveljavljanja pravic osebe, na katero se nanašajo osebni podatki.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
16	Se na vse zahteve oseb, na katere se nanašajo osebni podatki, odzvati brez nepotrebnih zamud.	Dobavitelj izvaja občasne preskuse, da zagotovi, da lahko podpira pravice oseb, na katere se nanašajo osebni podatki.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
17	Če Microsoft ne zahteva drugače, bo dobavitelj vse osebe, na katere se nanašajo osebni podatki, ki se obrnejo neposredno nanj, napotil neposredno na Microsoft, da uveljavijo svoje pravice oseb, na katere se nanašajo osebni podatki. Dobavitelj bo osebo, na katero se nanašajo osebni podatki, obvestil o korakih, ki so potrebni za dostop do Microsoftovih osebnih podatkov, povezanih z njo, ali drugačno uveljavljanje pravic, povezanih z njimi. *Za pomoč s to zahtevo se obrnite na SSPAHelp@microsoft.com.*	Dobavitelj obvesti o postopku, potrebnem za dostop do osebnih podatkov, in načinih, ki so na voljo za posodobitev teh podatkov.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
18	Pri odgovarjanju neposredno osebi, na katero se nanašajo osebni podatki in ki predloži zahtevo, preveril njeno identiteto.	Dobavitelj je dokumentiral način, uporabljen za prepoznavanje Microsoftovih oseb, na katere se nanašajo osebni podatki.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek F: Osebe, na katere se nanašajo osebni podatki (nadaljevanje)		
	Ko je preverjena pristnost osebe, na katero se nanašajo osebni podatki, mora dobavitelj:		
19	Ugotoviti, ali ima oziroma nadzira Microsoftove osebne podatke o zadevni osebi, na katero se nanašajo osebni podatki.	Dobavitelj ima vzpostavljene postopke za ugotavljanje, ali se hranijo osebni podatki.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
20	Razumno poskuša ugotoviti, kje so zahtevani Microsoftovi osebni podatki, ter poskrbeti za evidence, ki zadostno dokazujejo, da se je razumno potrudil pri iskanju.	Dobavitelj ima evidence, ki dokazujejo postopke, sprejete za izpolnjevanje zahtev oseb, na katere se nanašajo osebni podatki. Dokumentacija vključuje: ▪ datum in uro zahteve; ▪ ukrepe, izvedene kot odziv na zahtevo; in ▪ evidenco o tem, kdaj je bil Microsoft obveščen.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
21	Zabeleži datum in uro zahtev oseb, na katere se nanašajo osebni podatki, in ukrepov, ki jih je izvedel na podlagi takih zahtev. Microsoftu na zahtevo priskrbeti evidenco o zahtevah osebe, na katero se nanašajo osebni podatki, za dostop.	Dobavitelj hrani evidenco o zahtevah za dostop in dokumentira spremembe osebnih podatkov.	
	Ko je preverjena pristnost osebe, na katero se nanašajo osebni podatki, in je dobavitelj preveril, ali ima Microsoftove osebne podatke, mora:		
22	Za zahteve za pridobitev kopije osebnih podatkov osebi, na katero se nanašajo osebni podatki, v ustrezni tiskani, elektronski ali ustni obliki zagotoviti Microsoftove osebne podatke.	Dobavitelj osebi, na katero se nanašajo osebni podatki, zagotovi osebne podatke v obliki, ki je razumljiva in priročna tako za osebo, na katero se nanašajo osebni podatki, kot tudi za dobavitelja.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek F: Osebe, na katere se nanašajo osebni podatki (nadaljevanje)		
23	Osebi, na katero se nanašajo osebni podatki, ob zavrnitvi zahteve po Microsoftovi presoji zagotoviti pisno pojasnilo, ki je dosledno z morebitnimi prejšnjimi navodili Microsofta. *Za pomoč s to zahtevo se obrnite na SSPAHelp@microsoft.com.*	Dokumentirati primere, ko so zahteve zavrnjene, ter hraniti dokazila o Microsoftovem pregledu in odobritvi.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
24	Dobavitelj si mora razumno prizadevati zagotoviti, da se Microsoftovi osebni podatki, izdani osebi, na katero se nanašajo osebni podatki, ne uporabijo za prepoznavanje nekoga drugega.	Dobavitelj mora dokazati, da so uveljavljeni ustrezni previdnostni ukrepi, ki preprečujejo, da bi bilo iz izdanih podatkov mogoče prepoznati nekoga drugega (npr. ne sme fotokopirati celotne strani podatkov, če so zahtevani podatki za osebo, na katero se nanašajo osebni podatki, v samo eni vrstici).	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
25	Če se oseba, na katero se nanašajo osebni podatki, in dobavitelj ne strinjata glede tega, ali so Microsoftovi osebni podatki popolni in točni, mora dobavitelj zadevo poslati v obravnavo Microsoftu in z njim sodelovati, kot je potrebno za rešitev težave. *Za pomoč s to zahtevo se obrnite na SSPAHelp@microsoft.com.*	Dobavitelj dokumentira primere nesoglasij in težavo prenese v obravnavo Microsoftu.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek G: Razkritje tretjim osebam		
	Če namerava dobavitelj za obdelavo Microsoftovih osebnih ali zaupnih podatkov uporabiti podizvajalca, mora:		
26	Pridobiti Microsoftovo izrecno pisno soglasje pred oddajo storitev v izvajanje podizvajalcem ali izvajanjem kakršnih koli sprememb, povezanih z dodajanjem ali zamenjavo podizvajalcev. *Za pomoč s to zahtevo se obrnite na SSPAHelp@microsoft.com.*	Potrditi, da Microsoftove osebne podatke obdelujejo samo podjetja, ki jih Microsoft pozna, kot to zahteva upoštevna pogodba (npr. delovni nalog, dodatek, naročilnica) oziroma je navedeno v zbirki podatkov SSPA.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
27	Dokumentirati vrsto in obseg Microsoftovih osebnih in zaupnih podatkov, ki jih bodo nadalje obdelali podizvajalci, ter zagotoviti, da so zbrani podatki potrebni za izvajanje storitev.	Dobavitelj mora imeti dokumentacijo o Microsoftovih osebnih in zaupnih podatkih, razkritih ali prenesenih podizvajalcem.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
28	Poskrbeti, da podizvajalec Microsoftove osebne podatke uporablja skladno z deklariranimi nastavitvami obveščanja osebe, na katero se nanašajo osebni podatki.	Dokazati, kako podizvajalci uporabljajo prednostno nastavitev Microsoftove osebe, na katero se nanašajo osebni podatki. Zagotoviti podporno dokumentacijo, ki vključuje časovni okvir, v katerem mora podizvajalec izpolniti spremembo prednostne nastavitve.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
29	Omejiti podizvajalčevo obdelavo Microsoftovih osebnih podatkov na namene, potrebne za izpolnjevanje dobaviteljeve pogodbe z Microsoftom.	Dobavitelj lahko priskrbi dokumentacijo, ki prikazuje, da so Microsoftovi osebni podatki, posredovani podizvajalcu, potrebni za izvajanje.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
30	Preveriti, ali morebitne pritožbe kažejo na nedovoljeno ali nezakonito obdelavo Microsoftovih osebnih podatkov.	Dobavitelj lahko dokaže, da so vzpostavljeni sistemi in postopki za odzivanje na pritožbe glede podizvajalčeve nepooblaščene uporabe ali razkritja Microsoftovih osebnih podatkov.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek G: Razkritje tretjim osebam (nadaljevanje)		
31	Microsoft nemudoma obvestiti, če izve, da je podizvajalec Microsoftove osebne ali zaupne podatke obdelal za kakršen koli namen, razen izvajanja.	Dobavitelj je zagotovil navodila in način, na podlagi katerih lahko podizvajalec prijavi napačno uporabo Microsoftovih podatkov.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*
32	Nemudoma ukrepati za odpravljanje morebitne dejanske ali potencialne škode, ki jo povzroči podizvajalčeva nepooblaščena ali nezakonita obdelava Microsoftovih osebnih in zaupnih podatkov.	Dobavitelj lahko dokaže, da ima vpeljane načrt in postopke za primer, da podizvajalec napačno uporabi Microsoftove osebne in zaupne podatke.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*
	Razdelek H: Kakovost		
33	Dobavitelj mora zagotoviti celovitost vseh Microsoftovih osebnih podatkov ter poskrbeti, da so točni, popolni in relevantni za navedene namene, za katere se obdelujejo.	Dobavitelj lahko dokaže, da so vpeljani postopki za preverjanje Microsoftovih osebnih podatkov, ko se zbirajo, ustvarjajo in posodabljajo. Dobavitelj lahko dokaže, da so vzpostavljeni postopki za spremljanje in vzorčenje za sprotno preverjanje točnosti podatkov in njihovo popravljanje, če je potrebno.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek I: Spremljanje in uveljavljanje		
34	Dobavitelj ima načrt odzivanja na izredne dogodke, ki določa, da mora dobavitelj Microsoft nemudoma obvestiti, ko izve za podatkovni vdor ali varnostno ranljivost, povezano z dobaviteljevim ravnanjem z Microsoftovimi osebnimi ali zaupnimi podatki. *Dogodek prijavite na: SSPAHelp@microsoft.com.*	Dobavitelj ima načrt odzivanja na izredne dogodke, ki vključuje korak za obveščanje strank (Microsofta), kot je opisano v tem razdelku.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
35	Ne sme izdati nobenih obvestil za tisk ali kakršnega koli drugega javnega obvestila, ki se nanaša na podatkovni vdor, povezan z Microsoftovimi osebnimi ali zaupnimi podatki, ne da bi za to dobil Microsoftovo odobritev, razen če to zahteva zakonodaja.	Dobavitelj se strinja, da bo v primeru dogodka izpolnil to zahtevo.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
36	Mora uvesti načrt odpravljanja posledic podatkovnih vdorov in ranljivosti, povezanih z Microsoftovimi osebnimi ali zaupnimi podatki, ter spremljati odpravljanje, da se zagotovi pravočasna izvedba ustreznih korektivnih ukrepov.	Dobavitelj ima dokumentirane postopke, s katerimi se bo odzval za ustavitev podatkovnega vdora.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
37	Vzpostaviti mora formalni pritožbeni postopek za odzivanje na vse pritožbe glede varovanja podatkov, povezane z Microsoftovimi osebnimi podatki.	Dobavitelj ima način za prejemanje pritožb glede Microsoftovih osebnih podatkov in ima dokumentiran pritožbeni postopek za obravnavo pritožb.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost		
	Dobavitelj mora vzpostaviti, uvesti in izvajati program informacijske varnosti, ki vključuje pravilnike in postopke za zaščito in varovanje Microsoftovih osebnih in zaupnih podatkov skladno z dobrimi praksami v panogi in kot to zahteva zakonodaja. Dobaviteljev varnostni program mora ustrezati standardom, navedenim spodaj, zahteve 38–56.	Varnostni ukrepi lahko presegajo navedene, če je to potrebno zaradi predpisov (npr. HIPAA, GLBA) ali pogodbenih zahtev. Veljavno poročilo ISO 27001 ali SOC 2 z varnostjo je sprejemljiv nadomestek za razdelek J. Za uveljavljanje tega nadomestka se obrnite na SSPAHelp@microsoft.com. Opomba: Zagotoviti boste morali dokumentacijo, ki opisuje obseg teh potrdil/poročil.	
38	Izvesti letna ocenjevanja omrežne varnosti, ki vključujejo: ▪ pregled večjih sprememb okolja, kot so nove sistemske komponente, omrežna topologija in pravila požarnega zidu; ▪ izvajanje iskanj ranljivosti; in ▪ vodenje dnevnikov sprememb.	Dobavitelj je dokumentiral ocenjevanja omrežij, dnevnikov sprememb in rezultatov pregledov. Zahtevani dnevniki sprememb morajo slediti spremembe, vsebovati informacije o razlogih za spremembe ter ime in naziv imenovanega odobritelja sprememb.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
39	Dobavitelj mora opredeliti, objaviti in uvesti pravilnik za mobilne naprave, ki varuje in omejuje uporabo Microsoftovih osebnih ali zaupnih podatkov, do katerih se dostopa iz mobilne naprave ali se jih v njej uporablja.	Dobavitelj dokaže uporabo skladnega pravilnika za mobilne naprave, kjer je za obdelavo Microsoftovih osebnih ali zaupnih podatkov potrebna uporaba mobilne naprave.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost (nadaljevanje)		
40	Vsa sredstva, uporabljena v podporo izvajanja, morajo biti evidentirana in imeti imenovanega lastnika. Dobavitelj je odgovoren za vodenje inventure teh informacijskih sredstev, vzpostavljanje sprejemljive in dovoljene uporabe sredstev ter zagotavljanje ustrezne ravni zaščite sredstev skozi njihov celoten življenjski cikel.	Izvedba inventure sredstev naprav, uporabljenih v podporo izvajanju. Inventura teh sredstev mora vključevati: ▪ lokacijo naprave; ▪ podatkovno kategorizacijo podatkov v sredstvu; ▪ evidenco o vračilu sredstev po prekinitvi zaposlitve ali poslovne pogodbe; in ▪ evidenco o odstranjevanju medijev za shranjevanje podatkov, ko več niso potrebni.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost (nadaljevanje)		
41	Vzpostaviti in ohranjati postopke upravljanja pravic do dostopa za preprečevanje nepooblaščenega dostopa do morebitnih Microsoftovih osebnih ali zaupnih podatkov, ki so pod nadzorom dobavitelja.	Dobavitelj dokaže, da je uvedel načrt za upravljanje pravic do dostopa, ki vključuje naslednje: ▪ postopke za nadzor dostopa; ▪ identifikacijske postopke; ▪ postopke za zaklepanje po neuspešnih poskusih; ▪ ponastavitev gesla tako pogosto, kot je potrebno, vendar najpozneje vsakih 90 dni; ▪ zanesljive parametre za izbiro poverilnic za preverjanje pristnosti uporabnikov; in ▪ deaktiviranje uporabniških računov najpozneje 48 ur po prekinitvi zaposlitve. Dobavitelj dokaže, da ima vpeljan postopek pregledovanja uporabniškega dostopa do Microsoftovih osebnih in zaupnih podatkov z uveljavljanjem načela najmanjše pravice. Postopek vključuje: ▪ jasno opredeljene vloge uporabnikov; ▪ postopke za pregled in utemeljitev odobritev dostopa za vloge; in ▪ preskuse, ali imajo uporabniki z vlogami, ki imajo dostop do Microsoftovih podatkov, dokumentirano utemeljitev, da so v skupini/vlogi.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost (nadaljevanje)		
42	Opredeliti in uvesti postopke za upravljanje popravkov, ki dajejo prednost varnostnim popravkom za sisteme, ki se uporabljajo za obdelavo Microsoftovih osebnih ali zaupnih podatkov. Ti postopki vključujejo: ▪ pristop z opredeljenimi tveganji za prioritizacijo varnostnih popravkov; ▪ sposobnost obravnave in uvedbe nujnih popravkov; ▪ uporabnost za operacijski sistem in strežniško programsko opremo, kot so programski strežniki in programska oprema zbirk podatkov; ▪ dokumentiranje nevarnosti, ki jo odpravlja popravek, in spremljanje morebitnih izjem; in ▪ zahteve za prenehanje uporabe programske opreme, ki je podjetje, ki jo je razvilo, ne podpira več.	Dobavitelj lahko dokaže, da je uvedel postopek za upravljanje popravkov, ki izpolnjuje to zahtevo in obsega najmanj naslednje: ▪ dodelitev resnosti, na kateri temelji prioritizacija; (Opredelitve resnosti so dokumentirane.) ▪ dokumentiran postopek za uvajanje popravkov v sili; ▪ potrditev, da niso več v uporabi operacijski sistemi, ki jih podjetje, ki jih je razvilo, ne podpira več; ▪ evidence o upravljanju popravkov, ki sledijo odobritve in izjeme.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
43	V opremo, povezano z omrežjem in uporabljeno za obdelavo Microsoftovih osebnih podatkov, vključno s strežniki ter namiznimi računalniki za delovno uporabo in usposabljanje, mora namestiti programsko opremo za zaščito pred virusi in zlonamerno programsko opremo za zaščito pred morebitnimi škodljivimi virusi in zlonamerno programsko opremo. Dnevno ali tako pogosto, kot določa dobavitelj protivirusne programske opreme oz. rešitve za preprečevanje zlonamerne programske opreme, posodobiti definicije za preprečevanje zlonamerne programske opreme. Opomba: To velja za vse operacijske sisteme, vključno z Linuxom.	Obstajajo zapisi, ki dokazujejo, da se aktivno uporablja programska oprema za preprečevanje virusov in zlonamerne programske opreme. Opomba: Ta zahteva velja za vse operacijske sisteme.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
44	Dobavitelji, ki razvijajo programsko opremo za Microsoft, morajo v postopku izdelave vključiti načela načrtovane varnosti.	Dobaviteljevi dokumenti s tehnično dokumentacijo vključujejo kontrolne točke za varnostno preverjanje v dobaviteljevih razvojnih ciklih.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost (nadaljevanje)		
45	Uporaba programa za preprečevanje izgube podatkov (»PIP«). Podatke je treba ustrezno razvrstiti, označiti in zaščititi, dobavitelj pa mora spremljati, ali v informacijskih sistemih, v katerih se obdelujejo Microsoftovi osebni ali zaupni podatki, prihaja do vdorov ali druge nepooblaščene dejavnosti. Program DLP mora izpolniti te minimalne pogoje: ▪ določati mora uporabo sistemov za odkrivanje vdorov v gostitelju, omrežju in oblaku, ki ustrezajo panožnim standardom (»**SOV**«), če hranite Microsoftove osebne ali zaupne podatke; ▪ določati mora uvedbo naprednih sistemov za odkrivanje vdorov (»**SOV**«), konfiguriranih za spremljanje in aktivno preprečevanje izgube podatkov; ▪ ob vdoru v sistem mora določati obvezno analiziranje sistema in zagotoviti, da so odpravljene tudi morebitne preostale ranljivosti; ▪ opisati mora postopke, potrebne za spremljanje orodij za zaznavanje ogrozitev sistema; in ▪ vzpostaviti mora postopek za odziv na dogodke in njihovo upravljanje, ki se izvede, ko je ugotovljen podatkovni vdor.	Uveden dokumentiran SOV/PIP z vpeljanimi postopki za neposreden odziv v primeru ugotovitve ranljivosti ali podatkovnega vdora.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
46	Hitro posredovanje rezultatov preiskave od odziva na dogodek višji upravi in Microsoftu. *Obrnite se na SSPAHelp@microsoft.com, da obvestite Microsoft.*	Vzpostavljeni morajo biti sistemi in postopki za obveščanje Microsofta o rezultatih preiskave odziva na dogodek.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
47	Sistemski skrbniki, operativno osebje, uprava in tretje osebe se morajo udeleževati letnih varnostnih usposabljanj.	Vzpostaviti mora program varnostnega usposabljanja, ki vključuje: ▪ letno usposabljanje za odziv na dogodke; in ▪ simulirane dogodke in avtomatizirane mehanizme za omogočanje učinkovitega odziva v kriznih okoliščinah. Ozaveščanje za pripravljenost na preprečevanje dogodkov, kot so	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

		nevarnosti, povezane s prenosom zlonamerne programske opreme.	

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost (nadaljevanje)		
48	Dobavitelj mora zagotoviti, da postopki za varnostno kopiranje varujejo Microsoftove osebne in zaupne podatke pred nepooblaščeno uporabo, dostopom, razkritjem, spreminjanjem in uničenjem.	Dobavitelj lahko dokumentirane postopke odziva in obnovitve dokaže s podrobnim opisom, kako bo organizacija upravljala razdiralen dogodek in zagotovila vnaprej določeno raven informacijske varnosti glede na cilje glede kontinuitete informacijske varnosti, ki jih določi uprava. Dobavitelj lahko dokaže, da je opredelil in uvedel postopke za redno varnostno kopiranje, varno shranjevanje in učinkovito obnovitev nujnih podatkov.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*
49	Vzpostaviti in preskusiti načrte neprekinjenega poslovanja in ponovne vzpostavitve po katastrofi.	Načrt ukrepanja po katastrofi mora vključevati vse od navedenega: ▪ opredeljena merila za ugotavljanje, ali je sistem nujen za delovanje dobaviteljevega poslovanja; ▪ seznam nujnih sistemov, določenih na podlagi opredeljenih meril, ki so v prvi vrsti za obnovitev v primeru katastrofe; ▪ opredeljen postopek obnovitve po katastrofi za vsak nujen sistem, ki zagotavlja, da bo lahko inženir, ki ne pozna sistema, aplikacijo obnovil v manj kot 72 urah. ▪ Letno (ali pogostejše) preskušanje in pregled načrtov za obnovitev po katastrofi, da se zagotovi, da bo mogoče izpolniti cilje obnovitve.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost (nadaljevanje)		
50	Preden posamezniku podeli dostop do Microsoftovih osebnih ali zaupnih podatkov, mora preveriti njegovo pristnost.	Poskrbeti mora, da so vsi uporabniški ID-ji edinstveni in da se za vsakega uporablja standardni način preverjanja pristnosti, kot je Azure Active Directory. Za dostop z višjimi pravicami (skrbniške ali druge vrste višjih pravic) mora biti obvezna uporaba preverjanja v dveh korakih, kot je pametna kartica ali program za preverjanje pristnosti v telefonu.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
51	Dobavitelj mora Microsoftove osebne ali zaupne podatke med prenosom po omrežjih zaščititi s šifriranjem ob uporabi protokola Transport Layer Security (»**TLS**«) ali Internet Protocol Security (»**IPsec**«). Ti načini so opisani v standardih NIST 800-52 in NIST 800-57; uporabiti je mogoče tudi enakovreden standard v panogi. Dobavitelj mora zavrniti morebitne Microsoftove osebne ali zaupne podatke, poslane v nešifrirani obliki.	Postopek ustvarjanja, uvajanja in zamenjave potrdil TLS ali drugih potrdil mora biti opredeljen in uveljavljen.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
52	Vse naprave dobavitelja (prenosni računalniki, delovne postaje ipd.), ki bodo dostopale do Microsoftovih osebnih ali zaupnih podatkov ali jih obdelovale, morajo uporabljati šifriranje diskov.	Vse naprave, ki se uporabljajo za obdelavo Microsoftovih osebnih ali zaupnih podatkov, šifrirati, da ustrezajo ravni šifriranja v Bitlockerju ali drugi enakovredni rešitvi za šifriranje diskov v panogi.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost (nadaljevanje)		
53	Vpeljani morajo biti sistemi in postopki (ki uporabljajo trenutne panožne standarde, kot so tisti, opisani v standardu NIST 800-111) za šifriranje vseh in vsakršnih Microsoftovih osebnih in/ali zaupnih podatkov, navedenih spodaj, ko niso v uporabi (ko so shranjeni), med drugim tudi vključno z vsemi spodaj navedenimi: ▪ podatki o poverilnicah (npr. uporabniška imena in gesla); ▪ podatki o plačilnih sredstvih (npr. številke kreditnih kartic in bančnih računov); ▪ osebni podatki, povezani s priseljevanjem; ▪ podatki o zdravstvenih profilih (npr. številke zdravstvenih kartotek ali biometrični identifikatorji, kot so DNK, prstni odtisi, očesne mrežnice ali šarenice, glasovni vzorci, obrazni vzorci in mere rok, uporabljeni za preverjanje pristnosti); ▪ identifikacijski podatki, ki jih izdajo državni organi (npr. EMŠO ali številka vozniškega dovoljenja); ▪ podatki, ki pripadajo Microsoftovim strankam (npr. SharePoint, dokumenti v O365, stranke storitve OneDrive); ▪ gradivo, povezano z nepredstavljenimi Microsoftovimi izdelki; ▪ datum rojstva; ▪ podatki v profilih otrok; ▪ sprotni zemljepisni podatki; ▪ fizični osebni (neslužbeni) naslov; ▪ osebne (neslužbene) telefonske številke; ▪ veroizpoved; ▪ politična mnenja; ▪ spolna usmeritev/preference; ▪ odgovori na varnostna vprašanja (npr. preverjanje v dveh korakih, ponastavitev gesla); o materin dekliški priimek.	Preveriti, da so Microsoftovi osebni in zaupni podatki, navedeni v tej vrstici, šifrirani, ko niso v uporabi.	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*
54	Pri obdelavi kreditnih kartic v Microsoftovem imenu se mora držati upoštevnih standardov za obdelavo kreditnih kartic, ki jih določi izdajatelj kartic.	Skladnost mora izkazati z letno predložitvijo potrdila o skladnosti s standardom »**PCI-DSS**« (Payment Card Industry Data Services Standard). *Predložitev potrdil o skladnosti s standardi PCI DSS združenju SSPA. Če imate vprašanja, se*	*<Skladno> <Neskladno> <Ni upoštevno> <Pravno navzkrižje> <Navzkrižje s pogodbo>*

		obrnite na SSPAHelp@microsoft.com.	

#	Microsoftove zahteve za varstvo podatkov za dobavitelje	Dokazilo o skladnosti	Odgovor
	Razdelek J: Varnost (nadaljevanje)		
55	Dobavitelj mora Microsoftova fizična sredstva shranjevati v okolju z nadzorom dostopa.	Vzpostavljeni morajo biti sistemi in postopki za upravljanje fizičnega dostopa do digitalnih, fizičnih, arhivskih in varnostnih kopij Microsoftovih osebnih podatkov. Premik in uničenje fizičnih nosilcev podatkov, na katerih so Microsoftovi podatki, je treba spremljati s skrbniško verigo.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*
56	Anonimizirati je treba vse Microsoftove osebne podatke, uporabljene v razvijalskem ali preskuševalnem okolju.	Microsoftovih osebnih podatkov ni dovoljeno uporabljati v razvijalskih ali preskuševalnih okoljih; če ni druge možnosti, jih je treba anonimizirati, da se prepreči prepoznavanje oseb, na katere se nanašajo osebni podatki, ali napačna uporaba osebnih podatkov. Opomba: Anonimizirani podatki se razlikujejo od psevdonimiziranih podatkov. Anonimizirani podatki so podatki, ki se ne nanašajo na določeno ali določljivo fizično osebo, kjer osebe, na katero se nanašajo osebni podatki, ni mogoče ali ni mogoče več prepoznati.	*<Skladno>* *<Neskladno>* *<Ni upoštevno>* *<Pravno navzkrižje>* *<Navzkrižje s pogodbo>*