

Microsoftovi zahtjevi za zaštitu podataka o dobavljačima

Primjenjivost

Microsoftovi zahtjevi za zaštitu podataka o dobavljačima ("DPR") odnose se na svakog Microsoftovog dobavljača koji obrađuje Microsoftove osobne podatke ili Microsoftove povjerljive podatke u vezi s izvedbom tog dobavljača (npr. davanje usluga, softverske licence, usluge oblak) 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 statutarne 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.
- 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 ograničavanja 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 svih standardnih ugovornih uvjeta, obvezujućih korporacijskih pravila ili drugih shema koje su odobrile vlasti za zaštitu podataka, Europski odbor za zaštitu podataka ili Europska komisija, a koje je usvojila ili prihvatila tvrtka Microsoft, uključujući EU-SAD i Švicarska-SAD. Okviri Zaštite privatnosti i EU Odredba o općoj zaštiti podataka. Dobavljač se slaže da će obavijestiti tvrtku Microsoft ako Dobavljač odluči da više ne može poštivati svoje obaveze kako bi ponudio istu razinu zaštite kako je propisano principima Zaštite privatnosti. Dobavljač će također osigurati da se toga pridržavaju i svi podzakupci (kako je definirano Odredbom 1(d) u Standardnim ugovornim odredbama iz 2010. koje su objavljene kao Dodatak Odluci Europske komisije C(2010)593.

Ključne definicije

Sljedeći izrazi koji se koriste u ovom DPR-u imaju sljedeća značenja. Popis primjer 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“.

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

„**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.

„**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.

„**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.

„**Osobni podaci**“ označavaju sve podatke koji imaju veze s identificiranom stvarnom osobom ili onom koja se može identificirati (“**Subjekt podataka**”); stvarna osoba koja se može identificirati jest osoba koju se može 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 protivu obradi Microsoftovih osobnih podataka tog Subjekta podataka ako je to potrebno prema zakonu.

„**Probijanje podataka**“ označava kršenje sigurnosti koje vodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima ili Microsoftovim povjerljivim podacima koji su poslani, pohranjeni su ili su na drugi način obrađeni.

„**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.

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak A: Upravljanje			
1	<p>Svaki primjenjivi ugovor između tvrtke Microsoft i dobavljača (npr. glavni ugovor, izjava o radu, narudžbenice i ostale narudžbe) sadrži jezik o zaštiti podataka o privatnosti i sigurnosti u skladu s Microsoftovim povjerljivim ili osobnim podacima, kako je primjenjivo.</p> <p>Za tvrtke koje se ponašaju kao obrađivači, 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.</p>	<p>Dobavljač mora podnijeti primjenjivi ugovor između tvrtke Microsoft i dobavljača.</p> <p>Za obrađivače opisi obrade nalaze se u primjenjivom ugovoru (npr. izjava o radu, narudžbenice).</p> <p>Napomena: tvrtke s narudžbenicama tijekom leta mogu dodati potreban opis aktivnosti obrade kasnije tijekom postupka kupnje.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
2	<p>Dodijeliti odgovornost i pouzdanost u skladu s DPR-om određenoj osobi ili grupi unutar tvrtke.</p>	<p>Ime osobe ili grupe zadužene za osiguranje usklađenosti s DPR-om Microsoftovog dobavljača.</p> <p>Dokument opisuje ovlasti i odgovornosti ove osobe ili grupe koji pokazuje ulogu privatnosti i/ili sigurnosti.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
3	<p>Uspostavljanje, održavanje i obavljanje godišnje obuke o privatnosti i sigurnosti za zaposlenike koji će imati pristup Microsoftovim osobnim ili povjerljivim podacima.</p> <p>Ako vaša tvrtka nema pripremljen sadržaj, možete koristiti ovaj izvadak organizatora i prilagoditi ga svojoj tvrtki.</p>	<p>Dostupni su godišnji zapisi o pohađanju.</p> <p>Sadržaj o obuci obuhvaća principe o privatnosti i sigurnosti.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
4	<p>Obrađivati Microsoftove osobne podatke samo u skladu s Microsoftovim dokumentiranim uputama, uključujući imajući na umu prijenose Microsoftovih osobnih podataka trećoj zemlji ili međunarodnoj organizaciji, osim ako se to traži zakonom; u takvom slučaju obrađivač (dobavljač) će obavijestiti nadzornika (Microsoft) o tom pravnom zahtjevu prije obrade, osim ako zakon zabranjuje takve podatke na važnom temelju javnog interesa.</p>	<p>Dokumentirani dokaz o uputama kako je naloženo u ugovoru (npr. izjavi o radu ili narudžbenici) ili u sklopu dijela elektroničkog sustava koji se koristi u izvođenju.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak B: Obavijest			
5	<p>Dobavljač mora koristiti Microsoftovu Izjavu o zaštiti privatnosti kad prikuplja osobne podatke u ime tvrtke Microsoft.</p> <p>Obavijest o privatnosti mora biti jasna i dostupna Subjektima podataka kako bi im pomogla da odluče žele li dobavljaču dati svoje osobne podatke.</p> <p>Napomena: tamo gdje je vaša tvrtka nadzornik aktivnosti obrade, objavit ćete svoju vlastitu obavijest o privatnosti.</p> <p><i>Kontaktirajte SSPAHelp@microsoft.com za pristup odgovarajućim Microsoftovim obavijestima.</i></p>	<p>Dobavljač koristi fwdlink za aktualnu objavljenu Microsoftovu Izjavu o zaštiti privatnosti.</p> <p>Izjava o zaštiti privatnosti objavljuje se u bilo kojem kontekstu gdje će se prikupljati korisnički osobni podaci.</p> <p>Ako je primjenjivo, dostupna je izvanmrežna verzija te se nudi prije prikupljanja podataka.</p> <p>Bilo koje izvanmrežne Izjave o zaštiti privatnosti koje se koriste jesu najnovije objavljene verzije i ispravno su datirane.</p> <p>Za usluge Microsoftovih zaposlenika koristi se Microsoftova Obavijest o zaštiti podataka.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
6	<p>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.</p>	<p>Skripta za glasovne snimke uključuje kako se obrađuju Microsoftovi osobni podaci i uključuje</p> <ul style="list-style-type: none"> ▪ prikupljanje, ▪ upotrebu i ▪ zadržavanje. 	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak C: Izbor i pristanak			
7	<p>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.</p>	<p>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.</p> <p>Dobavljač može demonstrirati kako Subjekt podataka povlači pristanak za aktivnost obrade.</p> <p>Dobavljač može demonstrirati kako se provjeravaju preference prije pokretanja nove aktivnosti obrade.</p> <p>Dobavljač nadzire učinkovitost upravljanja preferencama kako bi osigurao vremenski okvir za promjenu preferenci i to je najrestriktivniji lokalni pravni zahtjev koji se primjenjuje.</p> <p>Napomena: dokaz može biti snimka zaslona interakcije s korisnikom; eksperimentiranje s uslugom ili mogućnost pregleda tehničke dokumentacije.</p>	<p><i><Usuglašeno></i> <i><Nije usuglašeno></i> <i><Ne primjenjuje se></i> <i><Sukob u vezi zakona></i> <i><Sukob u vezi ugovora></i></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak C: Izbor i pristanak (nast.)			
8	<p>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.</p> <p>Dobavljači koji izrađuju i upravljaju Microsoftovim web-mjestima i/ili aplikacijama moraju Subjektima podataka ponuditi transparentnu obavijest i odabir u vezi upotrebe kolačića.</p> <p>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.</p>	<p>Svrha svakog kolačića mora biti dokumentirana i mora obavještavati o vrsti implementiranog kolačića.</p> <ul style="list-style-type: none"> ▪ Dugotrajni kolačići ne smiju se koristiti kad su dostatni kolačići sesije. ▪ Kad se koriste dugotrajni kolačići, oni ne smiju imati datum isteka koji je dulji od 2 godine nakon što je korisnik posjetio web-mjesto. Za korisnike u EU datum isteka za dugotrajne kolačiće ne smije biti dulji od 13 mjeseci. <p>Provjerite usklađenost sa zakonima EU koji su primjenjivi, kao što je:</p> <ul style="list-style-type: none"> ▪ upotreba pravila za označavanje, „Privatnost i kolačići“ za izjavu o zaštiti privatnosti i ▪ osigurati korisnikov pristanak prije upotrebe kolačića u svrhu koja nije ključna, kao što je oglašavanje. 	<p><i><Usuglašeno></i> <i><Nije usuglašeno></i> <i><Ne primjenjuje se></i> <i><Sukob u vezi zakona></i> <i><Sukob u vezi ugovora></i></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
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.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
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.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
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.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
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.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak E: Zadržavanje			
13	<p>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.</p>	<p>Dobavljač radi u skladu s pravilima dokumentiranog zadržavanja ili zahtjevima zadržavanja koje određuje Microsoft u ugovoru (npr. izvaji o radu, narudžbenici).</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
14	<p>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.</p> <p>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.</p> <p>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.</p>	<p>Zadržati zapise o odbacivanju Microsoftovih osobnih i osjetljivih podataka za (npr. o vraćanju tvrtki Microsoft radi uništavanja).</p> <p>Ako je potrebno uništavanje ili ga Microsoft zahtijeva, dobavljač mora dati certifikat o uništenju koji je potpisao djelatnik dobavljača.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
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 sljedeće:		
15	Asistirati tvrtki Microsoft putem odgovarajućih tehničkih i organizacijskih mjera, onoliko koliko je moguće, da bi ispunio svoje obaveze u reagiraju na zahtjeve Subjekta podataka koji traže izvršiti svoja Prava Subjekta podataka.	Ovdje su postupci i procedure kako bi podržali izvršavanje Prava Subjekta podataka.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
16	Odgovoriti na sve zahtjeve Prava Subjekta podataka bez neopravdanog kašnjenja.	Dobavljač provodi periodične testove da bi osigurao da može podržavati Prava Subjekta podataka.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
17	Osim ako je drugačije odredio Microsoft, dobavljač će referirati sve Subjekte podataka koji kontaktiraju dobavljača izravno tvrtki Microsoft radi ostvarivanja njihovih Prava Subjekta podataka. 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. <i>Kontaktirajte SSPAHelp@microsoft.com za pomoć s ovim zahtjevom.</i>	Dobavljač mora dati korake koji su potrebni za pristup osobnim podacima, kao i načine dostupne za ažuriranje podataka.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
18	Kada odgovara izravno Subjektu podataka, provjeriti identitet Subjekta podataka koji podnosi zahtjev.	Dobavljač ima dokumentiranu metodu koja se koristi za identificiranje Microsoftovih Subjekta podataka.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak F: Subjekti podataka (nast.)			
	Nakon što potvrdi identitet Subjekta podataka, dobavljač mora sljedeće:		
19	Utvrđiti ima li ili nadgleda li Microsoftove osobne podatke o tom Subjektu podataka.	Dobavljač ima postavljene postupke za utvrđivanje ima li osobne podatke.	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
20	Uložiti razuman trud u lociranje zatraženih osobnih podataka za Microsoft te imati odgovarajuće zapise kako bi pokazao da je provedeno razumno pretraživanje.	<p>Dobavljač zadržava zapis koji pokazuje koji su koraci poduzeti da se udovolji zahtjevima Prava Subjekta podataka.</p> <p>Dokumentacija uključuje:</p> <ul style="list-style-type: none"> ▪ datum i vrijeme zahtjeva ▪ poduzete radnje kao odgovor na zahtjev i ▪ zapis kad je obaviještena tvrtka Microsoft. 	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
21	<p>Zabilježiti datum i vrijeme zahtjeva Prava Subjekta podataka i radnji koje je poduzeo dobavljač kao odgovor na takve zahtjeve.</p> <p>Daje zapise o zahtjevima Subjekta podataka tvrtki Microsoft po zahtjevu.</p>	Dobavljač održava zapise o zahtjevima za pristup i dokumentira promjene osobnih podataka.	
	Nakon potvrde identiteta Subjekta podataka te nakon što dobavljač potvrdi da ima zatražene Microsoftove osobne podatke, dobavljač mora sljedeće:		
22	Za zahtjeve za dobivanje kopije osobnih podataka, ponuditi Microsoftove osobne podatke Subjektu podataka u odgovarajućem tiskanom, elektroničkom ili verbalnom formatu.	Dobavljač daje osobne podatke Subjektu podataka u formatu koji je razumljiv te u obliku koji odgovara Subjektu podataka i dobavljaču.	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak F: Subjekti podataka (nast.)			
23	<p>Ako se njihov zahtjev odbije, s Microsoftove strane, Subjektu podataka treba dati pisano objašnjenje koje je ujednačeno sa svim relevantnim uputama koje je tvrtka Microsoft prethodno pružila.</p> <p><i>Kontaktirajte SSPAHelp@microsoft.com za pomoć s ovim zahtjevom.</i></p>	<p>Instance dokumenata kada se zahtjevi odbiju i zadržavanje dokaza Microsoftovog pregleda i odobrenja.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
24	<p>Dobavljač mora poduzeti razumne mjere opreza kako bi se osiguralo da se izdani Microsoftovi osobni podaci ne koriste za identifikaciju druge osobe.</p>	<p>Dobavljač mora pokazati da su poduzete razumne mjere opreza kako se druga osoba ne bi mogla identificirati iz izdanih podataka (npr. ne može fotokopirati cijelu stranicu podataka ako se traženi osobni podaci Subjekta podataka pojavljuju samo u jednom retku).</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
25	<p>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.</p> <p><i>Kontaktirajte SSPAHelp@microsoft.com za pomoć s ovim zahtjevom.</i></p>	<p>Dobavljač dokumentira slučajeve neslaganja i eskalira problem tvrtki Microsoft.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak G: Otkrivanje trećim stranama			
	Ako dobavljač namjerava koristiti podizvođača za obradu Microsoftovih osobnih ili povjerljivih podataka, dobavljač mora sljedeće:		
26	Dobiti Microsoftovo izričito pisano odobrenje prije unajmljivanja podizvođača usluga ili unošenja bilo kakvih izmjena u vezi dodavanja ili zamjene podizvođača. <i>Kontaktirajte SSPAHelp@microsoft.com za pomoć s ovim zahtjevom.</i>	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.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
27	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.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
28	Osigurati da podizvođač koristi Microsoftove osobne podatke u skladu s navedenim preferencama kontakta za Subjekt podataka.	Pokazati kako podizvođači koriste preference Microsoftovih Subjekata podataka. Ponuditi pomoćnu dokumentaciju koja obuhvaća vremenski okvir za podizvođača da ispoštuje promjene preferenci.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
29	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.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
30	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.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak G: Otkrivanje trećim stranama (nast.)			
31	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.	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
32	Odmah poduzeti postupke za umanjeње bilo koje stvarne ili potencijalne štete uzrokovane podizvođačevom neovlaštenom ili nezakonitom obradom Microsoftovih osobnih i privatnih podataka.	Dobavljač može demonstrirati da ima spreman plan i postupke ako dođe do zloupotrebe Microsoftih osobnih i povjerljivih podataka od strane podizvođača.	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
Odjeljak H: Kvaliteta			
33	Dobavljač mora zadržati integritet svih Microsoftovih osobnih podataka te osigurati da ostanu točni, potpuni i relevantni za navedene svrhe zbog kojih su obrađeni.	<p>Dobavljač može demonstrirati da postoje postupci za validaciju Microsoftovih osobnih podataka kad se prikupljaju, izrađuju i ažuriraju.</p> <p>Dobavljač može demonstrirati da postoje postupci za nadzor i uzorkovanje da bi se potvrdila točnost u svakom trenutku i ispravno, ako je to potrebno.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak I: Nadzor i provođenje			
34	Dobavljač ima plan odgovora na incident koji zahtijeva da dobavljač obavijesti tvrtku Microsoft bez odlaganja čim postane svjestan probijanja podataka ili sigurnosne ranjivosti povezane s dobavljačevim rukovanjem Microsoftovim osobnim ili povjerljivim podacima. <i>Kontaktirajte SSPAHelp@microsoft.com da biste prijavili incident.</i>	Dobavljač ima plan za odgovor na incident koji uključuje korak za obavještanje korisnika (Microsoft) kako je opisano u ovom odjeljku.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
35	Ne izdajte nikakve objave za medije niti bilo koje druge objave za javnost u vezi s probijanjem podataka koje se odnosi na Microsoftove osobne ili povjerljive podatke bez dopuštenja tvrtke Microsoft, osim ako je to uvjetovano zakonom.	Dobavljač pristaje ispuniti ovaj zahtjev ako dođe do događaja.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
36	Implementirati plan ispravljanja i nadzirati rješavanje probijanja podataka i ranjivosti povezanih s Microsoftovim osobnim ili povjerljivim podacima kako bi se osiguralo pravovremeno poduzimanje odgovarajućih radnji.	Dobavljač ima dokumentirane postupke koje će poduzeti kao odgovor na probijanje podataka i rješavanje problema.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>
37	Ustanoviti službeni žalbeni postupak za reakciju na sve žalbe u vezi sa zaštitom podataka koje se odnose na osobne podatke za Microsoft.	Dobavljač ima načine za primanje žalbi u vezi Microsoftovih osobnih podataka te ima dokumentirani postupak za žalbe kako bi ih riješio.	<Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost			
	<p>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.</p> <p>Sigurnosni program dobavljača mora udovoljavati standardima koji se nalaze niže, zahtjevi 38 - 56.</p>	<p>Sigurnosne mjere mogu premašivati one koje su navedene kao nužne za ispunjavanje regulatornih shema (npr. HIPAA, GLBA) ili ugovornih zahtjeva.</p> <p>Prihvatljiva zamjena za odjeljak J jest valjano izvješće ISO 27001 ili SOC 2 sa sigurnošću. Kontaktirajte SSPAHelp@microsoft.com da biste primijenili ovu zamjenu.</p> <p>Napomena: morat ćete podnijeti dokumentaciju koja opisuje opseg ovih certifikata/izvješća.</p>	
38	<p>Obaviti godišnju procjenu sigurnosti mreže koja obuhvaća:</p> <ul style="list-style-type: none"> ▪ pregled velikih izmjena okruženja, kao što su nova komponenta sustava, mrežna topologija, pravilo vatrozida, ▪ obavljanje skeniranja ranjivosti i ▪ održavanje zapisnika promjena. 	<p>Dobavljač ima dokumentiranu procjenu mreže, zapisnike o izmjenama i rezultate skeniranja.</p> <p>Potrebni zapisnici o izmjenama moraju pratiti izmjene, dati podatke o razlogu izmjene i uključivati ime i titulu dodijeljene osobe koja je to odobrila.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
39	<p>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.</p>	<p>Dobavljač demonstrira upotrebu pravila za mobilne uređaje gdje rukovanje Microsoftovim osobnim ili povjerljivim podacima zahtijeva upotrebu mobilnog uređaja.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost (nast.)			
40	Sva sredstva koja se koriste za održavanje 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 održavanje performansi. Inventar tih sredstava mora sadržavati: <ul style="list-style-type: none"> ▪ lokaciju uređaja ▪ klasifikaciju podataka na sredstvu ▪ zapis obnove sredstva nakon dovršetka posla ili poslovnog ugovora i ▪ zapis o odlaganju medija za pohranu podataka kad više nije potreban. 	<i><Usuglašeno></i> <i><Nije usuglašeno></i> <i><Ne primjenjuje se></i> <i><Sukob u vezi zakona></i> <i><Sukob u vezi ugovora></i>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost (nast.)			
41	<p>Uspostaviti i održati postupke za upravljanje pravima pristupa kako bi se spriječio neovlašteni pristup bilo kojim Microsoftovim osobnim ili povjerljivim podacima pod kontrolom dobavljača.</p>	<p>Dobavljač pokazuje da je implementirao plan pristupa upravljanja pravima koji obuhvaća:</p> <ul style="list-style-type: none"> ▪ pristup postupcima kontrole ▪ postupci identifikacije ▪ postupci za zaključavanje nakon neuspješnih pokušaja ▪ ponovno postavljanje lozinke onoliko često koliko je potrebno, ali ne dulje od svakih 90 dana ▪ robusni parametri za odabir vjerodajnica za autentifikaciju i ▪ deaktivacija korisničkih računa po završetku zadatka u roku od 48 sati. <p>Dobavljač pokazuje da je uspostavio postupak za pregled pristupa korisnika Microsoftovim osobnim i povjerljivim podacima, primjenjujući princip najmanje privilegije. Postupak uključuje:</p> <ul style="list-style-type: none"> ▪ jasno definirane korisničke uloge ▪ postupci za pregled i opravdanje odobrenja pristupa ulogama i ▪ testiranje da korisnici unutar uloga s pristupom Microsoftovim podacima imaju dokumentirano opravdanje za tu grupu/ulogu. 	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost (nast.)			
42	<p>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:</p> <ul style="list-style-type: none"> ▪ definirani pristup riziku radi davanja prioriteta sigurnosnim zakrpama ▪ mogućnost rukovanja i implementiranja hitnih zakrpa ▪ primjenjivost za operativni sustav i serverski softver, kao što su poslužitelj aplikacija i softver baze podataka ▪ dokumentiranje rizika koji zakrpa smanjuje i praćenje svih izuzetaka i ▪ zahtjevi za prekid korištenja softvera koji autorska tvrtka više ne podržava. 	<p>Dobavljač može demonstrirati implementirani postupak upravljanja zakrpama koji udovoljava ovom zahtjevu i pokriva barem sljedeće.</p> <ul style="list-style-type: none"> ▪ Određivanje ozbiljnosti za informiranje postavljanja prioriteta. (Definicije ozbiljnosti dokumentirane su.) ▪ Dokumentirani postupak za implementiranje hitnih zakrpa. ▪ Provjerite da se ne koriste operativni sustavi koji više nemaju podršku autorske tvrtke. ▪ Zapisi upravljanja zakrpama koji prate odobrenja i izuzetke. 	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
43	<p>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.</p> <p>Ažurirati definicije zlonamjernih programa svakodnevno ili kako je naveo dobavljač antivirusnog softvera i softvera protiv zlonamjernih programa.</p> <p>Napomena: to se odnosi na sve operativne sustave, uključujući Linux.</p>	<p>Postoje zapisi da je aktivan antivirusni softver i softver protiv zlonamjernih programa.</p> <p>Napomena: ovaj zahtjev primjenjuje se na sve operativne sustave.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
44	<p>Dobavljači koji razvijaju softver za Microsoft u postupak izrade moraju inkorporirati principe sigurnosti po dizajnu.</p>	<p>Dobavljačevi dokumenti s tehničkim specifikacijama uključuju točke provjere za provjeru sigurnosti u svojim razvojnim ciklusima.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost (nast.)			
45	<p>Implementiranje programa Prevencija gubitka podataka (“DLP”). 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:</p> <ul style="list-style-type: none"> ▪ upotrebu sustava Intrusion Detection Systems (“IDS”) na poslužitelju, mreži i u oblaku prema industrijskim standardima ako zadržavate Microsoftove osobne ili povjerljive podatke ▪ implementaciju naprednih sustava Intrusion Protection Systems (“IPS”) konfiguriranih za nadziranje i aktivno zaustavljanje gubitka podataka ▪ u slučaju probijanja sustava, zahtijeva analizu sustava kako bi se osiguralo rješavanje i svih zaostalih ranjivosti ▪ opisivanje potrebnih postupaka za nadzor sustava i kompromitaciju alata za otkrivanje i ▪ uspostavljanje odgovora na incident i izvođenje postupka upravljanja kad se otkrije događaj probijanja podataka. 	Dokumentirani IDS/IPS primijenjen s postupcima kao izravan odgovor kad se utvrdi ranjivost ili probijanje podataka.	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
46	<p>Odmah prenijeti rezultate istrage odgovora na incident višem menadžmentu i tvrtki Microsoft.</p> <p><i>Kontaktirajte SSPAHelp@microsoft.com da biste obavijestili tvrtku Microsoft.</i></p>	Sustavi i postupci tu su da prenesu rezultate istrage odgovora na incident tvrtki Microsoft.	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
47	Administratori sustava, radno osoblje, menadžment i treće strane moraju proći godišnju obuku o sigurnosti.	<p>Uspostaviti program obuke o sigurnosti koji obuhvaća sljedeće:</p> <ul style="list-style-type: none"> ▪ godišnja obuka o reagiranju na incident i ▪ simulirani događaji i automatizirani mehanizmi za omogućavanje učinkovitog reagiranja na krizne situacije. <p>Svijest o sprječavanju incidenata, kao što su rizici povezani s</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

		preuzimanjem zlonamjernog softvera.	
--	--	-------------------------------------	--

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost (nast.)			
48	Dobavljač mora osigurati da se postupcima planiranja sigurnosnog kopiranja zaštite Microsoftovi osobni i povjerljivi podaci od neovlaštenog korištenja, pristupa, otkrivanja, izmjene i uništenja.	<p>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.</p> <p>Dobavljač može pokazati da ima definirane i implementirane postupke za povremeno sigurnosno kopiranje, sigurnu pohranu i učinkovitu obnovu kritičnih podataka.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
49	Uspostaviti i testirati poslovni kontinuitet i planove o obnovi u slučaju katastrofe.	<p>Plan o obnovi nakon katastrofe mora sadržavati sve od sljedećeg.</p> <ul style="list-style-type: none"> ▪ Definirani kriteriji za utvrđivanje je li sustav kritičan za rad dobavljačevog poslovanja. ▪ Popis kritičnih sustava na temelju definiranih kriterija koji se moraju ciljati za obnovu u slučaju katastrofe. ▪ 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. ▪ Godišnje (ili češće) testiranje i pregled planova za obnovu nakon katastrofe kako bi se osiguralo ispunjavanje ciljeva obnove. 	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost (nast.)			
50	<p>Autentificirati identitet pojedinca prije nego što tom pojedincu odobri pristup Microsoftovim osobnim ili povjerljivim podacima.</p>	<p>Osigurati da su svi korisnički ID-jevi jedinstveni i da svaki ima metodu autentifikacije industrijskog standarda, kao što je Azure Active Directory.</p> <p>Povišen pristup (administrativni ili druge vrste poboljšanih privilegija) mora zahtijevati upotrebu drugog faktora, kao što je autentifikator na temelju pametne kartice ili telefona.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
51	<p>Dobavljač mora zaštititi Microsoftove osobne i povjerljive podatke u tranzitu između mreža putem šifriranja koristeći Transport Layer Security („TLS“) ili Internet Protocol Security („IPsec“).</p> <p>Ove su metode opisane u NIST 800-52 i NIST 800-57; može se koristiti i ekvivalentni industrijski standard.</p> <p>Dobavljač mora odbiti isporuku Microsoftovih osobnih ili povjerljivih podataka koje se prenose nešifriranim putovima.</p>	<p>Postupak izrade, primjene i zamjene TLS-a ili drugih certifikata mora biti definiran i primjenjivati se.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
52	<p>Svi uređaji dobavljača (prijenosna računala, radne stanice itd.) koji će pristupati ili rukovati Microsoftovim osobnim ili povjerljivim podacima moraju koristiti enkripciju na temelju diska.</p>	<p>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.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost (nast.)			
53	<p>Moraju postojati sustavi i postupci (koji koriste aktualne industrijske standarde, poput onih opisanih u standardu <u>NIST 800-111</u>) 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:</p> <ul style="list-style-type: none"> ▪ podatke vjerodajnica (npr. korisničko ime/lozinke) ▪ podatke o instrumentima plaćanja (npr. brojevi kreditnih kartica ili bankovnih računa) ▪ osobni podaci povezani s imigracijom ▪ 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) ▪ podaci o službenom identifikacijskom broju (npr. OIB ili broj vozačke dozvole) ▪ podaci koji pripadaju Microsoftovim korisnicima (npr. Sharepoint, O365 dokumenti, korisnici One Drivea) ▪ materijal povezan s nenajavljenim Microsoftovim proizvodima ▪ datum rođenja ▪ podaci o profilu djeteta ▪ geografski podaci u stvarnom vremenu ▪ fizička privatna adresa (koja nije poslovna) ▪ privatni brojevi telefona (koji nisu poslovni) ▪ vjeroispovijest ▪ politička stajališta ▪ seksualna orijentacija/preferenca ▪ odgovori na sigurnosno pitanje (npr. 2fa, ponovno postavljanje lozinke) <ul style="list-style-type: none"> ○ majčino djevojačko prezime 	<p>Provjerite da su Microsoftovi osobni i povjerljivi podaci navedeni u ovom retku šifrirani u mirovanju.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
54	<p>Prilikom obrade kreditnih kartica u ime tvrtke Microsoft, pridržavajte se primjenjivih standarda za rukovanje kreditnim karticama u skladu s izdavačem kartice.</p>	<p>Pokazati usklađenost pružanjem godišnje certifikacije Payment Card Industry Data Services Standard ("PCI-DSS").</p> <p>Poslati SSPA-u certifikate PCI DSS. Kontaktirajte SSPAHelp@microsoft.com ako imate pitanja.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>

#	Zahtjevi za zaštitu podataka o dobavljačima tvrtke Microsoft	Dokaz o usklađenosti	Odgovor
Odjeljak J: Sigurnost (nast.)			
55	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. Potrebno je slijediti lanac nadležnosti za premještanje i uništavanje fizičkih medija koji sadrže Microsoftove podatke.	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>
56	Učiniti anonimnim sve Microsoftove osobne podatke koji se koriste u okruženju za razvoj ili testiranje.	<p>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.</p> <p>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 podataka osobnih podataka više nije prepoznatljiv.</p>	<p><Usuglašeno> <Nije usuglašeno> <Ne primjenjuje se> <Sukob u vezi zakona> <Sukob u vezi ugovora></p>