Захтеви за заштиту података за добављаче корпорације Microsoft

Применљивост

Захтеви за заштиту података за добављаче корпорације Microsoft („**DPR**“) односе се на сваког Microsoft добављача који обрађује Microsoft личне податке или Microsoft поверљиве податке у вези са дејствовањем тог добављача (нпр. пружањем услуга, софтверских лиценци, услуга у облаку) под условима уговора са корпорацијом Microsoft (нпр. условима Поруџбеница, кровног уговора) („**Дејство“,** „**Дејствовање**“ или „**Делатност**“).

- У случају сукоба између овде наведених захтева и захтева из уговора између добављача и корпорације Microsoft, DPR има предност осим уколико применљиви добављач идентификује у форми DPR атеста тачну одредбу у уговору која је у сукобу са применљивим одељком DPR-а (у ком случају предност имају услови уговора).
- У случају сукоба између овде наведених захтева и било ког законског или уставног захтева, предност има законски односно уставни захтев.
- У случају да Microsoft добављач послује као Контролор, у смислу овог DPR-а, само захтеви из одељка И Безбедност и одељка А Управљање се примењују у односу на активности Обраде тог добављача.
- У случају да Microsoft добављач не обрађује Microsoft личне податке, већ само Microsoft поверљиве податке, у смислу овог DPR-а, само захтеви из одељка А Управљање, одељка Д Задржавање и одељка И Безбедност односе се на обраду Microsoft поверљивих података тог добављача.

Међународни пренос података

Без ограничавања других обавеза, добављач не сме да врши никакав међународни пренос Microsoft личних података, осим уколико Microsoft претходно достави писмено овлашћење за то, а добављач ће у сваком случају поступати у складу са захтевима за заштиту података свих стандардних уговорних одредби, обавезујућих правила пословања или другог нацрта који одобрава било које надлежно тело за заштиту података, Европски одбор за заштиту података или Европска комисија, а који усваја или на који пристаје Microsoft, укључујући релације ЕУ – САД и Швајцарска – САД оквире Штита приватности ЕУ-САД и Швајцарска-САД и Опште уредбе о заштити података ЕУ. Добављач прихвата да обавештава корпорацију Microsoft у случају да добављач донесе одлуку да више не може да испуњава обавезу да пружа онај ниво заштите који налажу принципи Штита приватности. Добављач такође обезбеђује да се било који и сви подобрађивачи података (како је дефинисано у клаузули 1. (д) Стандардних уговорних клаузула из 2010. године објављених као Анекс Одлуке Европске комисије Ц(2010)593) такође тога придржавају.

Главне дефиниције

Следећи појмови који се јављају у DPR-у имају следећа значења. Листа примера након израза „укључујући“, „као што је“, „нпр.“, „на пример“ и сличних израза који се користе у овом документу DPR тумаче се тако као да обухватају значење „без ограничења“ или „али не ограничавајући се на“, осим ако нема квалификације у виду речи „само“ или „искључиво“.

„**Microsoft лични подаци**“ обухватају све Личне податке које обрађује Microsoft или их неко обрађује у име корпорације Microsoft.

„**Microsoft поверљиви подаци**“ су све информације које, уколико се компромитују у смислу поверљивости или интегритета, могу да доведу до нарушавања репутације и финансијских губитака по Microsoft. То обухвата Microsoft хардверске и софтверске производе, интерне пословне апликације, маркетиншки материјал везан са прелиминарна издања, шифре лиценци за производе и техничку документацију везану за Microsoft производе и услуге.

„**Закон**“ означава све применљиве законе, правила, уставе, декрете, одлуке, налоге, прописе, пресуде, кодексе, акта, резолуције и захтеве свих надлежних државних органа (федералних, државних, локалних или међународних). „**Незаконито**“ означава све што крши закон.

„**Контролор**“ подразумева физичко или правно лице, јавни надлежни орган, агенцију или било које друго тело које самостално или заједно са другима одређује циљеве и начине за обраду Личних података. У случајевима у којима циљеве и начине обраде одређује Европска унија („**ЕУ**“) или закони државе чланице, ти закони могу да одређују контролора (или критеријуме за његово именовање).

„**Лични подаци**“ означавају све информације које се односе на физичко лице које је идентификовано или може да се идентификује („**Лице на које се односе подаци**“). Физичко лице које може да се идентификује подразумева особу која може директно или индиректно да се идентификује конкретно позивањем на идентификаторе као што су име, матични број, подаци о локацији, идентификатор на мрежи, као и на неке факторе карактеристичне за физички, физиолошки, генетски, ментални, економски, културни или социјални идентитет тог физичког лица.

„**Обрада**“ означава све операције или скупове операција које се обављају над свим Microsoft личним подацима или Поверљивим подацима, аутоматизованим или другим средствима као што су прикупљање, снимање, организовање, структурирање, складиштење, адаптација или измена, преузимање, консултација, коришћење, откривање путем преноса, дисеминација или други вид омогућавања доступности, поравнање или комбиновање, ограничавање, брисање или уништење. „Обрађивање“ и „Обрађено“ имају томе аналогна значења.

„**Обрађивач**“ означава физичко или правно лице, јавни орган, агенцију или неко друго тело које Обрађује Личне податке у име Контролора.

„**Право лица на које се односе подаци**“ означава права особе на коју се подаци односе да приступа подацима, избрише их, измени, извезе, ограничи или уложи жалбу на Обраду Microsoft личних података тог лица на које се односе подаци уколико то налаже закон.

„**Цурење података**“ подразумева нарушавање безбедности које доводи до случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања података или приступа Личним подацима или Microsoft поверљивим подацима који се преносе, складиште или на неки други начин обрађују.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак А: Управљање		
1	Сваки применљиви уговор између корпорације Microsoft и добављача (нпр. кровни уговор, изјава о обављању посла, поруџбенице и други налози) садржи речник који се односи на заштиту података о приватности и безбедности у односу на Microsoft поверљиве или личне податке, уколико је применљиво. За предузећа која послују као Обрађивачи, уговор мора да садржи и тему и трајање обраде, природу и циљ обраде, тип Microsoft личних података и категорије лица на која се односе подаци, као и обавезе и права корпорације Microsoft.	Добављач мора да покаже применљиви уговор између корпорације Microsoft и Добављача. За Обрађиваче описи Обраде су наведени у применљивом уговору (*нпр.* изјава о обављању посла, поруџбенице). Напомена: Предузећа са поруџбеницама за куповине током лета могу да обезбеде неопходан опис активности Обраде касније током процеса куповине.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
2	Доделите одговорности и обавезе за усклађеност са DPR смерницама именованој особи или групи унутар предузећа.	Име особе или групе надлежне за спровођење усклађености са Microsoft DPR смерницама за добављаче. Документ који описује надлежност и одговорност те особе или групе која представља улогу приватности и/или безбедности.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
3	Успоставите, одржавајте и обављајте годишњу обуку на тему приватности и безбедности за запослене који ће имати приступ Microsoft личним или поверљивим подацима. Ако ваше предузеће нема припремљен садржај, можете да користите овај нацрт сценарија и прилагодите га свом предузећу.	Доступне су годишње евиденције похађања. Садржај обуке обухвата принципе приватности и безбедности.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
4	Обрађујте Microsoft личне податке искључиво у складу са документованим упутствима корпорације Microsoft, укључујући и она која се односе на пренос Microsoft личних података у неку другу земљу или међународну организацију, осим ако вас закон на то не обавезује; у том случају, Обрађивач (добављач) мора да обавести контролора (Microsoft) о том законском захтеву пре	Документован доказ о упутствима као што је наведено у уговору (нпр. изјави о обављању посла или поруџбеници) или снимљено као део електронског система који се користи за Дејствовање.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

	Обраде, осим ако такав закон не забрањује такве информације о важним питањима од јавног значаја.		

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак Б: Обавештење		
5	Добављач мора да примењује Microsoft изјаву о приватности при прикупљању Личних података у име корпорације Microsoft. Обавештење о приватности мора да буде очигледно и доступно лицима на која се односе подаци да би им помогли да одлуче да ли да пошаљу своје личне податке добављачу. Напомена: Ако је ваше предузеће Контролор активности Обраде, треба да објавите сопствено обавештење о приватности. *Пошаљите поруку на SSPAHelp@microsoft.com да бисте добили приступ одговарајућим Microsoft обавештењима.*	Добављач користи везу прослеђивања до актуелне, објављене Microsoft изјаве о приватности. Изјава о приватности је објављена у сваком контексту у ком се Лични подаци корисника прикупљају. Ако је применљиво, верзија ван мрежне је доступна и наведена пре прикупљања података. Све Изјаве о приватности које се користе ван мреже су најновије, објављене, исправно датиране верзије. За услуге за Microsoft запослене користи се Обавештење о заштити Microsoft података.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
6	При прикупљању Microsoft личних података путем директног или снимљеног гласовног позива, добављачи морају да буду припремљени да са лицима на која се односе подаци поразговарају о применљивим праксама прикупљања података, њиховог руковања, коришћења и задржавања.	Скрипта за снимање гласа обухвата начин обраде Microsoft личних података и укључује ▪ прикупљање, ▪ коришћење и ▪ задржавање.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак B: Избор и сагласност		
7	Када се добављач ослања на пристанак као на правни основ за Обраду података, добављач мора да добави и забележи пристанак лица на које се подносе подаци за све своје активности Обраде (укључујући и све нове или ажуриране активности Обраде) пре прикупљања личних података тог лица на које се односе подаци.	Добављач може да демонстрира начин на који Лице на које се односе подаци даје пристанак за активност Обраде и чињеницу да пристанак покрива све активности Обраде добављача у односу на Личне податке тог Лица на које се односе подаци. Добављач може да демонстрира начин на који Лице на које се односе подаци повлачи пристанак за активност Обраде. Добављач може да демонстрира начин на који се жељене опције проверавају пре покретања нове активности Обраде. Добављач надгледа ефикасност управљања жељеним опцијама да би се уверио да временски оквир у ком треба да поштује промену жељене опције представља најрестриктивнији локални правни захтев који је на снази. Напомена: Доказ могу да буду снимци екрана интеракције, експериментисање са услугом или могућност приказивање техничке документације.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак B: Избор и сагласност (наст.)		
8	Колачићи су мале текстуалне датотеке које веб-сајтови и/или апликације чувају на уређајима и које садрже информације које се користе за препознавање лица на које се односе подаци или уређаја. Добављачи који праве Microsoft веб-сајтове и/или апликације и управљају њима морају да пруже лицима на које се односе подаци јасна обавештења и избор у погледу коришћења колачића. Добављачи који праве Microsoft веб-сајтове и/или апликације и управљају њима морају да се увере да је коришћење колачића у складу са обавезама наведеним у Microsoft изјави о приватности и локалним законским захтевима као што су правила која успоставља ЕУ.	Сврха сваког колачића мора да документује тако да садржи информације о типу колачића који се примењује. ▪ Трајни колачићи не смеју да се користе у случајевима када су довољни колачићи на нивоу сесије. ▪ Када се користе трајни колачићи, они не смеју да имају датум истека каснији од 2 године након тренутка када је корисник посетио сајт. За кориснике из ЕУ датум истека трајног колачића не сме да премашује 13 месеци. Потврдите усклађеност са применљивим законима ЕУ, као што су ▪ коришћење конвенције означавања, „Приватност и колачићи“ за изјаву о приватности и ▪ обезбедите потврдан пристанак корисника пре коришћења колачића у сврху која „није основна“ попут оглашавања.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак Г: Прикупљање		
9	Добављач мора да надгледа прикупљање Microsoft личних и/или поверљивих података да би се уверио да се прикупљају само подаци неопходни за Дејствовање.	Добављач може да достави документацију која показује да је прикупљање Microsoft личних и/или поверљивих података неопходно за Дејствовање.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
10	Ако добављач прикупља Личне податке од трећих лица у име корпорације Microsoft, добављач мора да потврди да су смернице и праксе трећег лица за заштиту података у складу са добављачевим уговором са корпорацијом Microsoft и DPR смерницама.	Добављач може да достави документацију о томе да су смернице и праксе трећег лица за заштиту података проверен са дужном ревношћу.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
11	Пре прикупљања Microsoft личних података путем инсталације или коришћења извршног софтвера на уређају лица на које се односе подаци, неопходност прикупљања тих информација мора да се документује у делотворном уговору добављача са корпорацијом Microsoft.	Microsoft споразум за коришћење извршног софтвера на уређају Лица на које се односе подаци је евидентиран у делотворном уговору.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
12	Пре прикупљања осетљивих Microsoft личних података (података који откривају расно или етничко порекло, политичке ставове, верска или филозофска уверења, чланство у синдикатима, генетичких података, биометријских података, података везаних за здравље или података који се тичу сексуалног живота или сексуалне оријентације физичког лица) неопходност прикупљања таквих Microsoft личних података мора да се документује у делотворном уговору добављача са корпорацијом Microsoft.	Неопходност прикупљања осетљивих Microsoft личних података је евидентирана у делотворном уговору са корпорацијом Microsoft.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак Д: Задржавање		
13	Уверите се да се Microsoft лични и поверљиви подаци не задржавају дуже него што је неопходно за Дејствовање, осим уколико закон налаже дуже задржавање Microsoft личних и/или поверљивих података.	Добављач се придржава документованих смерница за задржавање или захтева за задржавање које Microsoft наводи у уговору (нпр. изјави о обављању посла, поруџбеници).	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
14	Уверите се да се Microsoft лични о поверљиви подаци који се налазе у поседу добављача или који су под његовом контролом, по сопственом нахођењу корпорације Microsoft, врађају корпорацији Microsoft или уништавају по довршењу Дејствовања или по захтеву корпорације Microsoft. У самим апликацијама, процеси морају постојати да би се обезбедило безбедно брисање кад се подаци уклоне из апликације или експлицитно од стране корисника или на основу других окидача, као што је старост података. Када је неопходно уништавање Microsoft личних или поверљивих података, добављач мора да спали, распрши или исецка физичке ресурсе који садрже Microsoft личне и/или поверљиве податке тако да подаци не могу да се прочитају ни реконструишу.	Одржавајте евиденцију о одлагању Microsoft личних и поверљивих података (ово може да обухвата и врађање корпорацији Microsoft ради уништења). Ако је уништење неопходно или га налаже Microsoft, доставите потврду о уништењу коју је потписао представник добављача.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак Ђ: Лица на које се односе подаци		
	Лица на која се односе подаци имају право да приступају својим Личним подацима, бришу их, мењају, извозе, ограничавају и улажу жалбе на њихову Обраду („**Права лица на које се односе подаци**“). Ако Лице на које се односе подаци тражи да спроведе своја права у складу са Законом у вези са својим Microsoft личним подацима, добављач мора да уради следеће:		
15	Да асистира корпорацији Microsoft, путем одговарајућих техничких и организационих мера, у највећем могућем обиму, да испуни своје обавезе и одговори на захтеве лица на која се односе подаци која као таква желе да остваре своја права.	На снази су процеси и процедуре које подржавају спровођење Права лица на које се односе подаци.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
16	Да одговори на све захтеве Права лица на које се односе подаци у најкраћем року.	Добављач обавља периодична тестирања да би потврдио да може да подржи Права лица на које се односе подаци.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
17	Осим ако корпорација Microsoft не наложи другачије, добављач ће упутити сва Лица на које се односе подаци, а која контактирају с добављачем, директно корпорацији Microsoft, како би се остварила Права лица на које се односе подаци. Добављач ће обавестити лице на које се односе подаци о корацима које то лице треба да обави да би добило приступ својим Microsoft личним подацима или да би на неки други начин остварило своја права над тим подацима. *Пошаљите поруку на SSPAHelp@microsoft.com ако вам је потребна помоћ у вези с овим захтевом.*	Добављач обавештава о корацима које треба предузети ради приступа Личним подацима, као и доступним методима за ажурирање тих података.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
18	Кад се одговара директно Лицу на које се односе подаци, потврдити идентитет Лица које упућује захтев.	Добављач је документовао метод коришћен за идентификовање Microsoft лица на која се односе подаци.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак Ђ: Лица на које се подаци односе (наст.)		
	Једном кад Лице на које се односе подаци потврди идентитет, добављач мора да уради следеће:		
19	Да утврди да ли такво лице држи или контролише Microsoft личне податке о Лицу на које се односе подаци.	Добављач има активне процедуре за утврђивање да ли се Лични подаци задржавају.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
20	Да настоји у разумној мери да лоцира тражене Microsoft личне податке и да чува довољно евиденције која доказује да је спроведена таква разумна претрага.	Добављач одржава евиденцију из које се виде кораци предузети у циљу испуњавања захтева у вези са Правом лица на које се односе подаци. Документација садржи ▪ датум и време захтева, ▪ радње предузете ради одговора на захтев и ▪ евиденцију о томе када је Microsoft обавештен.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
21	Да забележи датум и време захтева у вези са Правом лица на које се односе подаци и радње које је добављач предузео као одговор на те захтеве. Да обезбеди евиденцију захтева Лица на које се односе подаци корпорацији Microsoft на захтев.	Добављач одржава евиденцију захтева за приступ и документује промене извршене у Личним подацима.	
	Када се потврди идентитет Лица на које се доносе подаци и добављач потврди да је то лице тражило Microsoft личне податке, добављач мора да уради следеће:		
22	За захтеве за добијање копије Личних података, да достави лицу на које се подаци односе Microsoft личне податке у одговарајућем одштампаном, електронском или вербалном облику.	Добављач доставља Личне податке Лицу на које се односе подаци у формату који је разумљив и у облику који одговара Лицу на које се односе подаци и добављачу.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак Ђ: Лица на које се подаци односе (наст.)		
23	Ако захтев буде одбијен, по сопственом нахођењу корпорације Microsoft, Лицу на које се односе подаци мора бити достављено писано објашњење које је у складу са свим релевантним упутствима које је корпорација Microsoft претходно обезбедила. *Пошаљите поруку на SSPAHelp@microsoft.com ако вам је потребна помоћ у вези с овим захтевом.*	Документовати случајеве одбијања захтева и задржати доказ прегледа и одобрења корпорације Microsoft.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
24	Добављач мора да предузме разумне мере и обезбеди да Microsoft лични подаци који се дају лицу на које се односе подаци не могу да се искористе за идентификовање неке друге особе.	Добављач мора да покаже да су предузете разумне мере тако да друга особа не може да се идентификује на основу објављених информација (нпр. не може да се фотокопира цела страница са подацима ако се тражени Лични подаци Лица на које се односе подаци налазе само у једном реду).	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
25	Ако се лице на које се односе подаци и добављач не слажу око тога да ли су Microsoft лични подаци комплетни и тачни, добављач мора да ескалира проблем корпорацији Microsoft и да сарађује са корпорацијом Microsoft у мери неопходној за решавање проблема. *Пошаљите поруку на SSPAHelp@microsoft.com ако вам је потребна помоћ у вези с овим захтевом.*	Добављач мора да документује случајеве неслагања и да проследи проблем корпорацији Microsoft.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак Е: Откривање трећим лицима		
	Ако добављач намерава да ангажује подизвођача за Обраду Microsoft личних или поверљивих података, добављач мора да уради следеће:		
26	Да набави експресни писмени пристанак корпорације Microsoft пре уговарања услуга подизвођача или било каквих промена које се односе на додавање или замену подизвођача. *Пошаљите поруку на SSPAHelp@microsoft.com да бисте добили помоћ у вези са овим захтевом.*	Потврдите да Microsoft личне податке обрађују само компаније познате корпорацији Microsoft као што се захтева у применљивом уговору (нпр. изјава о обављању посла, анекс, поруџбеница) или забележено у SSPA бази података.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
27	Да документује природу и опсег Microsoft личних и поверљивих података које накнадно обрађују подизвођачи и да се увери да су прикупљене информације потребне за Дејствовање.	Добављач одржава документацију у вези са Microsoft личним и поверљивим подацима који се откривају или преносе подизвођачима.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
28	Да се увери да подизвођач користи Microsoft личне податке у складу са жељеним начинима контакта које је навело лице на које се односе подаци.	Демонстрирајте на који начин подизвођачи употребљавају жељене опције Microsoft лица на које се односе подаци. Обезбедите пратећу документацију која садржи временски оквир током ког подизвођач мора да се придржава промене жељене опције.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
29	Да ограничи обраду Microsoft личних података коју обавља подизвођач на сврхе неопходне за испуњавање уговора између добављача и корпорације Microsoft.	Добављач може да достави документацију из које се види да су Microsoft лични подаци који су достављани подизвођачу неопходни за Дејствовање.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
30	Да прегледа жалбе ради проналажења индикација било какве неовлашћене или незаконите обраде Microsoft личних података.	Добављач може да демонстрира да су на снази системи и процеси за решавање жалби које се тичу неовлашћеног коришћења или откривања Microsoft личних података од стране подизвођача.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак Е: Откривање трећим лицима (наст.)		
31	Да обавести Microsoft чим сазна да је подизвођач обрађивао Microsoft личне или поверљиве податке у било коју другу сврху осим у вези са Дејствовањем.	Добављач је обезбедио подизвођачу упутства и средства за пријављивање злоупотребе Microsoft података.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
32	Да брзо реагује у циљу ублажавања сваке стварне или потенцијалне штете коју може да изазове неовлашћена или незаконита обрада Microsoft личних или поверљивих података коју је обавио подизвођач.	Добављач може да демонстрира да има примењен план и процедуре за случај да дође до злоупотребе Microsoft личних и поверљивих података од стране подизвођача.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
	Одељак Ж: Квалитет		
33	Добављач мора да одржава интегритет свих Microsoft личних података и обезбеди да остану тачни, комплетни и релевантни за наведене циљеве због којих се обрађују.	Добављач може да демонстрира да су на снази процедуре за валидацију Microsoft личних података при њиховом прикупљању, креирању и ажурирању. Добављач може да демонстрира да су на снази процедуре надгледања и узорковања ради континуиране потврде тачности и исправке по потреби.	*<Прихвата>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак 3: Праћење и спровођење		
34	Добављач има план реаговања у случају инцидента који обавезује добављача да без непотребног одлагања обавести Microsoft чим постане свестан цурења података или безбедносне рањивости у вези са добављачевим руковањем Microsoft личним или поверљивим подацима. *Пошаљите поруку на SSPAHelp@microsoft.com да бисте пријавили инцидент.*	Добављач има план реаговања у случају инцидента који садржи корак обавештавања клијента (корпорације Microsoft) као што је описано у овом одељку.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
35	Не објављујте никаква саопштења за јавност ни друга јавна обавештења у вези са цурењем података које се односи на Microsoft личне или поверљиве податке ако за то нисте добили одобрење од корпорације Microsoft, осим ако је другачије наведено у закону.	Добављач пристаје да испуни овај захтев уколико дође до догађаја.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
36	Примените план санације и надгледајте решавање Цурења података и рањивости везаних за Microsoft личне или поверљиве податке да бисте се уверили да се редовно предузимају одговарајуће корективне мере.	Добављач је документовао процедуре које ће бити потребне за реаговање на Цурење података и његово решавање.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
37	Успоставите формални процес подношења жалби да бисте одговорили на све жалбе у вези са заштитом података које се односе на Microsoft личне податке.	Добављач има начин за пријем жалби које укључују Microsoft личне податке и има документовану процедуру подношења жалбе за решавање жалби.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност		
	Добављач мора да успостави, примени и одржава програм за безбедност информација који обухвата смернице и процедуре да би заштитио и обезбедио Microsoft личне и поверљиве податке у складу са добрим индустријским праксама и оним што налаже закон. Безбедносни програм добављача мора да испуњава доленаведене стандарде, захтеве 38–56.	Могу постојати и друге заштитне мере сем оних наведених уколико је то потребно да би се задовољили регулаторни оквири (на пример, HIPAA, GLBA) или уговорне обавезе. Важећи ISO 27001 или SOC 2 извештај са безбедносним аспектом представља прихватљиву замену за Одељак И. Пошаљите поруку на SSPAHelp@microsoft.com да бисте применили ову замену. Напомена: Мораћете да доставите документацију у којој се описује опсег тих сертификата/извештаја.	
38	Једном годишње обављајте безбедносну процену мреже која обухвата: ▪ ревизију највећих промена у окружењу, на пример нове компоненте система, топологију мреже, правила заштитног зида, ▪ спровођење испитивања постојања рањивости и ▪ одржавање евиденције промена.	Добављач има документоване процене мреже, евиденције промена и резултате скенирања. Тражене евиденције промена морају да прате промене, пружају информације о разлозима за промене и да садрже име и позицију именованог даваоца одобрења.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
39	Добављач треба да дефинише, пошаље и примени смернице за мобилне уређаје које обезбеђују и ограничавају коришћење Microsoft личних или поверљивих података којима се приступа на мобилним уређајима или се на њима користе.	Добављач демонстрира коришћење усклађених смерница за мобилне уређаје када Microsoft лични или поверљиви подаци захтевају употребу мобилног уређаја.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
40	Сва средства која се користе ради бољег Дејствовања морају да буду урачуната и да имају идентификованог власника. Добављач је одговоран за одржавање инвентара тих информационих средстава, утврђивање прихватљивог и овлашћеног коришћења средстава и обезбеђивање одговарајућег нивоа заштите средстава током њиховог животног циклуса.	Инвентар ресурса у виду уређаја који се користе као подршка за Дејствовање. Инвентар тих ресурса треба да садржи ▪ локацију уређаја, ▪ класификацију података на ресурсу, ▪ евиденцију о опоравку ресурса након прекида радног односа или пословног уговора и ▪ евиденцију о одлагању медија за складиштење података када више није потребан.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
41	Успоставите и одржавајте процедуре управљања правима приступа да бисте спречили неовлашћен приступ Microsoft личним или поверљивим подацима који су под контролом добављача.	Добављач демонстрира да има примењен план управљања правима на приступ који обухвата ▪ процедуре за контролу приступа, ▪ процедуре за идентификацију, ▪ процедуре за блокирање после неуспешних покушаја, ▪ ресетовање лозинке онолико често колико је неопходно, али у периодима не дужим од 90 дана, ▪ јасне параметре за избор акредитива за потврду идентитета и ▪ деактивацију корисничких налога у року од 48 сати од прекида радног односа. Добављач демонстрира да има успостављен процес за ревизију корисничког приступа Microsoft личним и поверљивим подацима који намеће принцип најмањих привилегија. Процес обухвата ▪ јасно дефинисане улоге корисника, ▪ процедуре за ревизију и оправдање одобрења приступа одређеним улогама и ▪ проверу да ли корисници са улогама које имају приступ Microsoft подацима поседују документовано оправдање за присуство у групи/улози.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
42	Дефинишите и примените процедуре за управљање закрпама којим се даје приоритет безбедносним закрпама за системе који се користе за обраду Microsoft личних или поверљивих података. Те процедуре обухватају ▪ дефинисан приступ у случају ризика ради одређивања приоритета безбедносних закрпа ▪ могућност руковања безбедносним закрпама и њихове примене ▪ применљивост на софтвер за оперативне системе и сервере као што је софтвер сервера апликација и база података, ▪ документовање ризика који закрпа избегава и праћење изузетака и ▪ захтеве за повлачење софтвера који више не добија подршку компаније која га прави.	Добављач може да демонстрира примењену процедуру за управљање закрпама која испуњава ове захтеве и као минималан захтев покрива следеће. ▪ Додела степена озбиљности ради одређивања приоритета за обавештавање. (Дефиниције степена озбиљности су документоване.) ▪ Документована процедура за примену закрпа за хитне случајеве. ▪ Потврда да се не користи оперативни системи које компанија која их се креирала више не подржава. ▪ Евиденција управљања закрпама са праћењем одобрења и изузетака.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
43	Инсталирајте антивирусни и антималвер софтвер на опреми повезаној са мрежом која се користи за обраду Microsoft личних и поверљивих података, укључујући сервере и рачунаре за продукцију и обуку, да бисте се заштитили од потенцијално штетних вируса и злонамерних софтверских апликација. Ажурирајте антималверске дефиниције на дневној бази или како наложи добављач антивируса и антималвера. Напомена: Ово се односи на све оперативне системе, укључујући и Linux.	Евиденција постоји да би приказала активно коришћење антивирусног или антималвер софтвера. Напомена: Овај захтев се доноси на све оперативне системе.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
44	Добављачи који развијају софтвер за Microsoft морају у процес израде да укључе принципе пројектоване безбедности.	Документи са техничким спецификацијама добављача обухватају контролне тачке за безбедносну валидацију у својим циклусима развоја.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
45	Примените програм спречавања губитка података („**DLP**“). Подаци морају да се на одговарајући начин класификују, означе и заштите, а добављач мора да надгледа коришћене информационе системе на којима се обрађују Microsoft лични или поверљиви подаци да би установио да ли постоје упади, губици или друге неовлашћене активности. Програм DLP у најмањој мери ▪ захтева употребу хоста, мреже и система за откривање упада заснованих на облаку („**IDS**“) индустријске класе ако задржавате Microsoft личне или поверљиве податке, ▪ захтева примену напредних система заштите од упада („**IPS**“) конфигурисаних за надгледање и активно заустављање губитка података, ▪ у случају продора у систем захтева анализу система да би се разрешиле и преостале рањивости, ▪ описује процедуре потребне за надгледање алатки за откривање нарушавања система и ▪ успоставља процес реаговања у случају инцидента и процес управљања који треба да се обаве када се открију догађаји Цурења података.	Документовани примењени IDS/IPS са процедурама на снази за директно реаговање када се открије Цурење података.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
46	Одмах доставите резултате истраге одговора на инцидент вишем руководству и корпорацији Microsoft. *Пошаљите поруку на SSPAHelp@microsoft.com и обавестите корпорацију Microsoft.*	Системи и процеси морају бити на снази да би се резултати истраге реаговања у случају инцидента саопштавали корпорацији Microsoft.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
47	Администратори система, оперативни кадар, руководство и трећа лица морају да прођу годишњу обуку о безбедности.	Успоставите програм безбедносне обуке који обухвата ▪ годишњу обуку за реаговање у случају инцидента и ▪ симулиране догађаје и аутоматизоване механизме који олакшавају ефикасно реаговање у кризним ситуацијама. освешћивање о превенцији инцидената, као што су ризици у вези с преузимањем злонамерног софтвера.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
48	Добављач мора да обезбеди резервне процесе планирања који штите Microsoft личне и поверљиве податке од неовлашћеног коришћења, приступа, откривања, измене и уништења.	Добављач може да демонстрира документоване процедуре реаговања и опоравка са детаљним приказом како ће организација управљати догађајима који ометају рад и како ће одржавати безбедност информација на унапред одређеном нивоу на основу одобреног управљања циљевима непрекидне безбедности информација. Добављач може да демонстрира да има дефинисане и примењене процедуре за периодично прављење резервне копије, безбедно складиштење и ефикасан опоравак критичних података.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
49	Успоставите и тестирајте планове за континуирано пословање и опоравак од катастрофе.	План за опоравак од катастрофе мора да садржи све наведено. ▪ дефинисане критеријуме за одређивање да ли је систем од критичне важности за пословање добављача; ▪ листу критичних система засновану на дефинисаним критеријумима који за циљ морају имати опоравак у случају катастрофе; ▪ дефинисану процедуру опоравка од катастрофе за сваки критични систем која обезбеђује да инжењер који не познаје систем може да опорави апликацију за мање од 72 сата; ▪ годишње (или чешће) тестирање и преглед планова за опоравак од катастрофе како би се обезбедило испуњавање циљева.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
50	Потврдите идентитет особе пре него што јој дате приступ Microsoft личним или поверљивим подацима.	Уверите се да су сви ID-ови корисника јединствени и да сваки садржи метод потврде идентитета индустријског стандарда као што је Azure Active Directory. Пун приступ (административни или друге врсте напредних привилегија) мора захтевати коришћење другог фактора, као што је ауторизатор заснован на паметној картици или телефону.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
51	Добављач мора да штити Microsoft личне и поверљиве податке у преносу кроз мреже са шифровањем које користи Transport Layer Security („**TLS**“) или безбедност интернет протокола („**IPsec**“). Ове методе су описане у NIST 800-52 и NIST 800-57; еквивалентни индустријски стандард се такође може користити. Добављач мора да одбије испоруку свих Microsoft личних или поверљивих података који се преносе нешифрованим средствима.	Процес креирања, коришћења и замене TLS-а или других сертификата мора бити дефинисан и извршен.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
52	Сви уређаји добављача (лаптопови, радне станице итд.) који ће приступати Microsoft личним или поверљивим подацима или руковати њима морају да примењују шифровање диска.	Шифрујте све уређаје да бисте испунили захтеве Bitlocker или неког другог индустријског еквивалентног решења за шифровање дискова на свим клијентским уређајима који се користе за руковање Microsoft личним или поверљивим подацима.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
53	Системи и процедуре (који користе актуелне индустријске стандардне попут оних описаних у стандарду NIST 800-111) морају бити на снази ради шифровања у мировању (током складиштења) свих Microsoft личних и/или поверљивих података, укључујући све наведено: ▪ податке о акредитивима (нпр. корисничка имена/лозинке) ▪ податке о начинима плаћања (нпр. бројеви кредитних картица и банковних рачуна) ▪ личне податке у вези са имиграционим статусом ▪ податке о медицинском профилу (нпр. број медицинског картона или биометријске маркере или идентификаторе попут DNK, отисака прстију, очне зенице и шаренице, гласовних образаца, фацијалних образаца и димензија шаке који се користе у сврху потврде идентитета) ▪ податке за идентификацију које издају државни органи (нпр. ЈМБГ или број возачке дозволе) ▪ податке који припадају Microsoft клијентима (нпр. Sharepoint, O365 документи, One Drive клијенти) ▪ материјал везан за необјављене Microsoft производе ▪ датум рођења ▪ информације о профилу деце ▪ географске податке у реалном времену ▪ физичку личну (неслужбену) адресу ▪ личне (неслужбене) бројеве телефона ▪ веру ▪ политичке ставове ▪ сексуалну оријентацију/преференце ▪ одговоре на безбедносна питања (нпр. потврду идентитета у два корака, ресетовање лозинке) ○ девојачко презиме мајке	Проверите да ли су Microsoft лични и поверљиви подаци наведени у овом реду шифровани у мировању.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
54	При обради кредитних картица у име корпорације Microsoft, поштујте примењиве стандарде за руковање кредитном картицом према телу које је издало картицу.	Демонстрирајте усклађеност да бисте ћете једном годишње издавати сертификат за стандард услуге података за индустрију платних картица („**PCI-DSS**“). *Предати PCI DSS сертификате SSPA-у. Пошаљите поруку на*	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*

		SSPAHelp@microsoft.com ако имате питања.	

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усклађености	Одговор
	Одељак И: Безбедност (наст.)		
55	Добављач мора да складишти Microsoft физичке ресурсе у окружењу са контролисаним приступом.	Морају да постоје системи и процеси за управљање физичким приступом дигиталним, физичким, архивским и резервним копијама података корпорације Microsoft. Мора се пратити ланац власништва због кретања и уништавања физичког медија који садржи податке корпорације Microsoft.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*
56	Анонимизујте све Microsoft личне податке који се користе у окружењу за развој или тестирање.	Microsoft лични подаци не смеју да се користе у окружењима за развој или тестирање. Када не постоји алтернатива, морају да се анонимизују да би се спречила идентификација Лица на која се односе подаци или злоупотреба Личних података. Напомена: Анонимизовани подаци се разликују од Псеудонимизованих података. Анонимизовани подаци су подаци који нису повезани са физичким лицем које је идентификовано или може да се идентификује када лице на које се односе лични подаци није иденфитиковано или више не може да се идентификује.	*<Усклађен>* *<Није усклађен>* *<Не примењује се>* *<Сукоб закона>* *<Сукоб уговора>*