Захтеви за заштиту података за добављаче корпорације Microsoft

Применљивост

Захтеви за заштиту података за добављаче корпорације Microsoft („**ДПР**“) се примењују на сваког добављача корпорације Microsoft који обрађује њене Податке о личности или Поверљиве податке у вези с извршењем посла тог добављача (нпр. пружање услуга, лиценци за софтвер, услуга у облаку) под условима његовог уговора с корпорацијом Microsoft (нпр. услови поруџбенице, главног уговора) („**Извршити,**“ „**Извршава,**“ или „**Извршење посла**“**).**

- У случају сукоба између ДПР-а и захтева наведених у уговорима између добављача и корпорације Microsoft, ДПР има предност осим ако добављач не идентификује одговарајућу одредбу уговора која замењује применљиви захтев за заштиту података (у ком случају, предност имају услови уговора).
- У случају сукоба између захтева наведених у овом документу и било којих правних или законитих захтева, предност имају правни или законити захтеви.
- У случају да корпорација Microsoft делује као Руковалац, добављач може да има блаже захтеве у ДПР-у.
- У случају да добављач корпорације Microsoft не обрађује Податке о личности корпорације Microsoft већ само њене Поверљиве податке у погледу овог ДПР-а, добављач може да има блаже захтеве.

Међународни пренос података

Без ограничавања својих других обавеза, добављач не врши никакве међународне преносе Података о личности корпорације Microsoft осим ако Microsoft не достави претходно писано одобрење, а у сваком случају добављач мора да се придржава Захтева за заштиту података, укључујући Стандардне уговорне клаузуле, или по нахођењу корпорације Microsoft, друге одговарајуће механизме за прекогранични пренос које је одобрио надлежни орган за заштиту података или Европска комисија, како је применљиво, те које је усвојила или с којима је сагласна корпорација Microsoft. Накнадне Стандардне уговорне клаузуле које је усвојила (i) Европска комисија или Европски супервизор за заштиту података и одобрила Европска комисија, (ii) Уједињено Краљевство у складу с Општим савезним законом УК-а о заштити података, (iii) Швајцарска у складу са швајцарским савезним законом о заштити података или (iv) клаузуле које уређују међународни пренос података о личности које је званично усвојила влада у другој надлежности мимо Швајцарске, Уједињеног Краљевства те надлежности које су у саставу Европске уније/Европског економског региона су укључене и обавезујуће су за Добављача од дана њиховог усвајања. Добављач такође обезбеђује да се сви подобрађивачи придржавају захтева (како је дефинисано у Стандардним уговорним клаузулама).

Кључне дефиниције

Следећи појмови коришћени у овом ДПР-у имају следећа значења. Листа примера „укључујући,“ „као што су,“ „нпр.,“ „на пример,“ или слично који су коришћени у овом ДПР-у се тумачи као да укључује „без ограничења“ или „али није ограничено на,“ осим ако нису додатно описани речима као што су „само“ или „искључиво.“ Погледајте Глосар на крају овог документа за више информација.

„Руковалац“ подразумева субјект који одређује намене и начине обраде Података о личности. „Руковалац“ обухвата компанију, Руковаоца (јер је овај појам дефинисан у ГДПР-у), те еквивалентне појмове у Законима о заштити података, како контекст захтева.

„Колачићи“ су мале текстуалне датотеке које на уређајима чувају веб-сајтови и/или апликације, а који садрже информације коришћене за препознавање уређаја или Лица на које се подаци односе.

„Инцидент с подацима“ подразумева (1) повреду безбедности која доводи до случајног или незаконитог уништавања, губитка, измене, неовлашћеног откривања или приступа Подацима о личности или Поверљивим подацима корпорације Microsoft који се преносе, чувају или на други начин их обрађује Добављач или његови Подуговарачи, или

(2) безбедносну рањивост повезану с Добављачевим руковањем Подацима о личности или Поверљивим подацима корпорације Microsoft.

„Лице на које се подаци односе“ подразумева физичко лице које се може директно или индиректно идентификовати, нарочито позивајући се на идентификатор као што су име, идентификациони број, подаци о локацији, онлајн идентификатор или на један или више фактора који су специфични за физички, физиолошки, генетски, ментални, економски, културни или социјални идентитет тог физичког лица.

„Права лица на које се подаци односе“ подразумевају права Лица на које се подаци односе да приступи, избрише, уреди, извезе, ограничи или уложи приговор на обраду Података о личности корпорације Microsoft тог Лица на које се подаци односе ако то захтева закон.

„Закон“ подразумева све применљиве законе, правила, статуте, уредбе, одлуке, налоге, пресуде, кодексе, резолуције и захтеве сваког државног органа (савезног, државног, локалног или међународног) који има надлежност. „**Незаконито**” подразумева свако кршење закона.

„Поверљиви подаци корпорације Microsoft“ су све информације које ако се угрозе у погледу поверљивости или интегритета, могу да доведу до знатног губитка репутације или финансијског губитка за корпорацију Microsoft. Ови подаци укључују хардверске и софтверске производе корпорације Microsoft, њене интерне пословне апликације, маркетиншке материјале пре стављања производа у употребу, лиценцне кључеве за производе, као и техничку документацију која се односи на производе и услуге корпорације Microsoft.

„Подаци о личности корпорације Microsoft“ подразумевају податке који су обрађени од стране корпорације Microsoft или у њено име.

„Подаци о личности“ подразумевају све информације које се односе на Лице на које се подаци односе и све друге информације које по закону чине „податке о личности“ или „личне информације.“

„Обрада“ подразумева сваку операцију или скуп операција које се извршавају на свим Подацима о личности или Поверљивим подацима корпорације Microsoft, без обзира да ли се врши или не аутоматизованим средствима, као што је прикупљање, евидентирање, организација, структурисање, складиштење, прилагођавање или измена, повраћај, консултовање, коришћење, откривање преносом, ширењем или на други начин стављањем на располагање, усклађивањем или комбинацијом, ограничавањем, брисањем или уништавањем. „Обрађивање“ и „обрађен“ имају одговарајућа значења.

„Обрађивач“ подразумева субјект који обрађује Податке о личности у име другог субјекта и обухвата Пружаоца услуга, Обрађивача (јер је тај појам дефинисан у ГДПР-у) те еквивалентне појмове у Законима о заштити података, зависно од контекста.

„Подуговарач“ подразумева треће лице ком добављач делегира своје обавезе у вези с уговором који покрива његово извршење посла, укључујући филијалу добављача која није директно у уговорном односу с корпорацијом Microsoft.

„Подобрађивач“ подразумева треће лице које корпорација Microsoft ангажује да изврши посао, кад Извршење посла укључује обраду Података о личности корпорације Microsoft чији Обрађивач је корпорација Microsoft.

Одговор Добављача

Добављачи годишње потврђују усаглашеност са свим захтевима преко онлајн сервиса којим управља корпорација Microsoft. Погледајте Водич за програм ССПА да бисте разумели како се регулише усаглашеност.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	ОДЕЉАК А: Управљање	
1	Сваки применљиви уговор између корпорације Microsoft и добављача (нпр. главни уговор, спецификација посла , поруџбенице и остале поруџбине) садрже део о заштити приватности и безбедности података у односу на Поверљиве податке корпорације Microsoft те Податке о личности, према потреби, укључујући забране продаје Података о личности корпорације Microsoft и Обраду Података о личности корпорације Microsoft ван директног пословног односа између корпорације и добављача. За компаније које послују као Обрађивачи или Подобрађивачи у вези са извршењем, у односу на Податке о личности корпорације Microsoft, уговор мора да садржи предмет и трајање обраде, природу и сврху обраде, врсту Података о личности корпорације Microsoft те категорије Лица на које се подаци односе и обавезе и права корпорације Microsoft.	Добављач мора да покаже важећи уговор између корпорације Microsoft и Добављача. За Обрађиваче и Подобрађиваче, описи Обрађивања су наведени у важећем уговору (нпр. спецификација посла, поруџбенице). Напомена: компаније с поруџбеницама које су потврђене али нису извршене могу да имају опис активности обраде које су касније додате у процес наручивања.
2	Кад корпорација Microsoft потврди да ваши ангажмани испуњавају улогу Подобрађивача, добављач мора да има применљиве споразуме о заштити података с корпорацијом Microsoft. Напомена: корпорација Microsoft ће да објави ову ознаку на вашем профилу кад се ово примењује.	Стандарде уговорне клаузуле, Онлајн додатак о подацима клијената и/или Додатак за обраду података о професионалним услугама добављача и партнера.
3	Доделити одговорност за усаглашеност с ДПР-ом именованом лицу или групи унутар компаније.	Именовати функцију особе или групе задужене да осигура усаглашеност с ДПР-ом за добављаче корпорације Microsoft. Документ који описује ауторитет и одговорност ове особе или групе који показује функцију приватности и/или безбедности.
4	Успоставити, одржавати и извршавати годишњу обуку из приватности и безбедности за запослене који ће имати приступ Обрађеним подацима о личности од стране добављача у вези с Извршењем посла или Поверљивим подацима корпорације Microsoft. Ако ваша компанија нема припремљени садржај, можете користити овај преглед сценарија и прилагодити га за своју компанију. Напомена: можда ће особље добављача морати да заврши додатне обуке које пружају одељења корпорације Microsoft.	Годишње евиденције о присуству су доступне и могу на захтев да се доставе корпорацији Microsoft. Обука обухвата принципе приватности и безбедности. Документација о усаглашености са захтевима обуке ће обухватати доказ о обуци повезаној с регулаторним захтевима, обавезама безбедности и усаглашености с применљивим захтевима уговора и обавезама.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	ОДЕЉАК А: Управљање (наставак)	
5	Обрадити Податке о личности корпорације Microsoft само у складу с документованим упутствима корпорације Microsoft укључујући сценарије у односу на преносе Података о личности корпорације Microsoft у трећу земљу или међународну организацију, осим ако закон то не захтева; у ком случају, Обрађивач или Подобрађивач (добављач) обавештава руковаоца (Microsoft) о том законском захтеву пре Обраде, осим ако тај закон не забрањује такве информације по важним основама од јавног интереса.	Добављач прикупља и електронски води сва документована упутства корпорације Microsoft, (уговор, спецификацију посла или документацију о поруџбини), на једноставно доступној локацији запосленима добављача и уговарачима који учествују у Извршењу посла.
	Одељак Б: Обавештење	
6	Добављач мора да користи Изјаву о приватности корпорације Microsoft код прикупљања Података о личности у име корпорације Microsoft. Обавештење о приватности мора бити истакнуто и доступно Лицима на које се подаци односе да би им помогло да одлуче да ли да доставе добављачу своје Податке о личности. Напомена: кад је ваша компанија руковалац активности Обраде, требате да објавите своје властито обавештење о приватности.	Добављач користи fwdlink за ажурирану, објављену Изјаву о приватности корпорације Microsoft. Изјава о приватности се објављује у било ком контексту кад ће се прикупљати Подаци о личности корисника. Ако је применљиво, ванмрежна верзија је доступна пре прикупљања података. Све коришћене ванмрежне Изјаве и приватности су најновије, објављене верзије и уредно датиране. За услуге запослених корпорације Microsoft, користи се Обавештење о приватности корпорације Microsoft.
7	Кад се прикупљају Подаци о личности корпорације Microsoft преко позива уживо или снимљеног видео позива, добављачи морају да се припреме за разговор о праксама руковања, коришћења и чувања с Лицима на које се подаци односе.	Скрипта за гласовне снимке укључује начин на који се Подаци о личности корпорације Microsoft обрађују и укључује: ▪ прикупљање, ▪ коришћење и ▪ чување

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак Ц: Избор и пристанак	
8	Кад је применљиво, добављач мора да добије и евидентира пристанак Лица на које се подаци односе за све своје активности Обраде (укључујући све нове и ажуриране активности Обраде) пре прикупљање Података о личности тог Лица на које се подаци о односе. Добављач прати ефективност управљања преференцијама да би осигурао да је временски оквир за поштивање промена у преференцијама најрестриктивнији локални законски захтев који се примењује.	Добављач може да покаже како Лице на које се подаци односе даје пристанак за активност обраде и да обим пристанка покрива све активности Обраде добављача у односу на Податке о личности тог Лица на које се подаци односе. Добављач може да покаже како Лице на које се подаци односи повлачи пристанак за активност Обраде. Добављач може да покаже како се проверавају преференције пре покретања нове активности Обраде. Напомена: докази могу да буду снимци екрана о интеракцији корисника; експериментисање с услугом или могућност прегледа техничке документације.
9	Добављачи који израђују и управљају веб-сајтовима и/или апликацијама корпорације Microsoft или сајтовима који носе бренд корпорације Microsoft морају да обезбеде Лицима на које се подаци односе транспарентно обавештење и избор у вези с коришћењем колачића у складу с обавезама у изјави о приватности корпорације Microsoft и локалним законским захтевима. Осим ако уговорна пословна јединица специфично не захтева, да би управљали контролама избора, добављачи требају да користе стандардни банер који је произвео 1ES. Овај захтев се примењује кад сајтови циљају кориснике унутар Европске уније/Европског економског региона и других региона с применљивим законима о приватности и кад год се користи Изјава о приватности корпорације Microsoft. Напомена: пословни спонзори корпорације Microsoft требају да региструју веб-сајтове корпорације Microsoft на интерном веб-порталу корпорације Microsoft за усаглашеност (http://aka.ms/wcp) да би се списак колачића унео у каталог и да би се њима управљало.	Сврха сваког колачића мора да буде документована и мора се обавестити о врсти примењеног колачића. ▪ Трајни колачићи се не смеју користити кад су колачићи сесије довољни. ▪ Кад се користе трајни колачићи, они не смеју да имају датум истека који прелази 13 месеци након што је корисник посетио сајт. Потврдити усаглашеност са законима ЕУ према потреби, као што је: ▪ коришћење конвенције о означавању, „Приватност & колачићи“ за изјаву о приватности, ▪ обезбеђење потврдног пристанка корисника пре коришћења „неесенцијалних колачића“ за намене као што су оглашавање и ▪ пристанак мора да истекне или да се поново добије не дуже од сваких 6 месеци.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак Д: Прикупљање	
10	Добављач мора да прати прикупљање Података о личности или Поверљивих података корпорације Microsoft да би осигурао да се прикупе само подаци потребни за Извршење посла.	Добављач мора да обезбеди документацију која показује да су прикупљени Подаци о личности или Поверљиви подаци корпорације Microsoft потребни за Извршење посла. Добављач на захтев доставља документовани доказ корпорацији Microsoft.
11	Пре прикупљања података од деце (како дефинише применљива надлежност), Добављач мора да добије пристанак по локалним законима о приватности.	Добављач може да обезбеди документацију која показује пристанак родитеља/старатеља. Добављач на захтев доставља документовани доказ корпорацији Microsoft.
	Одељак Е: Чување	
12	Обезбедити да се Подаци о личности или Поверљиви подаци корпорације Microsoft чувају не дуже него што је потребно за Извршење посла осим ако наставак чувања Података о личности или Поверљивих података корпорације Microsoft није потребан по закону.	Добављач поштује документоване смернице чувања или захтеве чувања које је корпорација Microsoft навела у уговору (нпр. спецификација посла, поруџбеница). Добављач на захтев доставља документовани доказ корпорацији Microsoft.
13	Обезбедити да се по нахођењу корпорације Microsoft, Подаци о личности или Поверљиви подаци корпорације Microsoft који су у поседу добављача или под његовом контролом врате корпорацији Microsoft или униште по завршетку Извршења посла или на захтев корпорације Microsoft. Унутар апликација, процеси морају да буду успостављени да би се осигурало да се подаци безбедно бришу кад се уклоне из апликације било експлицитно од стране корисника или на основу других окидача као што је старост података. Кад је неопходно уништавање Података о личности или Поверљивих података корпорације Microsoft, добављач мора да спали, пулверизује или исецка физичка средства која садрже Податке о личности и/или Поверљиве податке корпорације Microsoft.	Водити евиденцију о располагању Подацима о личности и Поверљивим подацима корпорације Microsoft (ово може да укључује враћање корпорацији Microsoft ради уништавања). Ако је уништавање потребно или га захтева корпорација Microsoft, обезбедити сертификат о уништавању који је потписао службеник добављача.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак Ф: Лица на која се подаци односе	
	Лица на која се подаци односе по закону имају одређена права, укључујући право на приступ, брисање, уређивање, извоз, ограничавање и приговор на обраду њихових Података о личности **(„Права лица на која се подаци односе“).** Кад Лице на које се подаци односе тражи да оствари своја права под законом у погледу његових/њених Података о личности корпорације Microsoft, добављач мора да омогући корпорацији Microsoft да уради следеће или да изврши ове радње у име корпорације Microsoft:	
14	помогне корпорацији Microsoft, путем одговарајућих техничких и организационих мера, кад је могуће, да испуни своје обавезе да одговори на захтеве Лица на која се подаци односе тражећи да остваре своја права као Лица на која се подаци односе без непотребног одлагања. Осим ако корпорација Microsoft није дала другачија упутства, Добављач упућује сва Лица на која се подаци односе који контактирају Добављача директно на корпорацију Microsoft да би остварили своја права као Лица на која се подаци односе.	Добављач води евиденцију о документованим процесима и процедурама да би подржао остварење права Лица на која се подаци односе. Добављач води документовани доказ о тестирању. Доказ ће бити доступан на захтев корпорације Microsoft.
15	Кад директно одговара Лицу на које се подаци односе или кад Добављач пружа онлајн механизам самоуслуге, Добављач има успостављене процесе и процедуре да би идентификовао Лице на које се подаци односе, а које подноси захтев.	Добављач је документовао начин који је користио да би идентификовао Лица корпорације Microsoft на која се подаци односе. Добављач на захтев обезбеђује документовани доказ корпорацији Microsoft.
16	Ако корпорација Microsoft затражи лоцирање Података о личности корпорације Microsoft о Лицу на које се подаци односе, а који подаци нису доступни преко онлајн механизма самоуслуге, Добављач ће уложити разумне напоре да лоцира захтеване податке и води довољно забелешки да би показао да је извршена разумна претрага.	Добављач ће водити документован доказ о успостављеним процедурама да би утврдио да ли се чувају Подаци о личности корпорације Microsoft и обезбедиће документацију на захтев корпорације Microsoft. Добављач води евиденцију показујући предузете кораке да би испунио захтеве за права Лица на која се подаци односе. Документација обухвата: ▪ датум и време захтева, ▪ мере предузете да одговори на захтев и забелешку кад је обавештена корпорација Microsoft. Добављач на захтев обезбеђује доказ о вођењу евиденције корпорацији Microsoft.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак Ф: Лица на која се подаци односе (наставак)	
17	Добављач ће саопштити Лицу на која се подаци односе кораке које та особа мора да предузме да би добила приступ или на други начин остварила своја права у погледу својих Података о личности корпорације Microsoft.	Добављач ће водити документован доказ о комуникацијама и процедурама за приступ Подацима о личности корпорације Microsoft. Добављач ће водити документован доказ и доставити тај доказ на захтев корпорацији Microsoft.
18	Забележити датум и време захтева за права Лица на које се подаци односе и мере које је предузео добављач као одговор на такве захтеве. Ако се њихов захтев одбије, по налогу корпорације Microsoft, обезбедити писано обавештење Лицу на која се подаци односе. Обезбедити евиденцију о захтевима Лица на које се подаци односе на захтев корпорације Microsoft.	Добављач води евиденцију о захтевима за приступ/брисање и документује промене направљене у Подацима о личности корпорације Microsoft. Примери документа кад су захтеви одбијени и сачуван доказ о провери и одобрењу корпорације Microsoft. Добављач ће доставити доказ о вођењу евиденције о захтевима и одбијању приступа Подацима о личности корпорацији Microsoft.
19	Добављач мора да омогући корпорацији Microsoft или да добије копију захтеваних Података о личности корпорације Microsoft за потврђено Лице на које се подаци односе у одговарајућем штампаном, електронском или вербалном формату.	Добављач доставља Податке о личности корпорације Microsoft Лицу на које се подаци односе у формату који је разумљив те у облику који је прикладан за Лице на које се подаци односе.
20	Добављач мора да предузме разумне мере опреза да би обезбедио да Подаци о личности корпорације Microsoft који су објављени корпорацији или потврђеном Лицу на које се подаци односе не могу да се користе за идентификацију друге особе.	Добављач ће водити документован доказ о процедурама повезаним с мерама опреза да би избегао идентификацију Лица на које се подаци односе супротно условима Уговора. Добављач на захтев доставља доказ корпорацији Microsoft.
21	Ако Лице на које се подаци односе верује да његови/њени Подаци о личности нису потпуни и тачни, добављач мора да изнесе проблем корпорацији Microsoft и да сарађује с корпорацијом по потреби да би се решио проблем.	Добављач документује случајеве неслагања и износи проблем корпорацији Microsoft. Добављач на захтев доставља корпорацији Microsoft документовани доказ.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак Г: Подуговарачи	
	Ако добављач намерава да користи подуговарача да обрађује Податке о личности или Поверљиве податке корпорације Microsoft, добављач мора да:	
22	обавести корпорацију Microsoft пре подуговарања услуга или вршења било каквих промена у погледу додавања или замене подуговарача. Напомена: наведите своје прихватање ове обавезе чак и ако тренутно не ангажујете подуговараче али бисте могли у будућности.	Потврдити да Податке о личности корпорације Microsoft обрађују само компаније које су познате корпорацији Microsoft како то захтева применљиви уговор (нпр. спецификација посла, додатак, поруџбеница) или како се води у ССПА бази података. Добављач мора да објави свој списак подуговарача на мрежи и да укључи везу на страници у ССПА бази података.
23	Документовати природу и обим Података о личности и Поверљивих података корпорације Microsoft које подобрађују подуговарачи, обезбеђујући да су прикупљене информације потребне за Извршење посла.	Добављач води документацију која се односи на Податке о личности и Поверљиве податке корпорације Microsoft који су откривени или пренесени подуговарачима. Добављач на захтев доставља документовани доказ корпорацији Microsoft.
24	Кад је корпорација Microsoft руковалац Подацима о личности корпорације Microsoft, обезбедити да подуговарач користи Податке о личности корпорације Microsoft у складу с наведеним преференцијама за контакт Лица на које се подаци односе.	Показати како подуговарачи користе преференцију Лица корпорације Microsoft на које се подаци односе. Обезбедити пратећу документацију (нпр. снимку, СЛА, спецификацију посла итд.), која укључује временски оквир за подуговарача да се придржава промене у преференцији.
25	Ограничити подуговарачеву обраду Података о личности и Поверљивих података корпорације Microsoft на оне намене које су неопходне да се испуни добављачев уговор с корпорацијом Microsoft.	Добављач може да обезбеди документацију која показује да су прикупљени Подаци о личности или Поверљиви подаци корпорације Microsoft који су дати подуговарачу потребни за Извршење посла. Добављач на захтев доставља документовани доказ корпорацији Microsoft.
26	Прегледати притужбе о индикацијама на сваку неовлашћену или незакониту обраду Података о личности корпорације Microsoft.	Добављач може да покаже системе и процесе који постоје да би решио притужбе у погледу уговарачевог неовлашћеног коришћења или откривања Података о личности корпорације Microsoft. Добављач на захтев доставља документовани доказ корпорацији Microsoft.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак Г: Подуговарачи (наставак)	
27	Неодложно обавестити корпорацију Microsoft по сазнању да је подуговарач обрадио Податке о личности или Поверљиве податке корпорације Microsoft за било које намене мимо оних које се односе на Извршење посла.	Добављач је обезбедио упутства и средства подуговарачу да пријави злоупотребу података корпорације Microsoft. Добављач на захтев доставља документовани доказ корпорацији Microsoft.
28	Ако добављач прикупља Податке о личности од трећих лица у име корпорације Microsoft, добављач мора да потврди да су смернице и праксе трећег лица за заштиту података усаглашене с добављачевим уговором с корпорацијом Microsoft и ДПР-ом.	Добављач може да обезбеди документацију о извршеној дубинској анализи у погледу смерница и пракси трећег лица за заштиту података. Добављач на захтев доставља документовани доказ корпорацији Microsoft.
29	Брзо предузети мере да би ублажио сваку стварну или потенцијалну штету коју је проузроковала подуговарачева неовлашћена или незаконита обрада Података о личности и Поверљивих података корпорације Microsoft.	Добављач мора да води документован доказ о плану и процедури те да на захтев достави доказ о документацији корпорацији Microsoft.
	Одељак Х: Квалитет	
30	Добављач мора да одржава интегритет свих Података о личности корпорације Microsoft, обезбеђујући да они остану тачни, потпуни и релевантни за наведене намене за које су били обрађени.	Добављач може да покаже да су успостављене процедуре да би потврдио Податке о личности корпорације Microsoft кад се прикупљају, припремају и ажурирају. Добављач може да покаже да су успостављене процедуре праћења и узорковања да би се по потреби проверила тачност на сталној основи и вршило исправљање. Добављач на захтев доставља документовани доказ корпорацији Microsoft.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак И: Праћење и спровођење	
31	Добављач има план реаговања у инцидентним ситуацијама који захтева да Добављач обавести корпорацију Microsoft по захтевима уговора или без непотребног одлагања, што год наступи раније, по сазнању о Инциденту с подацима. На захтев или по упутству корпорације Microsoft, Добављач мора да сарађује с корпорацијом Microsoft у свакој истрази, ублажавању или санацији инцидента, укључујући пружање корпорацији Microsoft података, информација, приступа Добављачевом особљу или хардверу који је потребан за вршење форензичког прегледа. Напомена: погледати Водич за програм ССПА о начину обавештавања корпорације Microsoft о инциденту.	Добављач има план реаговања у инцидентним ситуацијама који укључује корак за обавештавање клијената (Microsoft) како је описано у овом одељку. Добављач на захтев доставља документовани доказ корпорацији Microsoft.
32	Провести план санације и праћења решавања сваког Инцидента с подацима да би обезбедио да је благовремено предузета одговарајућа корективна мера.	Добављач има документоване процедуре које проводи да би реаговао на Инцидент с подацима до елиминације инцидента. Добављач на захтев доставља документовани доказ корпорацији Microsoft.
33	Кад је корпорација Microsoft руковалац Података о личности корпорације Microsoft, успоставити формални процес притужби за одговарање на све притужбе о заштити података које укључују Податке о личности корпорације Microsoft.	Добављач има начине за примање притужби које се односе на Податке о личности корпорације Microsoft, те документовану процедуру о притужбама за њихово решавање. Добављач на захтев доставља документовани доказ корпорацији Microsoft.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак J: Безбедност	
	Добављач мора да успостави, изврши и одржава програм безбедности информација који укључује смернице и процедуре да би заштитио и чувао безбедним Податке о личности или Поверљиве податке корпорације Microsoft у складу с добром индустријском праксом и како захтева закон. Добављачев програм безбедности мора да задовољи доле наведене стандарде, захтеви 34-50.	Важећа сертификација по ИСО 27001 је прихватљива замена за Одељак J. Контактирати ССПА да би се применила ова замена. Напомена: требаћете доставити сертификацију.
34	Извршити годишње процене безбедности мреже које укључују: ▪ преглед главних промена у окружењу као што су компонента система, топологија мреже, правила заштитног зида, ▪ вршење скенирања рањивости и ▪ вођење дневника промена.	Добављач има документоване процене мреже, дневнике промена и резултате скенирања. Потребни дневник промена мора да прати промене, пружи информације у погледу разлога за промену, те да укључује име и функцију именованог одобраваоца.
35	Добављач мора да дефинише, саопшти и примени смернице за мобилни уређај које обезбеђују и ограничавају коришћење Података о личности или Поверљивих података корпорације Microsoft којим приступа или користи на мобилном уређају.	Добављач показује коришћење усаглашених смерница о мобилном уређају кад обрада Података о личности или Поверљивих података корпорације Microsoft захтева коришћење мобилног уређаја.
36	Сва средства која се користе као подршка Извршењу посла морају бити евидентирана и имати идентификованог власника. Добављач је одговоран за вођење инвентара о овим информационим средствима, успостављајући прихватљиво и одобрено коришћење тих средстава; и обезбеђујући одговарајући ниво заштите средстава током њиховог целог века трајања.	Инвентар уређаја који се користе за подршку Извршењу посла. Инвентар ових средстава треба да укључује: ▪ локацију уређаја, ▪ класификацију података на средству, ▪ евиденцију о повраћају средстава по престанку радног односа или пословног уговора, и ▪ евиденцију о одлагању медија за складиштење података кад више нису потребни.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак J: Безбедност (наставак)	
37	Успоставити и одржавати процедуре управљања правима приступа да би се спречио неовлашћени приступ свим Подацима о личности или Поверљивим подацима корпорације Microsoft који су под контролом добављача.	Добављач доказује да је применио план управљања правима приступа који укључује: ▪ процедуре контроле приступа, ▪ процедуре идентификације, ▪ процедуре закључавања након неуспешних покушаја, ▪ јаке параметре за одабир акредитива за аутентификацију, и ▪ деактивацију корисничких налога о раскиду запослења у року од 48 часова ▪ јаке контроле лозинки које намећу дужину лозинке, сложеност те спречавају да се поново користи Добављач показује да је успоставио процес да би проверио приступ корисника Подацима о личности и поверљивим подацима корпорације Microsoft. Овај процес укључује: ▪ јасно дефинисане корисничке улоге, ▪ процедуре да би се прегледало и оправдало одобрење приступа функцијама и ▪ тестове да корисници у оквиру функција с приступом подацима корпорације Microsoft имају документовано оправдање да буду у групи/ функцији.
38	Дефинисати и применити процедуре управљања закрпом које дају приоритет безбедносним закрпама за системе који се користе за обраду Података о личности и Поверљивих података корпорације Microsoft. Ове процедуре укључују: ▪ дефинисани приступ ризику да би се дао приоритет безбедносним закрпама ▪ способност руковања и примене хитних закрпа, ▪ применљивост на оперативни систем и серверски софтвер као што су сервер апликација и софтвер базе података, ▪ документовање ризика који се ублажава закрпом и праћење било каквих изузетак, и ▪ услове за повлачење софтвера који ауторско друштво више не подржава.	Добављач може показати примењену процедуру управљања закрпом која задовољава овај захтев и минимално, покрива следеће: ▪ додељивање озбиљности ради информисања о одређивању приоритета. (Дефиниције озбиљности су документоване.) ▪ Документовану процедуру за спровођење хитних закрпа. ▪ Потврду да нема користи од оперативних система које ауторско друштво више не подржава. ▪ Евиденцију управљања закрпама која прати одобрења и изузетке.
39	Инсталирати антивирусни и анти-малвер софтвер на опрему повезану на мрежу која се користи за обраду Података о личности и Поверљивих података корпорације Microsoft, укључујући сервере, десктоп рачунаре за производњу и обуку ради заштите од	Евиденције постоје да би се показало да је активно коришћење антивирусног и анти-малвер софтвера. Напомена: овај захтев се примењује на све оперативне системе.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак J: Безбедност (наставак)	
	потенцијално штетних вируса и злонамерних софтверских апликација. Ажурирати дневно дефиниције анти-малвера или према упутствима добављача анти-вируса/анти-малвера. Напомена: ово се примењује на све оперативне системе укључујући Linux.	
40	Добављачи који развијају софтвер за корпорацију Microsoft морају укључити принципе безбедности по дизајну у процес изградње.	Документација о техничкој спецификацији добављача укључује контролне тачке за безбедносну проверу у њиховим развојним циклусима.
41	Користити програм за спречавање губитка података („**ДЛП**“) да би се спречили упади, губитак и друге неовлашћене активности. Подаци морају бити правилно класификовани, означени и заштићени, а добављач мора да прати коришћене информационе системи у којима се обрађују Подаци о личности и Поверљиви подаци корпорације Microsoft ради упада, губитка и других неовлашћених активности. ДЛП програм, минимално: ▪ захтева коришћење стандардног индустријског хоста, мреже и Система за откривање упада у облаку („**ИДС**“) ако чувате Податке о личности и Поверљиве податке корпорације Microsoft, ▪ захтева коришћење напредних Система за заштиту од упада („**ИПС**“) који је конфигурисан да прати и активно зауставља губитак података, ▪ у случају да је систем пробијен, потребна је анализа система да би се обезбедило да су све преостале рањивости такође решене, ▪ описати потребне процедуре за праћење алата за откривање угрожености система, ▪ успоставља реакцију на инцидент и процес који се мора извршити кад се открије Инцидент с подацима и ▪ захтева комуникацију (за све запослене добављача и подуговарача који се искључују из добављачевог Извршења посла) у вези с неовлашћеним преузимањем и коришћењем Података о личности и Поверљивих података корпорације Microsoft.	Документовани ДЛП програм примењен с успостављеним процедурама да би се спречили упад, губитак и друге неовлашћене активности (и минимално, све ставке наведене у овом одељку).
42	Неодложно саопштити вишем руководству и корпорацији Microsoft резултате истраге реаговања на инцидент.	Системи и процеси морају да буду успостављени да би се корпорацији Microsoft саопштили резултати истраге реаговања на инцидент.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак J: Безбедност (наставак)	
43	Администратори система, оперативно особље, менаџмент и трећа лица морају проћи годишњу обуку из безбедности.	Успоставити програм обуке из безбедности који укључује: ▪ годишњу обуку из реаговања на инциденте, и ▪ симулиране догађаје и аутоматизоване механизме да би се олакшало ефикасно реаговање на кризне ситуације. ▪ Свесност о превенцији инцидената као што су ризици повезани с преузимањем злонамерног софтвера.
44	Добављач мора да обезбеди да процеси планирања резервних копија штите Податке о личности и Поверљиве податке корпорације Microsoft од неовлашћеног коришћења, приступа, откривања, измене и уништавања.	Добављач може да покаже документоване процедуре реаговања и опоравка с детаљима о томе како ће организација управљати ометајућим догађајем и одржавати своју безбедност информација на унапред одређеном нивоу на основу циљева сталне безбедности информација које је одобрио менаџмент. Добављач може да покаже да је дефинисао и применио процедуре за периодично прављење резервних копија, безбедно складиштење и ефикасно обнављање критичних података.
45	Успоставити и тестирати континуитет пословања и планове опоравка од катастрофе.	План опоравка од катастрофе мора да садржи следеће: ▪ дефинисане критеријуме за одређивање да ли је систем критичан за операције јединице добављача. ▪ Списак критичних система на основу дефинисаних критеријума који морају бити циљани за опоравак у случају катастрофе. ▪ Дефинисану процедуру опоравка од катастрофе за сваки критични систем која осигурава да инжењер који не познаје систем може поправити апликацију за мање од 72 сата. ▪ Годишње (или чешће) тестирање и преглед планова опоравка од катастрофе да би се осигурало да се циљеви опоравка могу испунити.
46	Потврдити идентитет појединца пре него што му се да приступ Подацима о личности и Поверљивим подацима корпорације Microsoft и уверити се да је приступ ограничен на обим активности одређеног појединца који је дозвољен за подршку Извршењу посла.	Уверити се да су сви кориснички ИД-ови јединствени и да сваки има индустријски стандардни метод аутентификације, као што је Azure Active Directory. Повишени приступ (административни или други типови побољшаних привилегија) мора да захтева коришћење другог фактора, као што је паметна картица или аутентификатор заснован на телефону.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
Одељак J: Безбедност (наставак)		
		Документовани програм безбедности информација који покрива процес којим се обезбеђује да сви запослени добављача и подуговарача приступе Подацима о личности и Поверљивим подацима корпорације Microsoft не више или дуже него што је потребно за подршку Извршењу.
47	Добављач мора да заштити све податке који се обрађују у вези с његовим извршењем у транзиту кроз мреже са шифровањем користећи Безбедност транспортног слоја („**ТЛС**“) или безбедност Интернет протокола („**ИПсец**“). Ове методе су описане у НИСТ 800-52 и НИСТ 800-57; може се користити и еквивалентан индустријски стандард. Добављач мора да одбије испоруку било којих Података о личности и Поверљивих података корпорације Microsoft пренетих путем нешифрованих средстава.	Процес креирања, примене и замене ТЛС-а или других сертификата мора да буде дефинисан и примењен.
48	Сви уређаји добављача (лаптопови, радне станице, итд.) који ће приступити или руковати Подацима о личности и Поверљивим подацима корпорације Microsoft морају користити шифровање засновано на диску.	Шифровати све уређаје да би се испунио BitLocker или друго еквивалентно индустријско решење за шифровање диска за све клијентске уређаје који се користе за руковање Подацима о личности и Поверљивим подацима корпорације Microsoft.
49	Системи и процедуре (користећи тренутне индустријске стандарде, као што су они описани у стандарду **НИСТ 800-111**) морају бити успостављени за шифровање у мировању (кад су ускладиштени) било којих и свих Података о личности и/или Поверљивих података корпорације Microsoft, примери укључују, али нису ограничени на: ▪ податке о акредитивима (нпр. корисничко име/лозинке) ▪ податке о инструменту плаћања (нпр. кредитна картица и бројеви банковног налога) ▪ податке о личности повезане с имиграцијом ▪ податке о медицинском профилу (нпр. бројеви медицинског картона или биометријски маркери или идентификатори, као што су ДНК, отисци прстију, мрежњаче ока и шаренице, обрасци гласа, обрасци лица и мерења руку, који се користе у сврхе провере аутентичности)	Проверите да су Подаци о личности и Поверљиви подаци корпорације Microsoft шифровани у стању мировања.

#	Захтеви за заштиту података за добављаче корпорације Microsoft	Доказ о усаглашености
	Одељак J: Безбедност (наставак)	
	▪ податке о идентификатору који је издала држава (нпр. бројеви социјалног осигурања или возачке дозволе) ▪ податке који припадају клијентима корпорације Microsoft (нпр. SharePoint, O365 документи, OneDrive клијенти) ▪ материјале повезане с ненајављеним производима корпорације Microsoft ▪ датум рођења ▪ информације о профилима деце ▪ географске податке у реалном времену ▪ физичку личну (није пословна) адресу ▪ личне (нису пословни) телефонске бројеве ▪ религију ▪ политичка мишљења ▪ сексуалну оријентацију/преференцију ▪ одговоре на безбедносна питања (нпр. 2фа, поновљено постављање лозинке) ▪ девојачко презиме мајке	
50	Анонимизовати све Податке о личности корпорације Microsoft који се користе у развојном или тестном окружењу.	Подаци о личности корпорације Microsoft не смеју се користити у развојним или тестним окружењима; кад нема алтернативе, морају бити анонимизовани да би се спречила идентификација Лица на која се подаци односе или злоупотреба Података о личности. Напомена: анонимизовани подаци се разликују од псеудонимизованих података. Анонимизовани подаци су подаци који се не односе на идентификовано физичко лице или физичко лице које се може идентификовати кад Лице на која се подаци односе није идентификовано или се више не може идентификовати.

Глосар

„Овлашћени представник“ је особа која има одговарајући ниво овлашћења да потписује у име компаније**.** Ова особа би имала потребно знање о приватности и безбедности или би се консултовала са стручњаком о теми пре него што би поднела свој одговор на меру у ССПА програму. Поред тога, додавањем свог имена у ССПА образац, они потврђују да су прочитали и разумели ДПР.

„ЕУДПР“ подразумева Уредбу (ЕУ) 2018/1725 Европског парламента и Савета од 23. октобра 2018. о заштити физичких лица у погледу обраде података о личности од стране институција, органа, канцеларија и агенција Уније и слободном кретању таквих података и укидање Уредбе (ЕЗ) бр. 45/2001 и Одлуке бр. 1247/2002/ЕЗ.

„Слободни сарадник“ подразумева појединце који обављају задатке или услуге на захтев, а које се набављају преко дигиталних платформи или на други начин.

„ГДПР“ подразумева Уредбу (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. о заштити физичких лица у погледу обраде података о личности и слободном кретању таквих података и укидање Директиве бр. 95/46/ЕЗ (Општа уредба о заштити података).

„Захтеви за заштиту приватности података “ подразумевају ГДПР, ЕУДПР, локалне законе ЕУ/ЕЕА о заштити података, калифорнијски закон о приватности потрошача, Кал. Див. Закон § 1798.100 и даље. (*„ЦЦПА“*), Закон о заштити података Уједињеног Краљевства из 2018. и све повезане или накнадне законе, прописе и друге правне захтеве који се примењују у УК, као и све применљиве законе, прописе и друге правне захтеве који се односе на (а) приватност и безбедност података; или (б) коришћење, прикупљање, задржавање, складиштење, безбедност, откривање, пренос, одлагање и другу обраду било којих Података о личности.

„Моделне клаузуле ЕУ“ и „Стандардне уговорне клаузуле“ подразумевају (i) стандардне клаузуле о заштити података за пренос података о личности обрађивачима основаним у трећим земљама које не обезбеђују адекватан ниво заштите података, како је описано у члану 46. ГДПР-а и одобрено одлуком Европске комисије (ЕУ) 2021/914 од 4. јуна 2021. године; (ii) све накнадне стандардне уговорне клаузуле које је усвојила (а) Европска комисија, (б) Европски супервизор за заштиту података и одобрила Европска комисија, (ц) Уједињено Краљевство у складу с Општим савезним актом Уједињеног Краљевства о заштити података, (д) Швајцарска у складу са швајцарским савезним законом о заштити података, или (е) страна влада у надлежности која није Швајцарска, Уједињено Краљевство и надлежности које су у саставу Европске уније/Европског економског региона где клаузуле регулишу међународни пренос података о личности, биће укључени и обавезујући за Добављача од дана њиховог усвајања.

„Хостовање веб-сајтова“ -услуга хостовања веб-сајтова је онлајн услуга која креира и/или одржава веб-сајтове у име корпорације Microsoft под њеном доменом, тј. добављач обезбеђује све материјале и услуге потребне за креирање и одржавање сајта и чини га доступним на Интернету. „Добављач услуга веб-хостовања“ или „веб-хост“ је добављач који обезбеђује алате и услуге потребне да би веб-сајт или веб-страница били прегледани на Интернету, као што су колачићи или веб-светионици за оглашавање.