

UGOVOR O DAVANJU SOFTVERSKOG RJEŠENJA ZA ZAŠTITU SIGURNOSTI ZA MICROSOFT OFFICE 365

Ovaj Ugovor ("Ugovor") sadrži uslove potrebne za vaš pristup i upotrebu softverskog rješenja Kaspersky Security for Microsoft Office 365 ("Proizvod") i podrazumijeva dogovor između firme AO Kaspersky Lab ("Kaspersky Lab" ili "Kaspersky") i vas ("Korisnik" ili "Vi"), kao organizacije koja je ovlastila fizičko lice da sklopi ovaj Ugovor za i u ime Vas. Ovaj Ugovor stupa na snagu kada kliknete na tipku "prihvatam" ili označite kockicu što ukazuje da prihvatate ove uslove.

Ukoliko postoji odvojeni ugovor koji je sklopljen između Kaspersky Lab-a i Vas ili između Vas i odgovarajućeg ovlaštenog partnera Kaspersky Lab-a ("Partner") do nivoa do kojeg je odvojeni ugovor ("Odvojeni ugovor") između Kaspersky Lab-a ili Partnera i Vas u sukobu sa bilo kojim odredbama ovog Ugovora, prevlađaće Odvojeni ugovor.

DIO A: OPŠTI USLOVI

1. Opis Proizvoda

Kaspersky Security for Microsoft Office 365 je softversko rješenje koje je namijenjeno za zaštitu online mailboksova kojim se upravlja putem Office-a 365. E-mail poruke se skeniraju zbog virusa, Trojanaca i drugih vrsta malvera koji se mogu prenijeti putem e-maila, kao i zbog spam-a i phishing-a.

Softversko rješenje Security for Microsoft Office 365 može izvršiti slijedeće operacije:

- **skeniranje e-mail poruka u korisničkim mailboksovima zbog malvera,**
- **filterisanje neželjene pošte (spam) iz korisničkih mailboksova,**
- **skeniranje e-mail poruka zbog phishing-a i zlonamjernih linkova,**
- **filterisanje priloga u e-mail porukama,**
- **premještanje poruka u podršku radi sprječavanja zaraze,**
- **davanje zajedničkog stava o stavkama koje se nalaze u podršci Kaspersky Security i karantinu Exchange Online, što administratoru omogućava da pregleda sve prekršaje sigurnosti i, ako bude potrebno, da locira i objavi odabrane stavke,**
- **obavještanje o porukama sa zlonamjernim objektima, filterisanim priložima i/ili phishing-om,**
- **prikazivanje statistike i generisanje izvještaja o aktivnosti Proizvoda.**

Kaspersky Security for Microsoft Office 365 napravljen je na infrastrukturi Kaspersky Lab-a.

Funkcionalnost Kaspersky Security for Microsoft Office 365 nalazi se u rubrici online podrška ("Online podrška").

2. Davanje i ograničenja Licence

- 2.1. **Licenca.** Kaspersky Lab daje Korisniku neisključivu, neprenosivu ograničenu licencu za pristup i upotrebu Proizvoda po ovom Ugovoru i samo u internu poslovnu svrhu Korisnika. Korisnik se mora pridržavati svih tehničkih zahtjeva iz Online podrške. Dodatni uslovi i ograničenja upotrebe Proizvoda biće definisani u primjenljivom Sertifikatu licence (u skladu sa dole navedenom definicijom) i/ili u Odvojenom ugovoru.

- 2.2. **Sertifikat licence.** Sertifikat licence je odvojeni dokument koji Kaspersky Lab napravi nakon izvršenja naloga od strane Korisnika. Sertifikat licence sadrži glavne informacije i opis licence za Proizvod(e).
- 2.3. **Pristup Proizvodu.** Proizvod je obezbijeđen putem davanja korisničkog pristupa web portalu na cloud.kaspersky.com ("Portal"). Korisnik će identifikovati korisničko ime i lozinku koje koristi za pristup svom računu na Portalu. Korisnik neće dati svoje korisničko ime ili lozinku ni jednom trećem licu i biće odgovoran za djela ili propuste bilo kojeg lica koje pristupa Proizvodu putem lozinki ili procedura pristupa koje su obezbijeđene Korisniku. Kaspersky Lab zadržava pravo da odbije registraciju ili da obustavi ili otkáže informacije za prijavu koje Korisnik koristi za pristup Proizvodu iz bilo kojeg razloga, uključujući prekršaj uslova iz ovog Ugovora od strane Korisnika.
- 2.4. Kaspersky Lab zadržava pravo da bilo kada promijeni Proizvod i/ili njegove komponente uključujući ali bez ograničenja Softver, Online podršku.
- 2.5. Osim UOP (kako je definisano u dijelu USLOVI OBRADE I ZAŠTITE PRIVATNOSTI PODATAKA), Kaspersky Lab zadržava pravo da bilo kada promijeni ovaj Ugovor i da nametne nove ili dodatne uslove upotrebe Proizvoda. Te promjene će odmah stupiti na snagu kada se uvrste u Ugovor. Vaša stalna upotreba Proizvoda smatraće se njegovim prihvatanjem.

3. Obaveze Korisnika

- 3.1. Korisnik se mora pridržavati svih tehničkih ograničenja Proizvoda koji su utvrđeni u Online podršci.
- 3.2. Korisnik se mora pridržavati svih zakona i propisa u vezi sa njegovom upotrebom Proizvoda, uključujući ali bez ograničenja sve važeće zakone o privatnosti, ličnim podacima, zaštiti podataka i povjerljivosti komuniciranja. Korisnik je odgovoran za davanje odgovora na bilo koji zahtjev neke treće strane o njegovoj upotrebi Proizvoda.
- 3.3. Korisnik neće prodati, iznajmiti, unajmiti ili posuditi Proizvod i/ili Softver bilo kojoj trećoj strani ili koristiti Proizvod za kreiranje vlastitih proizvoda ili usluga detektovanja, blokiranja ili tretiranja prijetnji ili u bilo koju drugu svrhu.
- 3.4. Korisnik ne može ukinuti ili mijenjati bilo koja autorska ili druga vlasnička prava na Proizvod, dokumentaciju ili materijale u vezi s njim.
- 3.5. Korisnik ne može ispitivati, skenirati ili testirati ranjivost Proizvoda ili Portala ili bilo kojeg srodnog sistema ili mreže, ili prekršiti bilo koje mjere sigurnosti ili provjere vezano za Proizvod i Portal i takve sisteme i mreže.
- 3.6. Ukoliko Korisnik prekrši bilo koju svoju obavezu ili ograničenje licence iz ovog Ugovora ili drugog zakonski obavezujućeg dokumenta koji je potpisan između Korisnika i Kaspersky Lab-a i/ili Partnera, Kaspersky Lab može otkazati licencu i onemogućiti upotrebu Proizvoda.

4. Trajanje i raskid

- 4.1. **Trajanje.** Početni datum isteka licence utvrđen je u Sertifikatu licence. Korisnik može obnoviti licencu na Proizvod za jedan ili više dodatnih vremenskih perioda nakon potpisivanja dodatne narudžbe za Proizvod. U tom slučaju Korisnik ima licencu za upotrebu Proizvoda u periodu obnavljanja. Ovaj Ugovor ostaće na snazi tokom cijelog perioda trajanja licence ("Trajanje licence").
- 4.2. **Raskid.** U slučaju da Korisnik izvrši materijalni prekršaj ovog Ugovora, Kaspersky Lab može odmah raskinuti ovaj Ugovor i Licencu za upotrebu Proizvoda putem pismene obavijesti Korisniku. Ako dođe do bilo kojeg drugog prekršaja ovog Ugovora, Kaspersky Lab može poslati pismenu obavijest Korisniku o tom prekršaju u roku od petnaest (15) dana i ukoliko Korisnik ne riješi taj problem u roku od petnaest (15) dana, Kaspersky Lab može odmah raskinuti ovaj Ugovor. Nakon svakog raskida, pravo Korisnika da koristi i pristupa Proizvodu biće oduzeto.

5. Plaćanje

- 5.1. **Plaćanje.** Licencne naknade i svi važeći porezi dospijevaju na plaćanje u periodu koji je definisan na fakturi koju Kaspersky Lab ili Partner dostave Korisniku.

6. Testna upotreba

- 6.1. Korisnik može naručiti verziju Proizvoda za testnu upotrebu. Nakon što Kaspersky Lab dobije narudžbu, Korisnik može pristupiti i koristiti Proizvod samo u svrhu analize i bez upotrebe u proizvodnji. Korisnik može koristiti Proizvod trideset (30) dana u skladu s ovom Klauzulom. Ako Kaspersky Lab utvrdi drugi rok testnog perioda, Korisnik će biti obaviješten prije nego što Korisniku da dozvolu za pristup i upotrebu. Kaspersky Lab ne daje tehničku podršku za vrijeme testne upotrebe Proizvoda.

7. Tehnička podrška

- 7.1. Tokom ugovorenog perioda licence Kaspersky Lab daje Korisniku tehničku podršku za Proizvod (osim za vrijeme testne upotrebe Proizvoda) u skladu sa pravilima tehničke podrške. Pravila tehničke podrške mogu se naći na stranici <https://support.kaspersky.com>.

8. Elektronsko obavještanje

- 8.1. Kaspersky Lab može dostaviti Korisniku bitne informacije i obavijesti o Proizvodu elektronskim putem, uključujući putem e-maila i Portala. U tu svrhu Kaspersky Lab može koristiti sve potrebne informacije o Vama, uključujući informacije o Korisnikovom računu na Portalu.

9. Ograničenje odgovornosti i odricanje

- 9.1. Proizvod može sadržavati ili pokazati linkove na web stranicama ili resursima trećih strana u vezi sa Proizvodom. Kaspersky Lab daje te linkove samo radi praktičnosti i nije odgovoran za sadržaj, resurse ili linkove za proizvode ili usluge koje pružaju. Samo vi ste odgovorni i preuzimate kompletan rizik kada koristite web stranice ili resurse treće strane.

- 9.2. Kaspersky Lab i/ili Partneri nisu odgovorni za bilo koje kašnjenje, propuste i odricanje pristupa Proizvodima koje može prouzrokovati Vaš davalac mobilne ili usluge Interneta.
- 9.3. OSIM OVDJE NAVEDENIH OBAVEZA KASPERSKY LAB-A PROIZVOD JE OBEZBIJEĐEN U ORIGINALNOM STANJU I KASPERSKY LAB NE ZASTUPA I NE GARANTUJE NJEGOVU UPOTREBU ILI IZVEDBU. OSIM BILO KOJE GARANCIJE, USLOVA, ZASTUPANJA ILI ROKA DO KOJEG NE MOŽE BITI ISKLJUČEN ILI OGRANIČEN PUTEM VAŽEĆEG ZAKONA. KASPERSKY LAB I NJEGOVI PARTNERI NE DAJU NIKAKVU GARANCIJU, USLOV, ZASTUPANJE ILI ROK (IZRIČIT ILI IMPLICITAN, BILO PO STATUTU, ZAKONU, OBIČAJU, UPOTREBI ILI DRUGAČIJE) ZA BILO KOJU STVAR UKLJUČUJUĆI, BEZ OGRANIČENJA, NEKRŠENJE PRAVA TREĆE STRANE, SPREMNOSTI ZA PRODAJU, ZADOVOLJAVAJUĆI KVALITET, INTEGRACIJU ILI PRIMJENU ZA ODREĐENU SVRHU. KORISNIK PREUZIMA SVU ODGOVORNOST I SAV RIZIK PO PITANJU IZVEDBE I ODGOVORNOST ZA IZBOR PROIZVODA RADI POSTIZANJA REZULTATA KOJE JE KORISNIK PLANIRAO, KAO I ZA INSTALACIJU, UPOTREBU I REZULTATE DOBIJENE OD PROIZVODA. BEZ OGRANIČENJA PRETHODNIH ODREDBI, KASPERSKY LAB NE ZASTUPA I NE GARANTUJE DA ĆE PROIZVOD BITI BEZ GREŠKE ILI BEZ PREKIDA ILI DRUGIH SMETNJI ILI DA ĆE PROIZVOD ISPUNITI BILO KOJI ILI SVE KORISNIČKE ZAHTJEVE BEZ OBZIRA DA LI SU OTKRIVENI KASPERSKY LAB-U.

10. Isključenje i ograničenje odgovornosti

- 10.1. DO MAKSIMALNOG ZAKONSKI DOZVOLJENOG NIVOA, NI U KOJEM SLUČAJU KASPERSKY LAB NEĆE BITI ODGOVORAN ZA BILO KOJE SPECIJALNE, SLUČAJNE, KAZNENE, INDIREKTNE ILI POSREDNE ŠTETE (UKLJUČUJUĆI, ALI BEZ OGRANIČENJA, ŠTETE ZBOG GUBITKA PROFITA ILI POVJERLJIVE ILI DRUGE INFORMACIJE, PREKIDA POSLOVANJA, GUBITKA PRIVATNOSTI, KORUPCIJE, ŠTETE I GUBITKA PODATAKA ILI PROGRAMA, PROPUSTA U IZVRŠENJU BILO KOJE OBAVEZE UKLJUČUJUĆI BILO KOJU ZAKONSKU OBAVEZU, OBAVEZU DOBRONAMJERNOSTI ILI RAZUMNE BRIGE, NEMAR, EKONOMSKI GUBITAK I BILO KOJI DRUGI FINANSIJSKI ILI DRUGI GUBITAK) ZBOG ILI U VEZI S UPOTREBOM ILI NEMOGUĆNOSTI UPOTREBE PROIZVODA, DAVANJA ILI NEDAVANJA PODRŠKE ILI DRUGIH PROIZVODA, INFORMACIJE, USLUGE I SRODNOG SADRŽAJA PUTEM PROIZVODA ILI DRUGAČIJE KAO REZULTAT UPOTREBE PROIZVODA, ILI DRUGAČIJE U OKVIRU ILI U VEZI SA BILO KOJOM UGOVORNOM ODREDBOM, ILI ŠTO PROISTIČE IZ BILO KOJEG PREKRŠAJA UGOVORA ILI BILO KOJEG DELIKTA (UKLJUČUJUĆI NEMAR, POGREŠNO PREDSTAVLJANJE, BILO KOJU STRIKTNU ODGOVORNOST ILI DUŽNOST), ILI BILO KOJEG PREKRŠAJA ZAKONSKE OBAVEZE, ILI BILO KOJEG PREKRŠAJA GARANCIJE KASPERSKY LAB-A, ČAK I AKO JE KASPERSKY LAB OBAVIJEŠTEN DA SU TAKVE ŠTETE MOGUĆE.

11. Vlasništvo nad intelektualnom imovinom

- 11.1. Prihvatate da su Proizvod i autorstvo, sistemi, ideje, metode rada, dokumentacija i ostale informacije o Proizvodu intelektualno vlasništvo i/ili poslovna tajna Kaspersky Lab-a ili njegovih Partnera i da su Kaspersky Lab i njegovi Partneri, kako bude primjenljivo, zaštićeni građanskim i krivičnim zakonom i zakonom o autorskim pravima, poslovnoj tajni, zaštitnim oznakama i patentima u Ruskoj Federaciji, Evropskoj Uniji i SAD, kao i ostalim zemljama i međunarodnim ugovorima. Ovaj Ugovor ne daje Vam nikakva prava na intelektualno vlasništvo, uključujući bilo koje zaštitne znakove ili servisne znakove Kaspersky Lab-a i/ili njegovih Partnera ("Zaštitne znakove"). Zaštitne znakove možete koristiti samo radi identifikacije odštampanog materijala koji je Proizvod napravio u skladu sa prihvaćenom praksom, uključujući identifikaciju imena vlasnika Zaštitnog znaka. Takva upotreba bilo kojeg Zaštitnog znaka ne daje vam pravo vlasništva na taj Zaštitni znak. Kaspersky Lab i/ili njegovi Partneri imaju i zadržavaju sva prava, vlasništvo i interes za Proizvod, uključujući bez ograničenja sve korekcije grešaka, unapređenja, ažuriranja ili druge modifikacije Proizvoda, bilo da ih je izvršio Kaspersky Lab ili bilo koja treća strana, i sva autorska prava, patente, prava poslovne tajne, zaštitne znakove i ostala prava intelektualnog vlasništva. Vaše posjedovanje, instalacija ili upotreba Proizvoda ne podrazumijeva nikakav prenos na vas bilo kojeg prava na intelektualno vlasništvo u Procesoru, i nećete steći nikakva prava na Proizvod osim izričito u skladu s ovim Ugovorom. Sve kopije Proizvoda moraju sadržavati iste obavijesti o vlasništvu koje se pojavljuju na i u Proizvodu. Osim kako je ovdje navedeno, ovaj Ugovor ne daje Vam nikakva prava intelektualnog vlasništva na Proizvod i potvrđujete da Vam licenca, po donjoj definiciji, dodijeljena u okviru ovog Ugovora daje samo pravo na ograničenu upotrebu u skladu s ovim Ugovorom. Kaspersky Lab zadržava sva prava koja vam nisu izričito data u ovom Ugovoru.
- 11.2. Prekršaj intelektualnih prava na Proizvod prouzrokuje građansku, administrativnu i kaznenu odgovornost u skladu sa zakonom.

12. Vladajući zakon

- 12.1. Osim po dole navedenim Klauzulama 12.2. i 12.3., ovaj Ugovor će se pridržavati i biti tumačen po zakonima koji su navedeni u donjem tekstu za zemlju ili teritoriju na kojoj ste dobili Sertifikat licence, bez pozivanja na ili primjene principa zakonskih konflikata, kako slijedi:
- a. Rusija. Ako ste Sertifikat licence dobili u Rusiji, zakoni Ruske Federacije.
 - b. SAD, Portoriko, Američka Samoa, Guam i Američka Djevičanska Ostrva. Ukoliko ste Sertifikat licence dobili u prethodno navedenim zemljama, zakoni Masačusetsa, SAD, međutim, pod uslovom da zakoni američke države u kojoj živite budu mjerodavni za zahtjeve po pitanju zaštite korisnika, nelojalne konkurencije ili sličnih zakona. Do maksimalnog zakonski dozvoljenog nivoa, Kaspersky Lab i vi ovim izričito prihvatate da se odreknete bilo kojeg prava na suđenje pred porotom.
 - c. Kanada. Ako ste Sertifikat licence dobili u Kanadi, zakoni Provincije Ontario.
 - d. Meksiko. Ako ste Sertifikat licence dobili u Meksiku, savezni zakoni Republike Meksiko.
 - e. Evropska Unije (EU). Ako ste Sertifikat licence dobili u zemlji članici EU, zakoni Njemačke.

- f. Australija. Ako ste Sertifikat licence dobili u Australiji, zakoni države ili teritorije na kojoj ste dobili Licencu.
 - g. Specijalna administrativna oblast (SAO) Hong Konga i SAO Makao. Ako ste Sertifikat licence dobili u SAO Hong Kong ili SAO Makao, zakoni SAO Hong Konga.
 - h. Tajvan. Ako ste Sertifikat licence dobili u Tajvanu, zakoni Tajvana.
 - i. Japan. Ako ste Sertifikat licence dobili u Japanu, zakoni Japana.
 - j. Bilo koja druga zemlja ili teritorija. Ako ste Sertifikat licence dobili u nekoj drugoj zemlji, primijenit će se zakoni zemlje u kojoj je izvršena kupovina.
- 12.2. Uprkos prethodnog, ukoliko zakoni ili građanska politika bilo koje zemlje ili teritorije na kojoj je ovaj Ugovor sproveden ili protumačen zabranjuju primjenu ovdje definisanog zakona, onda će se primijeniti zakoni te zemlje ili teritorije do nivoa koji je potreban u skladu sa tim zakonima ili građanskom politikom. Isto tako, ako ste pojedinačni potrošač, odredbe Klauzule 12.1. neće uticati na bilo koje pravo koje možete imati na djelovanje u zemlji u kojoj boravite po zakonima te zemlje.
- 12.3. Ovaj Ugovor neće se tumačiti po Konvenciji UN-a o ugovorima o međunarodnoj prodaji robe, čija primjena je izričito isključena.
- 12.4. Korisnik je odgovoran za stupanje u direktni kontakt samo sa Kaspersky Lab-om ili njegovim Partnerima u slučaju bilo kakvih problema sa Proizvodom.

13. Period za pokretanje postupka

- 13.1. Ni jedna strana ne može pokrenuti ni jedan postupak, bez obzira na njegovu formu, koji nastane iz transakcija u okviru ovog Ugovora više od jedne (1) godine nakon što uzrok tog postupka nastane, ili se otkrije da je nastao, osim što se može pokrenuti postupak u slučaju povrede prava intelektualnog vlasništva u maksimalno važećem zakonskom periodu.

14. Cijeli Ugovor; odvojivost odredbi; bez odricanja

- 14.1. Ako neki nadležni sud utvrdi da je bilo koja odredba ovog Ugovora nevažeća ili nesprovodiva iz bilo kojeg razloga, u cjelosti ili djelimično, ta odredba biće prilagođena tako da bude zakonita i sprovodiva, i cijeli Ugovor neće propasti zbog toga a bilans Ugovora će se nastaviti u punoj snazi do maksimalnog zakonski dozvoljenog nivoa zadržavajući, do maksimalno mogućeg nivoa, svoju prvobitnu svrhu. Odricanje bilo koje odredbe ili uslova neće biti važeće osim ako je u pismenoj formi potpisano od strane vas i ovlaštenog predstavnika Kaspersky Lab-a pod uslovom da odricanje bilo kojeg prekršaja bilo koje odredbe ovog Ugovora neće predstavljati odricanje bilo kojeg prethodnog, trenutnog ili naknadnog prekršaja. Propust Kaspersky Lab-a da insistira na strogom izvršenju bilo koje odredbe ovog Ugovora ili prava neće se tumačiti kao odricanje bilo koje takve odredbe ili prava.

DIO B: OBRADA PODATAKA I USLOVI ZAŠTITE PRIVATNOSTI

1. Obrada podataka u ime Korisnika

- 1.1. Korisnik koristi Proizvod za zaštitu Exchange Online mailboksova pod kontrolom Korisnika, kada Korisnik prikuplja, čuva i obrađuje podatke, što može obuhvatiti lične podatke ("Korisnički podaci").
- 1.2. Korisnički podaci, uključujući Lične podatke po definiciji iz Propisa EU o zaštiti opštih podataka 2016/679 ("GDPR"), koji su dostavljeni Kaspersky Lab-u u ime Korisnika, ako ih ima, i njihova obrada biće primijenjeni po rokovima i uslovima iz Ugovora o obradi podataka ("UOP") iz softverskog rješenja Kaspersky Security for Microsoft Office 365. Kaspersky Lab će obavijestiti Korisnika o svakoj materijalnoj promjeni u UOP-u.
- 1.3. UOP je sastavni dio ovog Ugovora. Osim ako se Korisnik i Kaspersky Lab i/ili Partner pismeno dogovore drugačije, prihvata se i potvrđuje se da je Korisnik Kontroler a Kaspersky Lab je Obrađivač (u skladu sa GDPR-om i UOP-om) naročito po pitanju svih Ličnih podataka obuhvaćenih u Korisničkim podacima. Spisak podataka i svrhe obrade podataka nalaze se u UOP.
- 1.4. Korisnik će imati pristup Korisničkim podacima koji se čuvaju u Proizvodu na infrastrukturi i u sistemima Kaspersky Lab-a. Kaspersky Lab će čuvati Korisničke podatke na Korisničkom računu u ograničenom modu u periodu koji je utvrđen u Online podršci nakon isteka ili raskida Korisničke licence tako da Korisnik može izvaditi Korisničke podatke. Po završetku perioda čuvanja, Kaspersky Lab će izbrisati Korisničke podatke. Kaspersky Lab nije odgovoran za brisanje Korisničkih podataka u skladu s ovom Klauzulom.
- 1.5. Samo Korisnik je odgovoran za upoznavanje sa Online podrškom, naročito sa UOP-om i Dijelom "Obrada podataka i uslovi privatnosti" ovog Ugovora. Samo Korisnik je odgovoran da samostalno odluči da li su prethodni dokumenti u skladu sa zahtjevima Korisnika.
- 1.6. Prilikom upotrebe Proizvoda Korisnik snosi potpunu odgovornost da obrada Ličnih podataka koji su obuhvaćeni u Korisničkim podacima bude zakoniti, naročito u okviru značenja Člana 6 (1) (a) do (f) GDPR-a (ako je računar ili mobilni uređaj u EU) ili važećih zakona o povjerljivim informacijama, ličnim podacima, zaštiti podataka i slično.
- 1.7. Korisnik će imati odgovornost prema Kaspersky Lab-u za bilo koju štetu zbog kršenja ovog Ugovora, posebno u vezi sa Dijelom "Obrada podataka i uslovi privatnosti" ili UOP-om.
- 1.8. Korisnik će obešteti Kaspersky Lab u vezi sa trećim stranama u slučaju bilo kojeg zahtjeva usljed propusta Korisnika u izvršenju obaveza iz Dijela "Obrada podataka i uslovi privatnosti" ovog Ugovora koji treće strane, naročito organi za zaštitu privatnosti, potvrde protiv Kaspersky Lab-a.

2. Obrada podataka za Proizvod

- 2.1. **Svrha obrade podataka.** Tokom upotrebe Proizvoda obrada podataka je potrebna za zaštitu Korisnika od poznatih prijetnji po sigurnost informacija, u skladu sa Online podrškom, i za osiguranje neprekinute izvedbe Proizvoda. Ta informacija može se smatrati ličnom po važećim zakonima određenih zemalja. Kontrolor je Kaspersky Lab po pitanju podataka iz Pod-dijela 2 "Obrada podataka za Proizvod".

Obrađeni podaci

Kaspersky Lab će redovno obrađivati slijedeće podatke u svrhu zaštite Korisnika od poznatih prijetnji po sigurnost informacija:

- IP adresa pošiljaoca skenirane poruke,
- provjere (MD5, SHA2-256, SHA1) skeniranog objekta,
- URL adresa za koju je zahtijevana reputacija,
- nazivi najviših domena u web adresama u skeniranim porukama,
- provjera (MD5) naziva fajlova u prilogu poruke,
- broj IP adresa (v4 i v6) u zaglavlju poruke i oznaka adrese koja pripada lokalnoj ili eksternoj mreži,
- nepovratna hash funkcija naziva domena u zaglavlju skenirane poruke,
- rezultat skeniranja poruke i ocjena spama,
- provjera (MD5) e-mail adrese pošiljaoca skenirane poruke,
- URL adrese iz skeniranih poruka sa obrisanim lozinkama,
- provjera (MD5) grafičkih objekata u poruci,
- kratki tekstualni potpisi sastavljeni od teksta poruke (nepovratni tekstualni kratki prikazi koji se ne mogu koristiti za obnavljanje originalnog teksta, prenos samog teksta nije izvršen) koji se koriste za filterisanje poznatih spam mailinga i odluka o njima,
- IP adrese pošiljaoca poruke i posredni mail serveri, verzija mail klijenta pošiljaoca, ID poruke, informacija o popunjavanju polja poruke, provjera (CRC32) fragmenata poruke koji su definisani putem markup jezika, nazivi domena pošiljaoca koji su uzeti iz SMTP sesije i MIME-zaglavlja, provjera (CRC32) naziva pošiljaoca koji je uzet iz SMTP sesije i MIME-zaglavlja, provjera (CRC32) naziva i domena pošiljaoca koji je uzet iz SMTP sesije.

Kaspersky Lab će redovno obrađivati slijedeće podatke da se izvedba Proizvoda ne bi prekidala:

- veličina poruke,
- veličina i vrsta skeniranog objekta,
- predmet poruke,
- ID poruke,
- ID EWS objekta,
- naziv mailboksa i primarna SMTP adresa,
- naziv Exchange Online organizacije,
- vremenska oznaka poruke,
- pošiljalac poruke,
- primaoci poruke,
- rezultat skeniranja poruke,

- IP adresa i anonimna e-mail adresa administratora koji je modificovao postavke Proizvoda,
 - lista postavki koje su modificovane bez naznake o stvarnim vrijednostima parametra,
 - ID organizacije Kaspersky Security for Microsoft Office 365, datum podešavanja organizacije, IP adresa računara koji je korišten za podešavanje organizacije,
 - vrsta licence,
 - broj detekcija sa slijedećim statusima: čist / zaražen / spam / grupni mail / phishing / filterisanje priloga,
 - broj objekata u podršci Kaspersky Security for Microsoft Office 365 i karantinu Exchange Online,
 - ukupan broj mailboksova u organizaciji, broj mailboksova koje pokriva licenca, broj mailboksova koji su odabrani za zaštitu,
 - status zaštite (modul omogućen / modul onemogućen) za svaki aplikativni modul (anti-virus, anti-phishing, anti-spam, filterisanje priloga po formatu, maska fajla, fajlovi Microsoft Office-a koji sadrže macros), odabrana aktivnost na detektovanim objektima,
 - broj korisnika (objekti u aktivnom direktoriju) u organizaciji.
- 2.2. **Zaštita i obrada podataka.** Kaspersky Lab tretira podatke koje dobije od Korisnika u skladu s odredbama ovog Pod-dijela 2 "Obrada podataka za Proizvod" i Kaspersky Lab-ovom Politikom privatnosti koja je objavljena na stranici <https://www.kaspersky.com/Products-and-Services-Privacy-Policy>.
- 2.3. Tokom upotrebe Proizvoda Korisnik snosi potpunu odgovornost za zakonitost obrade ličnih podataka nosioca podataka, naročito u okviru značenja Člana 6 (1) (a) do (f) GDPR-a (ako je nosilac podataka u Evropskoj Uniji) ili važećih zakona o povjerljivim informacijama, ličnim podacima, zaštiti podataka i slično.
- 2.4. U slučaju da Korisnik želi da se zakonitost obrade zasniva na saglasnosti nosilaca podataka, Korisnik mora obezbijediti da ta saglasnost, koja ispunjava sve zahtjeve važećih zakona, posebno ako je nosilac podataka u Evropskoj Uniji i primjenjuje se Član 6 (1) (a) GDPR-a, bude data od strane svakog nosioca podataka prije upotrebe Proizvoda. Korisnik garantuje da je saglasnost svakog Korisnikovog nosioca podataka dobijena prije obrade Ličnih podataka.
- 2.5. Kaspersky Lab i Korisnik su se dogovorili da je, u slučaju stavke 2.4 ovog Pod-dijela, Korisnik odgovoran da dokaže da postoji saglasnost s obradom ličnih podataka, naročito po Članu 7 (1) GDPR-a u kojem je nosilac podataka u EU. Korisnik garantuje da može i da će dokazati da postoji saglasnost svakog nosioca podataka uvijek na osnovu zahtjeva Kaspersky Lab-a u roku od 5 radnih dana počev od zahtjeva Kaspersky Lab-a.
- 2.6. Nadalje, u slučaju stavke 2.4 ovog Pod-dijela, Korisnik je obavezan i snosi potpunu odgovornost za davanje svakom pojedinačnom nosiocu podataka svih informacija koje su zakonski potrebne za dobijanje saglasnosti, naročito po Članu 13 GDPR-a (ako je nosilac podataka u Evropskoj Uniji), prije obrade Ličnih podataka. Korisnik je posebno obavezan da svakom nosiocu podataka u Evropskoj Uniji, ili gdje zahtijeva važeći zakon, dostavi Kaspersky Lab-ovu Politiku privatnosti (<https://www.kaspersky.com/Products-and-Services-Privacy-Policy>) prije obrade Ličnih podataka.

- 2.7. Korisnik će biti u potpunosti odgovoran Kaspersky Lab-u za bilo koju štetu zbog prekršaja ovog Ugovora, naročito Korisnikovog propusta da dobije saglasnost nosioca podataka, gdje je izvodivo, i/ili zbog nedobijanja dovoljne saglasnosti i/ili zbog nedostatka dokaza i/ili zakašnjelog dokaza o saglasnosti nosioca podataka i/ili zbog bilo kojeg drugog prekršaja neke obaveze iz ovog Ugovora.
- 2.8. Korisnik će nadoknaditi Kaspersky Lab-u u vezi sa trećim stranama odštete zbog Korisnikovog propusta u izvršenju obaveza iz Pod-dijela 2 "Obrada podataka za Proizvod" koji treće strane, posebno nadzorni organi za zaštitu podataka, imaju protiv Kaspersky Lab-a.

Ugovor Kaspersky Endpoint Security Cloud verzija 1.0

Ova verzija Ugovora je na snazi od 25.05.2018. godine.

Najnovija verzija ovog Ugovora nalazi se na stranici <https://cloud.kaspersky.com/Home/LegalDocuments>.

KASPERSKY LAB – POLITIKA ZAŠTITE PRIVATNOSTI ZA PROIZVODE I USLUGE

Uvod

AO Kaspersky Lab, koji se nalazi na adresi Bldg. 3, 39A, Leningradskoe Shosse, Moskva, 125212, Ruska Federacija, i sve firme unutar grupe "Kaspersky Lab" poštuju vašu privatnost. Ova Politika privatnosti za proizvode i usluge ("Politika privatnosti") opisuje kako koristimo informacije koje dostavljate kada koristite naše proizvode i usluge, i odluke koje možete donijeti o našoj upotrebi informacija. Opisujemo i mjere koje preduzimamo u svrhu zaštite informacija i način na koji nas možete kontaktirati u vezi sa vašom privatnosti.

Vežano za određene proizvode ili usluge koje Kaspersky Lab nudi, dobili ste ugovore, uslove upotrebe i izjave koje su dodatak ove politike po pitanju opsluživanja podataka.

Ova politika se može promijeniti zbog promjena u zakonima, zahtjeva organa vlasti ili promjena u našim aktivnostima obrade ličnih podataka. Revidovana politika biće na snazi odmah nakon što se postavi na našoj web stranici www.kaspersky.com/Products-and-Services-Privacy-Policy.

Ova verzija politike je na snazi od 01.02.2018. godine.

Izvori informacija

Kaspersky Lab može dobiti informacije o vama iz različitih izvora kao što su:

- **proizvodi i usluge,**
- **nakon što se prijavite za proizvode ili usluge Kaspersky Lab-a,**
- **kao odgovor na tehničku podršku ili drugu komunikaciju radi obezbijedenja potrebne realizacije proizvoda i usluga,**
- **na našim web stranicama,**

- kao odgovor na tržišno ili drugo komuniciranje,
- putem učešća u nekoj ponudi, programu ili promociji.

Također možete dati saglasnost za otkrivanje informacije o vama od strane trećih strana koje su je dobile.

Informacije koje su dostavili Korisnici i kako ih koristimo

Kaspersky Lab uvijek vrši obradu ličnih podataka na zakonski i pošten način.

Uvijek ćete znati kakve informacije dajete Kaspersky Lab-u prije nego što počnete da koristite proizvode i usluge ili potvrdite svoju saglasnost.

Podaci koje dostavljate zavise od usluga, proizvoda i karakteristika koje koristite. Za više informacija o podacima koje dostavljate molimo da pogledate licencni ugovor sa krajnjim korisnikom, izjavu o mrežnoj sigurnosti i ostalu dokumentaciju o proizvodima i uslugama koje koristite a naročito kako slijedi:

ZA PRIVATNE KORISNIKE (B2C):

- **DIO B EULA-e, KOJI NAVODI PODATKE KOJE TREBA OBRADITI RADI IZVRŠENJA SVIH UGOVORNIH OBAVEZA;**
- **IZJAVA O MREŽNOJ SIGURNOSTI, KOJA NAVODI PODATKE ZA POVEĆANJE EFIKASNOSTI VAŠE ZAŠTITE;**
- **TRŽIŠNA IZJAVA, KOJA NAVODI PODATKE ZA UNAPREĐENJE APLIKATIVNE PERFORMANSE KOJI NAM POMAŽU DA ANALIZIRAMO NIVO ZADOVOLJSTVA KORISNIKA;**
- **IZJAVE O KARAKTERISTIKAMA, KOJE OPISUJU OBRADU PODATAKA O NEKIM KARAKTERISTIKAMA PROIZVODA, NPR. ANTI-SPAM. MOŽETE SE UPOZNATI SA OVIM IZJAVAMA KADA ODLUČITE DA AKTIVIRATE KARAKTERISTIKE U PROIZVODU.**

ZA POSLOVNE KORISNIKE (B2B):

- **IZJAVA O MREŽNOJ SIGURNOSTI, KOJA NAVODI PODATKE POTREBNE ZA POVEĆANJE EFIKASNOSTI VAŠE ZAŠTITE. ZA NEKE PROIZVODE, IT ADMINISTRATOR ILI NEKI DRUGI UPOSLENIK KOJI JE ZADUŽEN ZA PODEŠAVANJE PROIZVODA IMAĆE MOGUĆNOST DA ODABERE OBIM PODATAKA KOJI ĆE SE OBRADIVATI.**

Podaci za obradu zavise od proizvoda ili usluge i preporučuje se da korisnici pažljivo pročitaju ugovore i izjave koje su prihvaćene tokom instalacije ili upotrebe softvera ili usluge.

Neki podaci nisu lični u skladu sa zakonima određenih zemalja. Bez obzira na vrstu podataka i teritoriju na kojoj su podaci primljeni ili obrađeni, koristimo najviše standarde zaštite podataka i primjenjujemo različite zakonske, organizacione i tehničke mjere da bi zaštitili korisničke podatke, garantovali sigurnost i povjerljivost, kao i obezbijedili prava korisnika koja su garantovana važećim zakonom.

Podaci zavise od proizvoda i usluga koje koristite i mogu obuhvatiti slijedeće:

- **Informacija o licenci/pretplati**

Obrađuje se u svrhu prepoznavanja zakonskih korisnika. Ovaj podatak je potreban za očuvanje komunikacije između proizvoda i usluga Kaspersky Lab-a – slanje i prijem baza podataka proizvoda, ažuriranja, itd.

- **Informacija o proizvodu**

Podatak o funkcionisanju proizvoda i njegova interakcija sa korisnikom je također predmet analize. Na primjer, koliko dugo traje skeniranje prijetnje? Koje karakteristike se koriste češće od ostalih? Odgovori na ova i ostala pitanja pomažu tehnolozima da unaprijede proizvode i učine ih bržim i lakšim za upotrebu.

- **Podatak o uređaju**

Podaci kao što su vrsta uređaja, operativni sistem, itd., mogu zatrebati da korisnik ne bi morao kupiti novu licencu za sigurnosni proizvod nakon reinstalacije operativnog sistema. Ova informacija nam pomaže i da analiziramo sajber prijetnje jer pokazuje koliko uređaja je pod određenom prijetnjom.

- **Otkrivene prijetnje**

Ako se pronađe prijetnja (nova ili poznata) na nekom uređaju, informacija o tome šalje se Kaspersky Lab-u. To nam omogućava da analiziramo prijetnje, njihove izvore, principe infekcije, itd., što dovodi do većeg kvaliteta zaštite svakog korisnika.

- **Informacija o instaliranim aplikacijama**

Ova informacija pomaže da napravimo liste 'bijelih' ili neškodljivih aplikacija i sprječava da sigurnosni proizvodi pogrešno identifikuju te aplikacije kao zlonamjerne. Ovaj podatak se koristi i za ažuriranje i proširenje programskih kategorija za karakteristike kao što su 'roditeljska kontrola' i 'kontrola početka aplikacije'. Pored toga, ova informacija omogućava nam da korisnicima ponudimo rješenja sigurnosti koja najbolje odgovaraju njihovim potrebama.

- **Posjećeni URL-ovi**

URL-ovi se mogu poslati na provjeru da li su zlonamjerni. Ova informacija pomaže da napravimo liste 'bijelih' ili neškodljivih aplikacija i sprječava da sigurnosni proizvodi pogrešno identifikuju te aplikacije kao zlonamjerne. Ovaj podatak se koristi i za ažuriranje i proširenje kategorija web stranice za rješenja kao što je 'Kaspersky sigurna djeca' i omogućava bolju zaštitu finansijskih transakcija u proizvodima kao što je 'Kaspersky sprječavanje prevare'. Pored toga, ova informacija omogućava nam da korisnicima ponudimo rješenja sigurnosti koja najbolje odgovaraju njihovim potrebama. Vršimo filterisanje informacija o prijavama i lozinkama iz prenesenih URL-ova, čak i ako se čuvaju u početnom korisničkom zahtjevu za pretraživanje.

- **Događaji u operativnom sistemu**

Novi malver često može biti identifikovan samo ako se sumnjivo ponaša. Zbog toga proizvod analizira podatke o procesima koji teku na uređaju. To omogućava ranu identifikaciju procesa koji ukazuju na zlonamjernu aktivnost i sprječavanje svih štetnih posljedica kao što je uništenje korisničkih podataka.

- **Sumnjivi dokumenti i dokumenti koje bi mogli uljezi koristiti**

Ako neki (još) nepoznati dokument ukazuje na sumnjivo ponašanje na uređaju, može se automatski poslati na detaljniju analizu od strane mašinskih tehnologija na bazi učenja i, u rijetkim slučajevima, analitičara malvera. Lični dokumenti (fotografije ili dokumenti) rijetko su zlonamjerni i ne ponašaju se sumnjivo. Kao rezultat, kategorija 'sumnjivo' obuhvata uglavnom izvršne fajlove (.exe). Radi ispitivanja incidenata u vezi sa sigurnosti informacija, mogu se poslati izvršni i neizvršni 'bijeli fajlovi' ili njihovi dijelovi.

- **Podaci o Wi-Fi priključku**

Ova informacija se analizira da bi se korisnici upozorili na nesigurne (tj. loše zaštićene) tačke Wi-Fi pristupa, što pomaže pri sprječavanju nehotičnog presretanja ličnih podataka.

- **Podatak za stupanje u kontakt s korisnikom**

E-mail adrese se koriste za autorizaciju na web portalima Kaspersky Lab-a (My Kaspersky, Company Account, Kaspersky Endpoint Security Cloud, itd.), koji korisnicima omogućavaju da daljinski upravljaju svojom zaštitom. E-mail adrese se koriste za slanje sigurnosnih poruka (npr. sa važnim upozorenjima) korisnicima proizvođača Kaspersky Lab-a. Korisnici mogu također definisati imena (ili nadimke) kojim žele da im se obraća na portalu My Kaspersky i u e-mailovima. Korisnici po svom nahođenju daju informacije za stupanje u kontakt s njima.

- **Odbačeni i praćeni dokumenti**

Označavanjem posebne kockice u postavkama proizvođača korisnici mogu podijeliti i izvještaje o greškama na serverima Kaspersky Lab-a. Ova informacija pomaže (1) tokom analize grešaka na proizvodu i njihovu modifikaciju tako da funkcionišu brže se krećući naprijed, i (2) prilikom sprječavanja i ispitivanja incidenata po pitanju sigurnosti informacija.

- **Sadržaj vaših e-mailova**

Za vrijeme vaše upotrebe funkcionalnosti za zaštitu od spama možemo dobiti i analizirati informacije o e-mailovima, uključujući sadržaj i pošiljaoca da bi vas zaštitili od spama i prevare. Ova funkcionalnost je namijenjena za zaštitu korisnika od svih neželjenih e-mailova ili spama. Funkcionalnost za zaštitu od spama analizira informacije iz e-mailova koje prijavite kao spam ili koje su netačno identifikovane kao spam od strane softvera.

- **Podatak o ukradenom uređaju**

Karakteristika za zaštitu od krađe daje određeni daljinski pristup i kontrolu radi zaštite podataka na vašem mobitelu u slučaju krađe i omogućava vam da dobijate informacije o mjestu na kojem je uređaj ukraden. Karakteristika za zaštitu od krađe mora čuvati podatke o vašem telefonu i odobrenim korisnicima da bi ove funkcije radile.

- **Podatak za zaštitu djece**

Ukoliko roditelj ili nosilac roditeljske odgovornosti želi da koristi karakteristiku za zaštitu sigurnosti djeteta kao što je 'Kaspersky sigurna djeca', on ili ona može dobijati informacije o djetetovom uređaju i lokaciji. Pored toga, roditelj ili nosilac roditeljske odgovornosti može

konfigurirati parametre u svrhu blokiranja ili davanja dozvole za određene web stranice i/ili omogućavanja ili sprječavanja određenih aplikacija na dječjem uređaju. Kaspersky Lab ne skuplja dječje podatke izvan okvira te karakteristike.

KASPERSKY LAB ĆE OBRADIVATI SAMO LIČNE PODATKE U ODREĐENE UNAPRIJED DEFINISANE SVRHE U SKLADU SA VAŽEĆIM ZAKONOM, KOJI SU BITNI ZA POSLOVANJE KASPERSKY LAB-A.

- **Osiguranje izvršenja ugovora sa korisnicima i potrebne izvedbe proizvoda i usluga za klijente.**
- **Zaštita korisnika od poznatih prijetnji po sigurnost informacija.**
- **Provjera zakonitosti licence.**
- **Povećanje djelotvornosti zaštite vašeg računara, naročito davanje bržeg odgovora na nove prijetnje po sigurnost mreže i informacija, povećanje djelotvornosti zaštite softvera, smanjenje mogućnosti za lažnu pozitivnost.**
- **Unapređenje korisničke interakcije i iskustva sa našim proizvodima i uslugama, naročito promjena interfejsa i davanje željenog sadržaja i reklame, u vezi sa tržištem.**
- **Davanje tehničke podrške klijentima vezano za proizvode i usluge i poboljšanje kvaliteta proizvoda i usluga.**

Kaspersky Lab će čuvati lične podatke sve dok bude potrebno za ispunjavanje svrhe zbog koje su podaci obrađeni u skladu sa ciljevima koji su utvrđeni u ugovorima (KSN izjave, EULA, saglasnosti) ili za usklađivanje sa važećim zakonskim zahtjevima.

OGRANIČENA ILI ZABRANJENA OBRADA PODATAKA

UKOLIKO ODLUČITE DA NE DAJETE PODATAK KOJI JE POTREBAN ZA FUNKCIONISANJE NEKOG PROIZVODA ILI USLUGE, NEĆETE MOĆI KORISTITI Taj PROIZVOD ILI KARAKTERISTIKU. OVAJ OBAVEZNI PODATAK NAVEDEN JE U LICENCNOM UGOVORU SA KRAJNJIM KORISNIKOM. KASPERSKY-EVA IZJAVA O MREŽNOJ SIGURNOSTI ILI IZJAVA O MARKETINGU SADRŽI LISTU PODATAKA ZA KOJE KORISNICI MOGU ODLUČITI DA NAM DOSTAVE BILO KADA OZNAČAVANJEM ODGOVARAJUĆE KOČKICE U POSTAVKAMA PROIZVODA (MOGU TAKOĐER PROMIJENITI OVU ODLUKU KAD GOD ŽELE).

Šta nećemo obrađivati

Kaspersky Lab nikada u svojim proizvodima i uslugama ne obrađuje "osjetljive" podatke kao što su podaci o vjeri, političkim stavovima, seksualnoj orijentaciji ili zdravlju ili o ostalim specijalnim kategorijama ličnih podataka. Ne želimo da dobijamo takve podatke i nećemo ih tražiti od vas.

Proizvodi Kaspersky Lab-a moraju biti instalirani i korišteni od strane odraslih osoba. Djeca mogu koristiti uređaj na kojem je instaliran proizvod Kaspersky Lab-a samo uz dozvolu roditelja ili nosioca roditeljske odgovornosti. Osim "podataka za zaštitu djeteta", nemamo namjeru da obrađujemo lične podatke djece, niti želimo da dobijamo lične informacije djece.

Gdje obrađujemo informacije i kako ih dijelimo

Lični podaci koje korisnici dostave Kasperky Lab-u mogu biti obrađeni u slijedećim zemljama,

uključujući zemlje izvan Evropske Unije (EU) ili Evropske ekonomske oblasti (EEO):

U EU ili EEO:

- **Njemačka**
- **Holandija**
- **Francuska**
- **Velika Britanija**
- **Švajcarska**

Izvan EU ili EEO:

- **Kanada**
- **Singapur**
- **Rusija**
- **Japan**
- **SAD**
- **Meksiko**
- **Kina**
- **Azerbejdžan**

U skladu sa našom poslovnom praksom, podaci koje dobijamo od korisnika iz EU obrađuju se na serverima koji se nalaze u EU i Rusiji.

Lični podaci mogu se obrađivati na destinacijama izvan EU ili EEO i neke od njih nemaju adekvatan nivo zaštite podataka kako je utvrdila Evropska Komisija. Može ih obrađivati i osoblje koje radi izvan EU ili EEO koje radi za nas ili za nekog od naših isporučilaca.

Prilikom svake obrade podataka koristimo najviše standarde zaštite podataka i primjenjujemo različite zakonske mjere zaštite korisničkih podataka, garantujemo sigurnost i povjerljivost i obezbjeđujemo prava korisnika. Da biste više saznali o odlukama Evropske Komisije o adekvatnosti zaštite ličnih podataka u zemljama u kojim Kaspersky Lab obrađuje podatke, molimo da odete na stranicu ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

Nikada ne dajemo državnim organizacijama ili trećim stranama podatke ili pristup podacima. Možemo otkriti samo slijedeće informacije:

- **Unutar grupe firmi Kaspersky Lab. Podaci se mogu dijeliti.**
- **Davaoci usluge. Možemo dijeliti vaše informacije i sa prodavcima koji daju usluge nama, uključujući firme koje daju usluge web analitike, obrade podataka, reklamiranja, distribucije e-mailova, obrade plaćanja, izvršenja narudžbi i ostale usluge.**

Napominjemo da neki od naših proizvoda, npr. Kaspersky siguran priključak, obuhvata linkove za proizvode trećih strana čije se aktivnosti zaštite privatnosti razlikuju od naših. Ako date lične podatke bilo kojem od tih proizvoda, njihove izjave o zaštiti privatnosti su mjerodavne za vaše podatke.

Vaša prava i opcije

Imate određena prava po pitanju vaših ličnih podataka. Nudimo vam i određene opcije o tome koje lične podatke nam dostavljate, kako koristimo te informacije i kako komuniciramo s vama.

U većini slučajeva možete odlučiti da nam ne dostavljate lične podatke kada koristite proizvode, usluge i web stranice Kaspersky Lab-a. Isto tako možete odbiti da informacije šalžete direktno nama. Međutim, ako ne pošaljete lične podatke kad se zatraži, nećete moći koristiti sve proizvode i usluge Kaspersky Lab-a i nećemo moći da vam šalžemo informacije o proizvodima, uslugama i promocijama.

Uvijek možete odlučiti da ne dobijate obavijesti o marketingu putem e-maila tako što ćete kliknuti na link za odjavu u e-mailovima o marketingu koje dobijete od nas.

Ukoliko vaš poslodavac pošalže vaše lične podatke Kaspersky Lab-u, imaćete određene opcije vezano za Kaspersky Lab-ovu upotrebu ili otkrivanje te informacije. Molimo da kontaktirate svog poslodavca da se informišete i iskoristite opcije koje imate.

Do zakonski dozvoljenog nivoa, možete uvijek povući bilo koju saglasnost koju ste nam dali, ili objekat na zakonskim osnovama, za obradu vaših ličnih podataka. Primijenićemo ono što vam više odgovara i ići dalje. U nekim okolnostima, povlačenje vaše saglasnosti sa Kaspersky Lab-ovom upotrebom ili otkrivanjem vaših ličnih podataka podrazumijevaće da ne možete iskoristiti određene proizvode ili usluge Kaspersky Lab-a.

U skladu sa važećim zakonom, možete imati pravo: da dobijete potvrdu da čuvamo vaše lične podatke, da tražite pristup i dobijate informacije o vašim ličnim podacima, da dobijate kopije vaših ličnih podataka, da ažurirate i ispravljate greške u vašim ličnim podacima, da se protivite obradi vaših ličnih podataka i da se informacije blokiraju, brišu ili budu anonimne, kako je prihvatljivo. Pravo na pristup ličnim podacima može biti ograničeno u nekim okolnostima po lokalnom zakonu. Da biste ostvarili ta prava, molimo da stupite u kontakt s nama u skladu sa dole navedenim uputstvom.

Ukoliko nam dostavite bilo koju informaciju ili materijal o drugom pojedincu, trebate obezbijediti da to dijeljenje s nama i naša dalja upotreba kako vam je opisano bude u skladu sa važećim zakonima; tako na primjer trebate propisno obavijestiti tog pojedinca o obradi njegovih/njenih ličnih podataka i dobiti saglasnost za to, što može biti potrebno po važećim zakonima.

Ako ne ispunimo vaša očekivanja u vezi sa obradom vaših ličnih podataka ili želite da uložite žalbu o našim aktivnostima zaštite privatnosti, molimo da nam se obratite jer nam to daje mogućnost da riješimo problem. Možete nas kontaktirati putem podataka koje smo dali u donjem dijelu "Kako stupiti u kontakt s nama". Da biste nam pomogli da odgovorimo na vaš zahtjev, molimo da nam dostavite sve detalje o problemu. Pokušavamo da pregledamo i odgovorimo na sve žalbe u razumno vrijeme.

Principi zaštite privatnosti

Obrada ličnih podataka u Kaspersky Lab-u zasniva se na slijedećim principima:

Saglasnost i mogućnost izbora

- **Davanje mogućnosti izbora korisnicima da odluče da li dozvoljavaju obradu njihovih ličnih podataka osim ako korisnici ne mogu slobodno zadržati saglasnost ili ako važeći zakon specifično dozvoljava obradu ličnih podataka bez saglasnosti fizičkog lica. Korisnik mora odlučiti po slobodnoj volji i na osnovu informacija;**
- **Informisanje korisnika, prije dobijanja saglasnosti, o njihovim pravima po principu pojedinačnog učešća i pristupa;**
- **Davanje korisnicima, prije dobijanja saglasnosti, informacija po principu otvorenosti, transparentnosti i obavještanja; i**
- **Davanje objašnjenja korisnicima o posljedicama davanja ili nedavanja saglasnosti.**

Zakovitost i definisanje svrhe

- **Obezbijeđenje da svrha bude u skladu sa važećim zakonom i da se zasniva na dozvoljenoj zakonskoj osnovi;**
- **Obavještanje korisnika o svrsi prije nego što se informacija upotrijebi po prvi put u novu svrhu;**
- **Korištenje jezika koji je i jasan i adekvatno prilagođen okolnostima.**

Ograničenje obrade podataka

- **Ograničenje prikupljanja ličnih podataka na one koji su u okviru važećeg zakona i strogo potrebni za određenu svrhu;**
- **Brisanje i raspolaganje ličnim podacima kada istekne svrha obrade ličnih podataka, kada nema zakonskih zahtjeva za čuvanje ličnih podataka ili kada je to izvodivo.**

Ograničenje upotrebe, čuvanja i otkrivanja

- **Ograničenje upotrebe, čuvanja i otkrivanja ličnih podataka na one koji su potrebni za ispunjavanje određene, eksplicitne i zakonske svrhe;**
- **Ograničenje upotrebe ličnih podataka na svrhe koje je definisao Kaspersky Lab prije prijema podataka, osim ako je drugačija svrha eksplicitno potrebna po važećem zakonu;**
- **Čuvanje ličnih podataka samo koliko je potrebno za ispunjavanje navedene svrhe, i nakon toga njihovo sigurno uništenje ili stavljanje u stanje anonimnosti; i**
- **Zaključavanje (tj. arhiviranje, osiguranje i izuzimanje ličnih podataka iz dalje obrade) svih ličnih podataka kada i sve dok ne istekne navedena svrha, ali uz čuvanje ako bude potrebno po važećim zakonima.**

Tačnost i kvalitet

- **Omogućavanje da obrađeni lični podaci budu tačni, potpuni, ažurirani (osim ako postoji zakonska osnova za čuvanje zastarjelih podataka), adekvatni i relevantni za svrhu upotrebe;**
- **Obezbijeđenje pouzdanosti ličnih podataka koji su dobijeni od izvora koji nisu korisnici prije nego što budu obrađeni;**

- **Provjera, odgovarajućim sredstvima, važnosti i ispravnosti zahtjeva korisnika prije bilo kojih promjena u ličnim podacima (da bi se osiguralo da promjene budu pravilno ovlaštene), gdje je prikladno;**
- **Uspostava procedura za obradu ličnih podataka u svrhu osiguranja tačnosti i kvaliteta;**
- **Uspostava mehanizama kontrole za periodičnu provjeru tačnosti i kvaliteta obrade ličnih podataka.**

Otvorenost, transparentnost i obavještanje

- **Davanje korisnicima jasnih i lako dostupnih informacija o politikama Kaspersky Lab-a;**
- **Uspostava procedura i aktivnosti za obradu ličnih podataka;**
- **Stavljanje u obavijesti činjenice da su lični podaci obrađeni, svrhe zbog koje je to urađeno, vrsta privatnih dioničara kojim lični podaci mogu biti otkriveni i identiteta cjeline koja definiše gore navedeno i način stupanja u kontakt;**
- **Otkrivanje opcija i sredstava koje nudi Kaspersky Lab korisnicima u svrhu ograničavanja obrade, i za pristup, ispravke i uklanjanja njihove informacije;**
- **Obavještanje korisnika kada dođe do velikih promjena u procedurama upotrebe ličnih podataka.**

Pojedinačno učešće i pristup

- **Davanje mogućnosti korisnicima da nas kontaktiraju (putem informacija iz dijela "Kako stupiti u kontakt s nama") i pregledaju svoje lične podatke, pod uslovom da je njihov identitet prvo autentifikovan uz odgovarajući nivo tačnosti i da taj pristup nije zabranjen važećim zakonom;**
- **Davanje mogućnosti korisnicima (putem informacija iz dijela "Kako stupiti u kontakt s nama" ili interfejsa naših proizvoda i usluga) da provjere tačnost i kompletnost ličnih podataka i da ih promijene, isprave ili uklone što je prikladnije moguće u određenom kontekstu;**
- **Dostava bilo kojeg amandmana, ispravke ili ukidanja obrađivačima ličnih podataka i trećim stranama kojim su lični podaci otkriveni, tamo gdje su poznati;**
- **Uspostava procedura koje omogućavaju korisnicima da ostvare ova prava na jednostavan, brz i djelotvoran način koji ne prouzrokuje nepropisno kašnjenje ili trošak.**

Sigurnost informacija: kako štitimo vašu privatnost

Sigurnost informacija je najvažnija aktivnost Kaspersky Lab-a. Svi podaci i sve informacije koje nam dostavite su po pravilu povjerljive. Kaspersky Lab će zato uvijek primjenjivati mjere tehničke i organizacione zaštite sigurnosti podataka radi zaštite ličnih podataka koji su odgovarajući i prikladni, uzimajući u obzir konkretne rizike obrade ličnih podataka kao i najnovije standarde i procedure zaštite sigurnosti. Da bi identifikovao i postigao odgovarajući nivo zaštite, Kaspersky Lab klasifikuje sisteme obrade sa ličnim podacima i primjenjuje kaskadne setove mjera zaštite.

Kaspersky Lab također provodi fizičke, elektronske i proceduralne mjere zaštite informacija od gubitka, zloupotrebe, oštećenja ili modifikacije i neovlaštenog pristupa ili otkrivanja. Neke od ostalih glavnih karakteristika našeg programa zaštite sigurnosti informacija su slijedeće:

- Odjel za zaštitu sigurnosti informacija koji dizajnira, primjenjuje i daje uvid u naš program zaštite sigurnosti informacija;
- Utvrđivanje rizika po sigurnost ličnih podataka tokom obrade u sistemu obrade Kaspersky Lab-a;
- Upotreba odgovarajućih alata za zaštitu sigurnosti informacija;
- Procjena izvedbe primijenjenih mjera zaštite sigurnosti ličnih podataka prije ispitivanja sistema obrade;
- Primjena kontrola radi identifikacije, autentifikacije i ovlaštenja pristupa različitim uslugama ili web stranicama;
- Utvrđivanje činjenica u vezi sa neovlaštenim pristupom ličnim podacima i usvajanje odgovarajućih mjera;
- Oporavak ličnih podataka koji su modifikovani ili uništeni;
- Uspostava pravila pristupa ličnim podacima koji su obrađeni u sistemima obrade Kaspersky Lab-a kao i snimanje i obračun svih aktivnosti koje su preduzete sa ličnim podacima u ovim sistemima;
- Šifrovanje između naših klijenata i servera (i između naših različitih centara podataka);
- Pristup ograničavamo na naše uposlenike i ugovarače koji trebaju znati informacije da bi ih za nas obradili i koji su podložni strogim obavezama ugovorne povjerljivosti u vezi sa ličnim informacijama. Mogu biti kažnjeni ili se njihov ugovor može raskinuti ukoliko ne izvrše ove obaveze;
- Praćenje naše systemske infrastrukture radi otkrivanja slabosti i mogućih upada;
- Praćenje mjera koje su preduzete u svrhu zaštite sigurnosti ličnih podataka;
- Odgovarajuća obuka osoblja Kaspersky Lab-a i stalno ažuriranje naših aktivnosti zaštite sigurnosti u svjetlu novih rizika i razvoja tehnologije.

Kako da stupite u kontakt s nama

Ukoliko imate neko pitanje ili komentar o ovoj Politici zaštite privatnosti, aktivnostima Kaspersky Lab-a po pitanju zaštite privatnosti ili ako želite da ažuriramo ili uklonimo informaciju ili prioritete koje ste nam dostavili, molimo da posjetite stranicu <https://www.kaspersky.com/global-privacy-policy>, kontaktirate nas elektronskim putem na stranici <https://support.kaspersky.com/privacy> ili da pošaljete dopis našem Odjelu za zaštitu privatnosti na adresu AO Kaspersky Lab, Bldg. 3, 39A, Leningradskoe Shosse, Moskva, 125212, Ruska Federacija.

UGOVOR O OBRADI PODATAKA U OKVIRU SOFTVERSKOG RJEŠENJA KASPERSKY SECURITY FOR MICROSOFT OFFICE 365

Ovaj Ugovor o obradi podataka ("UOP") čini sastavni dio Ugovora o davanju usluge online zaštite poslovnih korisnika ("Ugovor") i softverskog rješenja Kaspersky Security for Microsoft Office 365 ("Proizvod") između Kaspersky Lab-a i Korisnika. Priloženi aneksi i dodaci dopunjavaju uslove ovog UOP-a. Ukoliko su strane ranije sklopile neki ugovor o obradi podataka u vezi sa Proizvodom, ovaj UOP će sada zamijeniti prethodni.

Svi termini iz ovog UOP-a imaju isto značenje kao u Ugovoru. Ovdje korišteni termini koji se pozivaju na Propis EU o zaštiti podataka (2016/679), kao što su "prekršaj ličnih podataka", "obrada", "kontrolor", "procesor" i "nosilac podataka", imaju isto značenje kao u Članu 4 GDPR-a.

Ovaj UOP definiše rokove i uslove aktivnosti obrade Korisničkih podataka, naročito po pitanju obrade ličnih podataka ("Lični podaci") koji su obuhvaćeni u Korisničkim podacima, u vezi sa Ugovorom.

1. Djelokrug i uloge

- 1.1. Ovaj UOP primjenjuje se na obradu Korisničkih podataka od strane Kaspersky Lab-a u ime Korisnika.
- 1.2. Korisnik i Kaspersky Lab prihvataju da je Korisnik kontrolor ("Kontrolor") Korisničkih podataka a da je Kaspersky Lab obrađivač ("Obrađivač") tih podataka.
- 1.3. Ovaj UOP ne ograničava ili ne smanjuje Kaspersky Lab-ove obaveze zaštite podataka prema Korisniku u Ugovoru ili drugim dogovorima između Korisnika i Kaspersky Lab-a i/ili njegovih Partnera.
- 1.4. Korisnički podaci biće korišteni samo u svrhu davanja Proizvoda Korisniku, uključujući svrhe koje su potrebne i u skladu sa davanjem Proizvoda po Aneksu 1 ovog UOP-a. Korisnik zadržava sva prava, pravo vlasništva i interes na Korisničke podatke. Kaspersky Lab nema nikakva prava na Korisničke podatke osim onih koja su potrebna za davanje Proizvoda Korisniku.
- 1.5. UOP će ostati na snazi sve dok svi Korisnički podaci ne budu izbrisani ili povučeni iz sistema Kaspersky Lab-a po Ugovoru i Aneksu 1 ovog UOP-a.
- 1.6. Ovaj UOP se ne primjenjuje ako je Kasperky Lab kontrolor obrađenih podataka.
- 1.7. Prije upotrebe Proizvoda Korisnik mora odrediti lokaciju njegove organizacije koja će definisati gdje će Korisnički podaci biti obrađeni u skladu sa Online podrškom Kaspersky Lab-a ili njegovih podružnica ili pod-ugovarača. U skladu s ovom instrukcijom Korisnik imenuje Kaspersky Lab da izvrši prenos Korisničkih podataka na odabranu lokaciju i da pohrani i obradi Korisničke podatke radi davanja Proizvoda. Kaspersky Lab ne kontroliše ili ne ograničava oblasti iz kojih Korisnik ili njegovi krajnji korisnici mogu imati pristup ili prebaciti Korisničke podatke.
- 1.8. Prilikom davanja tehničke podrške Korisniku Kaspersky Lab će imati pristup Korisničkim podacima iz Rusije.
- 1.9. Aneks 2 ovog UOP-a čine standardne ugovorne klauzule (obrađivači) koje se zasnivaju na Odluci komisije od 05.02.2010. godine o standardnim ugovornim klauzulama o prenosu Ličnih podataka na obrađivače u trećim zemljama po Direktivi 95/46/EC. Standardne ugovorne klauzule primjenjuju se na prenos i obradu Ličnih podataka izvan EEO-a u trećoj zemlji koja ne daje odgovarajuću zaštitu ličnih podataka tokom davanja Proizvoda. Standardne ugovorne klauzule će prevladati nad bilo kojim spornim dijelom UOP-a i/ili Ugovora.

2. Obaveze Kaspersky Lab-a

- 2.1. Kaspersky Lab neće angažovati drugi procesor bez prethodne specifične ili opšte pismene saglasnosti Korisnika. U slučaju davanja opšte pismene saglasnosti, Kaspersky Lab će obavijestiti Korisnika o svim planiranim promjenama po pitanju dodavanja ili zamjene ostalih procesora, dajući tako priliku Korisniku da uloži prigovor na te promjene.
- 2.2. Predmet i trajanje obrade, priroda i svrha obrade, vrsta Korisničkih podataka, kategorije podatkovnih predmeta i prava i obaveze Korisnika utvrđeni su u Ugovoru i ovom UOP-u. Kaspersky Lab će naročito izvršiti sljedeće:
- **obradiće Korisničke podatke, uključujući u vezi sa prenosima Korisničkih podataka u neku treću zemlju ili međunarodnu organizaciju, samo po uputama Korisnika u okviru djelokruga i u svrhu Proizvoda po Ugovoru i ovom UOP-u. Ugovor i ovaj UOP, zajedno sa Korisnikovom upotrebom i konfiguracijom karakteristika Proizvoda, su Korisnikove kompletne upute Kaspersky Lab-u za obradu Korisničkih podataka;**
 - **osiguraće da se osobe ovlaštene za obradu Korisničkih podataka obavežu na povjerljivost ili imaju odgovarajuću zakonsku obavezu povjerljivosti;**
 - **preduzeće sve mjere u skladu sa Članom 32 GDPR-a;**
 - **pridržiće se uslova za angažovanje drugog procesora;**
 - **uzimajući u obzir prirodu obrade, pomoći će Korisniku putem adekvatnih tehničkih i organizacionih mjera, sve dok je moguće, pri izvršenju Korisnikove obaveze da odgovori na zahtjeve za ostvarivanje prava na nosilac podataka iz Dijela III GDPR-a;**
 - **pomoći će Korisniku da se pridržava obaveza u skladu sa Članovima 32 do 36 GDPR-a uzimajući u obzir prirodu obrade i informacije koje su raspoložive Kaspersky Lab-u;**
 - **po izboru Korisnika, izbrisaće ili vratiti Korisniku sve Korisničke podatke po završetku davanja Proizvoda i izbrisaće postojeće kopije;**
 - **staviće Korisniku na raspolaganje sve informacije koje su potrebne da se ukaže na usklađenost sa obavezama iz Člana 28 GDPR-a i omogućiće i učestvovaće u revizijama, kao i inspekcijama, koje vodi Korisnik ili drugi revizor po ovlaštenju Korisnika.**
- 2.3. Kaspersky Lab će obavijestiti Korisnika bez kašnjenja nakon što sazna za povredu ličnih podataka u zakonskoj formi. Obavijest će biti dostavljena jednom ili više Korisnikovih administratora putem bilo kojeg sredstva koje odabere Kaspersky Lab, uključujući putem e-maila. Samo Korisnik je odgovoran da obezbijedi da njegovi administratori čuvaju tačne kontakt informacije. Obaveza da prijavi ili reaguje na povredu ličnih podataka nije potvrda Kaspersky Lab-a bilo kojeg propusta ili odgovornosti u vezi sa tom povredom ličnih podataka.
- 2.4. Kaspersky Lab će primijeniti i održavati odgovarajuće tehničke i organizacione mjere zaštite Korisničkih podataka u skladu sa Aneksom 1 Pod-odjeljak 2 ovog UOP-a od slučajnog, neovlaštenog ili nezakonitog pristupa, otkrivanja, zamjene, gubitka ili uništenja. Tehničke i organizacione mjere su podložne tehničkom razvoju. Kaspersky Lab može primijeniti odgovarajuće alternativne mjere koje omogućavaju bar isti nivo zaštite sigurnosti kao definisane mjere.

- 2.5. Korisnik i Kaspersky Lab će preduzeti korake da obezbijede da bilo koje lice koje djeluje po ovlaštenju Korisnika ili Kaspersky Lab-a a koje ima pristup Korisničkim podacima ne vrši njihovu obradu osim na osnovu uputstava Korisnika.

3. Obaveze Korisnika

- 3.1. Korisnik će biti odgovoran za primjenu važećih zakona i propisa o zaštiti podataka uključujući ali bez ograničenja kompletan prenos Korisničkih podataka Kaspersky Lab-u.
- 3.2. Korisnik može pismeno obavijestiti Kaspersky Lab u roku od trideset (30) dana od isteka ili raskida Korisničke licence povući Korisničke podatke putem razumnih mjera ili izbrisati pohranjene Korisničke podatke. Korisnik će obavijestiti Kaspersky Lab bez nepropisnog kašnjenja ako ne bude mogao povući Korisničke podatke u ovom periodu. Po isteku tog perioda bez obavijesti od strane Korisnika, Kaspersky Lab će izbrisati sve pohranjene Korisničke podatke, osim ako mu bude po zakonu zabranjeno da to uradi.

4. Revizija od strane Korisnika

- 4.1. Korisnik će imati dozvolu za reviziju aktivnosti Kaspersky Lab-a koje se odnose na izvršenje njegovih obaveza iz ovog UOP-a po važećim zakonima o zaštiti podataka. U tu svrhu Kaspersky Lab će razumno podržavati Korisnika i davati mu potrebne informacije na osnovu njegovog pismenog zahtjeva.
- 4.2. Nakon obavještanja Kaspersky Lab-a bar pet sedmica unaprijed, Korisnik može izvršiti reviziju putem terenske inspekcije uređaja i aktivnosti vezano za Kaspersky Lab-ovu obradu podataka u redovno radno vrijeme i bez ozbiljnog prekida dnevnih aktivnosti Kaspersky Lab-a. Za vođenje revizije u njegovo ime Korisnik može odabrati neku dovoljno kvalifikovanu samostalnu treću stranu kao revizora koji ima obavezu povjerljivosti i nije konkurent Kaspersky Lab-u.
- 4.3. Korisnik će dokumentovati proces revizije i poslati Kaspersky Lab-u izvještaj o svim utvrđenim prekršajima Kaspersky Lab-ovih obaveza iz ovog UOP-a, ako je primjenljivo. Korisnik i Kaspersky Lab će se dogovoriti o razumnim mjerama radi obezbijedenja usaglašenosti u budućnosti.
- 4.4. Korisnik će snositi sve troškove vođenja revizija i nadoknadiće Kaspersky Lab-u sve lične resurse koji su potrošeni na podršku revizije po tadašnjim važećim cijenama profesionalnih usluga Kaspersky Lab-a.

5. Pod-obrada podataka

- 5.1. Korisnik daje ovlaštenje Kaspersky Lab-u da angažuje pod-obrađivače za obradu Korisničkih podataka po ovom UOP-u. Spisak trenutnih pod-obrađivača nalazi se na URL-u <https://help.kaspersky.com/Cloud/1.0/en-US/172033.htm>. Kaspersky Lab će obavijestiti Korisnika bar četrnaest (14) dana prije davanja ovlaštenja za bilo kojeg novog pod-obrađivača za pristup Korisničkim podacima.
- 5.2. Kaspersky Lab će obezbijediti da pod-obrađivači budu obavezni u skladu sa pismenim dogovorima koji od njih zahtijevaju da pruže bar isti nivo zaštite podataka koji se traži od Kaspersky Lab-a putem ovog UOP-a.

6. Odvojivost odredbi

- 6.1. Trajanje ovog UOP-a prati trajanje Ugovora. Ukoliko pojedinačne odredbe ovog UOP-a budu nevažeće ili nesprovodive, to neće uticati na važnost i sprovodivost ostalih odredbi ovog UOP-a.

ANEKS 1. DODATNI USLOVI OBRADE PODATAKA I ZAŠTITE SIGURNOSTI

1. Dodatni uslovi obrade podataka

- 1.1. **Trajanje obrade podataka.** Obrada podataka će trajati dok traje Licenca. Po isteku ili raskidu Korisnikove licence Kaspersky Lab će izbrisati ili vratiti Korisničke podatke po rokovima iz Ugovora.
- 1.2. **Razlog za obradu podataka.** Razlog za obradu podataka je davanje Proizvoda Korisniku, davanje tehničke podrške Korisniku, izvršenje ostalih obaveza iz Ugovora.
- 1.3. **Kategorija predmeta podataka.** Kategorije predmeta podataka su Korisnikovi predstavnici i krajnji korisnici, kao što su uposlenici, ugovarači, saradnici i klijenti.
- 1.4. **Djelokrug i svrha obrade ličnih podataka.** Korisnik koristi Proizvod radi zaštite Exchange Online mailboksova pod kontrolom Korisnika. U tu svrhu Obrađivač može dobijati, čuvati i obrađivati slijedeće vrste podataka:
- 1) identifikacioni podaci Globalnog administratora Office-a 365 koji su potrebni za davanje ovlaštenja za kreiranje servisnog računa sa potrebnim dozvolama u Exchange Online-u. Proizvod ne zavisi od računa Globalnog administratora nakon kreiranja servisnog računa i ne čuva svoje identifikacione podatke za buduću upotrebu.
 - 2) identifikacioni podaci servisnog računa koji se koriste za povezivanje Proizvoda sa Office-om 365,
 - 3) lista svih mailboksova zaštićene organizacije Exchange Online-a,
 - 4) lista svih prihvaćenih domena u zaštićenoj organizaciji Exchange Online-a,
 - 5) e-mail poruke i sastanci, prilozi i X-zaglavlja poruke. Proizvod prima ove stavke u svrhu njihovog skeniranja i obrađuje ih u skladu sa postavkama zaštite. E-mail poruke i stavke se ne čuvaju na infrastrukturi Kaspersky Security for Microsoft Office 365,
 - 6) meta podaci e-mail poruka (pošiljalac, primalac, predmet, primarna SMTP adresa srodnog mailboksa),
 - 7) e-mail adresa koja je definisana za vrijeme prijave i odgovarajuća IP adresa,
 - 8) postavke Proizvoda koje su raspoložive na Portalu,
 - 9) e-mail adrese koje su isključene iz skeniranja,
 - 10) e-mail adrese koje su definisane u postavkama obavještanja,
 - 11) statistika o Proizvodu (pošiljaoci, primaoci, predmeti i rezultati skeniranja e-mail poruka),
 - 12) nazivi grupe Aktivni direktorij, ID grupe i informacije o članstvu u grupi.

- 1.5. **Tehnička podrška.** Kaspersky Lab će imati pristup i obrađivati Korisničke podatke radi davanja usluge tehničke podrške. Korisnički podaci biće korišteni samo u svrhu davanja podrške, uključujući svrhe koje su potrebne i usklađene sa davanjem podrške, kao što su rješavanje ponavljajućih problema i unapređenje podrške i/ili Proizvoda.

Usluga tehničke podrške i njena pravila mogu se naći na stranici <https://support.kaspersky.com>.

2. Zaštita sigurnosti

- 2.1. Kaspersky Lab primjenjuje i pridržava se slijedećih mjera zaštite sigurnosti Proizvoda, za koje je samo Kaspersky Lab odgovoran po pitanju zaštite sigurnosti Korisničkih podataka:

Organizacija zaštite sigurnosti informacija

1. Imenuje se jedan ili više službenika za zaštitu sigurnosti koji su zaduženi za koordinaciju i praćenje pravila i procedura zaštite sigurnosti.
2. Osoblje koje ima pristup Korisničkim podacima podložno je obavezama povjerljivosti.
3. Vršiti se procjena rizika prije obrade Korisničkih podataka ili puštanja usluga u rad.

Upravljanje imovinom

4. Čuva se inventar kompletne imovine (na kojoj se pohranjuju Korisnički podaci). Pristup inventarima tih medija ograničen je na osoblje koje je ovlašteno da ima taj pristup.
5. Korisnički podaci se klasifikuju da bi se podržala njihova identifikacija i omogućilo da pristup podacima bude adekvatno ograničen.
6. Potrebno je posebno ovlaštenje prije pohranjivanja Korisničkih podataka na prenosivim uređajima, daljinskog pristupa Korisničkim podacima ili obrade Korisničkih podataka izvan firme.

Zaštita sigurnosti kadrovskih potencijala

7. Kaspersky Lab obavještava svoje osoblje o odgovarajućim procedurama zaštite sigurnosti i njihovim ulogama.
8. Kaspersky Lab obavještava svoje osoblje i o mogućim posljedicama kršenja procedura i pravila zaštite sigurnosti.
9. Kaspersky Lab vrši obuku iz zaštite sigurnosti ličnih podataka.

Fizička i sigurnost sredine

10. Kaspersky Lab ograničava pristup objektima u kojim su smješteni informacioni sistemi koji obrađuju Korisničke podatke na identifikovane ovlaštene pojedince:

- **zaštitarci pružaju uslugu zaštite sigurnosti 24 sata dnevno 7 dana u sedmici**
- **sistem elektronskog pristupa putem kartica kontroliše pristup perimetru**
- **barijera se koristi na svim ulaznim tačkama predviđenim za upotrebu kartica**
- **uposlenici moraju nositi Kaspersky Lab-ov bedž**

- posjetioci se registruju i moraju nositi bedževe za posjetioce; posjetioci imaju prатnju tokom posjete
- kompletan pristup perimetru i zaštićene zone nadziru se putem CCTV-a kojeg nadziru zaštitari

11. Kaspersky Lab čuva zapise dolaznih i odlaznih medija, uključujući vrstu medija, ovlaštenog pošiljaoca/primaoca, datum i vrijeme, broj medija.
12. Koriste se različiti industrijski standardni sistemi zaštite od gubitka podataka zbog nestanka napajanja ili linijskog miješanja.
13. Primjenjuju se industrijski standardni procesi za brisanje Korisničkih podataka nakon što nisu više potrebni.

Upravljanje komunikacijama i operacijama

14. Kaspersky Lab čuva dokumente o zaštiti sigurnosti koji opisuju njegove mjere zaštite sigurnosti i odgovarajuće procedure i odgovornosti njegovog osoblja koje ima pristup Korisničkim podacima.
15. Kopije Korisničkih podataka i procedura za oporavak podataka čuvaju se na drugom mjestu u odnosu na ono na kojem je smještena primarna računarska oprema za obradu Korisničkih podataka.
16. Primjenjuje se anti-malver kontrola radi sprječavanja da zlonamjerni softver dobije neovlašteni pristup Korisničkim podacima, uključujući zlonamjerni softver sa javnih mreža.
17. Korisnički podaci koji se prenose preko javnih mreža su šifrovani.
18. Kaspersky Lab evidentira pristup i upotrebu informacionih sistema koji sadrže Korisničke podatke i registruje pristupni ID, vrijeme, dato ili odbijeno ovlaštenje i odgovarajuću aktivnost.

Kontrola pristupa

19. Kaspersky Lab čuva i ažurira evidenciju o osoblju koje je ovlašteno da pristupa sistemima koji sadrže Korisničke podatke.
20. Kaspersky Lab identifikuje osoblje koje može dati, promijeniti ili otkazati ovlašteni pristup podacima i resursima.
21. Kaspersky Lab obezbijeduje da tamo gdje više pojedinaca ima pristup sistemima koji sadrže Korisničke podatke, ti pojedinci imaju zasebne identifikatore/prijave.
22. Tehničko osoblje ima dozvolu za pristup Korisničkim podacima samo po potrebi.
23. Kaspersky Lab ograničava pristup Korisničkim podacima samo za pojedince koji trebaju taj pristup za izvršenje svojih poslovnih obaveza.
24. Kaspersky Lab primjenjuje kontrolu pristupa na osnovu uloge.
25. Osoblje je dobilo upute da onemogućiti administrativne sesije prilikom napuštanja kontrole prostorija ili kada su računari ostavljeni bez nadzora.
26. Lozinke se čuvaju tako da budu nerazumljive dok su u upotrebi.
27. Kaspersky Lab koristi industrijske standardne prakse za identifikaciju i autentifikaciju korisnika koji pokušavaju da pristupe informacionim sistemima.
28. Kaspersky Lab je uspostavio politiku lozinke koja zabranjuje dijeljenje lozinke, daje uputstvo u slučaju otkrivanja lozinke, traži redovnu promjenu lozinke i zamjenu pogrešne lozinke.
29. Kaspersky Lab-ova politika lozinke definiše zahtjeve za kompleksnost lozinke.
30. Sve lozinke se čuvaju putem jednosmjernog hashing algoritma i uvijek se šalju šifrovane.

31. Kaspersky Lab ima kontrole za sprječavanje pojedinaca da preuzmu prava pristupa koja nisu dobili za pristup Korisničkim podacima kojim nisu ovlašteni da pristupaju.
32. Kaspersky Lab-ov interni mrežni kanal zaštićen je putem firewalls-a.
33. Svi prenosi podataka između Kaspersky Lab-a, pravnih lica i partnera i klijenata zaštićeni su putem TLS/SSL protokola.

Upravljanje incidentima po pitanju zaštite sigurnosti informacija

34. Kaspersky Lab ima evidenciju o prekršajima sigurnosti koja obuhvata opis prekršaja, vrijeme, posljedice prekršaja, ime izvjestioca i lica kojem je prekršaj prijavljen i proceduru obnove podataka.

Upravljanje ranjivosti

35. Informacioni resursi Kaspersky Lab-a redovno se provjeravaju putem skenera za provjeru njegove ranjivosti. Kaspersky Lab vrši testiranje penetracije informacionih resursa i revizije zaštite sigurnosti.

ANEKS 2

STANDARDNE UGOVORNE ODREDBE (OBRAĐIVAČI)

U svrhu Člana 26 (2) Direktive 95/46/EC za prenos ličnih podataka obrađivačima u trećim zemljama koji ne omogućavaju odgovarajući nivo zaštite podataka

Korisnik, koji je naveden u Ugovoru o obradi podataka ("izvoznik podataka") i AO Kaspersky Lab, Bldg. 3, 39A, Leningradskoe Shosse, Moskva, 125212, Ruska Federacija ("uvoznik podataka")

pojedinačno kao "strana", zajedno kao "strane",

PRIHVATILI SU slijedeće Ugovorne odredbe ("Odredbe") da bi predočili odgovarajuće mjere zaštite privatnosti i osnovnih ljudskih prava i sloboda za prenos ličnih podataka iz Dodatka 1 od strane izvoznika podataka uvozniku podataka.

Odredba 1

Definicije

U svrhu Odredbi:

- (a) 'lični podaci', 'specijalne kategorije podataka', 'obrada', 'kontrolor', 'obrađivač', 'nosilac podataka' i 'nadzorni organ' imaće isto značenje kao u Direktivi 95/46/EC Evropskog Parlamenta i Vijeća od 24.10.1995. godine o zaštiti pojedinaca po pitanju obrade ličnih podataka i o slobodnom kretanju podataka;
- (b) 'izvoznik podataka' je kontrolor koji prenosi lične podatke;
- (c) 'uvoznik podataka' je obrađivač koji prihvata da dobija od izvoznika podataka lične podatke planirane za obradu u njegovo ime nakon prenosa po ovim uputama i uslovima Odredbi i koji nije podložan sistemu treće zemlje dajući adekvatnu zaštitu u okviru značenja Člana 25 (1) Direktivi 95/46/EC;
- (d) 'pod-obrađivač' je bilo koji obrađivač kojeg je angažovao uvoznik podataka ili neki drugi pod-obrađivač uvoznika podataka koji prihvata da dobija od uvoznika podataka ili nekog drugog pod-obrađivača uvoznika podataka lične podatke koji su isključivo planirani za obradu koja će se izvršiti u ime izvoznika podataka nakon prenosa po ovim uputama, uslovima Odredbi i uslovima pismenog pod-ugovora;

- (e) 'važeći zakon o zaštiti podataka' je zakon koji štiti osnovna ljudska prava i slobode i, naročito, pravo na privatnost vezano za obradu ličnih podataka koji su primjenljivi na kontrolora podataka u zemlji članici u kojoj je osnovan izvoznik podataka;
- (f) 'mjere tehničke i organizacione sigurnosti' su mjere čiji je cilj zaštita ličnih podataka od slučajnog ili nezakonitog uništenja ili slučajnog gubitka, zamjene, neovlaštenog otkrivanja ili pristupa, naročito ako obrada obuhvata prenos podataka preko mreže, i od svih ostalih nezakonitih oblika obrade.

Odredba 2

Podaci o prenosu

Podaci o prenosu a naročito specijalne kategorije ličnih podataka gdje je primjenljivo definisani su u Dodatku 1 koji čini sastavni dio Odredbi.

Odredba 3

Treća strana kao korisnik

1. Nosilac podataka može sprovesti protiv izvoznika podataka ovu Odredbu, Odredbu 4 (b) do (i), Odredbu 5 (a) do (e) i (g) do (j), Odredbu 6 (1) i (2), Odredbu 7, Odredbu 8 (2) i Odredbe 9 do 12 kao treća strana kao korisnik.
2. Nosilac podataka može sprovesti protiv uvoznika podataka ovu Odredbu, Odredbu 5 (a) do (e) i (g), Odredbu 6, Odredbu 7, Odredbu 8 (2) i Odredbe 9 do 12 u slučajevima kada izvoznik podataka nestane ili prestane da postoji po zakonu osim ako bilo koji nasljednik ne preuzme sve zakonske obaveze izvoznika podataka putem ugovora ili primjene zakona, što dovodi do njegovog preuzimanja prava i obaveza izvoznika podataka, i u tom slučaju nosilac podataka može ih sprovesti protiv te cjeline.
3. Nosilac podataka može sprovesti protiv pod-obrađivača ovu Odredbu, Odredbu 4 (b) do (i), Odredbu 5 (a) do (e) i (g), Odredbu 6, Odredbu 7, Odredbu 8 (2) i Odredbe 9 do 12 u slučajevima kada i izvoznik i uvoznik podataka nestanu ili prestanu da postoje po zakonu ili postanu nesolventni osim ako bilo koji nasljednik ne preuzme sve zakonske obaveze izvoznika podataka putem ugovora ili primjene zakona, što dovodi do njegovog preuzimanja prava i obaveza izvoznika podataka, i u tom slučaju nosilac podataka može ih sprovesti protiv te cjeline. Odgovornost pod-obrađivača prema trećim licima biće ograničena na njegove vlastite aktivnosti obrade u skladu s Odredbama.
4. Strane nisu protivne da nosioca podataka predstavlja neko udruženje ili drugi organ ukoliko nosilac podataka to izričito želi i ukoliko je zakonski dozvoljeno.

Odredba 4

Obaveze izvoznika podataka

Izvoznik podataka prihvata i garantuje slijedeće:

- (a) da je obrada, uključujući prenos, ličnih podataka bila i biće i dalje izvršavana po odgovarajućim odredbama važećeg zakona o zaštiti podataka (i, gdje je primjenljivo, relevantni organi vlasti zemlje članice u kojoj je osnovan izvoznik podataka biće obaviješteni) i da ne krši odgovarajuće odredbe te zemlje;
- (b) da je dao i da će davati uvozniku podataka upute tokom trajanja usluga obrade ličnih podataka radi obrade ličnih podataka čiji prenos je izvršen samo u ime izvoznika podataka i po važećem zakonu o zaštiti podataka i Odredbama;
- (c) da će uvoznik podataka dati dovoljno garancija za mjere tehničke i organizacione sigurnosti koje su definisane u Dodatku 2 ovog Ugovora;

- (d) da su, nakon analize zahtjeva važećeg zakona o zaštiti podataka, mjere sigurnosti adekvatne za zaštitu ličnih podataka od slučajnog ili nezakonitog uništenja ili slučajnog gubitka, zamjene, neovlaštenog otkrivanja ili pristupa, naročito ako obrada obuhvata prenos podataka preko mreže, i od svih ostalih nezakonitih oblika obrade, i da ove mjere obezbijavaju nivo sigurnosti koji je adekvatan rizicima obrade i prirodi podataka koji će se zaštititi s obzirom na savremenost i cijenu njihove primjene;
- (e) da će obezbijediti usaglašenost sa mjerama sigurnosti;
- (f) da je, ako prenos obuhvata specijalne kategorije podataka, nosilac podataka bio ili će biti obaviješten prije ili što prije nakon prenosa da se može izvršiti prenos njegovih podataka u neku treću zemlju koja ne pruža adekvatnu zaštitu u okviru značenja Direktive 95/46/EC;
- (g) da će proslijediti organu za nadzor zaštite podataka sve obavijesti koje dobije od uvoznika podataka ili pod-obrađivača po Odredbama 5 (b) i 8 (3) ukoliko izvoznik podataka odluči da nastavi prenos ili da ukine suspenziju;
- (h) da stavi na raspolaganje na osnovu zahtjeva nosioca podataka kopiju Odredbi, izuzev Dodatka 2, i kratki opis mjera sigurnosti, kao i kopiju svakog ugovora o uslugama pod-obrađivanja koji mora biti sastavljen u skladu s Odredbama, osim ako Odredbe ili ugovor sadrže komercijalne informacije, i u tom slučaju može ukloniti te komercijalne informacije;
- (i) da se, u slučaju pod-obrade, obrada vrši po Odredbi 11 od strane pod-obrađivača koji daje bar isti nivo zaštite ličnih podataka i prava nosioca podataka kao uvoznik podataka u skladu s Odredbama; i
- (j) da će obezbijediti usaglašenost sa Odredbom 4 (a) do (i).

Odredba 5

Obaveze uvoznika podataka

Uvoznik podataka prihvata i garantuje slijedeće:

- (a) da će obrađivati lične podatke samo u ime izvoznika podataka i po uputama i Odredbama; ukoliko to ne može obezbijediti iz bilo kojeg razloga, prihvata da odmah obavijesti izvoznika podataka o tome i u tom slučaju izvoznik podataka ima pravo da obustavi prenos podataka i/ili da raskine ugovor;
- (b) da nema razloga da vjeruje da ga važeći zakon sprječava da slijedi upute izvoznika podataka i vrši svoje obaveze iz ugovora i da će u slučaju promjene zakona koji bi mogao imati značajan suprotni efekat na garancije i obaveze iz Odredbi, odmah obavijestiti izvoznika podataka čim sazna za tu promjenu, i u tom slučaju izvoznik podataka ima pravo da obustavi prenos podataka i/ili da raskine ugovor;
- (c) da je primijenio mjere tehničke i organizacione sigurnosti koje su definisane u Dodatku 2 prije obrade ličnih podataka čiji prenos je izvršen;
- (d) da će odmah obavijestiti izvoznika podataka o slijedećem;
 - i. o bilo kojem zakonski obavezujućem zahtjevu za otkrivanje ličnih podataka od strane organa za provođenje zakona osim ako bude zabranjeno drugačije, kao što je zabrana po krivičnom zakonu da se čuva povjerljivost istrage o provođenju zakona;
 - ii. o bilo kojem slučajnom ili neovlaštenom pristupu; i
 - iii. o bilo kojem zahtjevu koji je dobio direktno od nosioca podataka bez davanja odgovora na taj zahtjev, osim ako je drugačije ovlašten da to uradi;
- (e) da će odmah i pravilno rješavati sve upite izvoznika podataka o obradi ličnih podataka koji su predmet prenosa i pridržavati se savjeta nadzornog organa po pitanju obrade prenesenih podataka;

- (f) da će na osnovu zahtjeva izvoznika podataka poslati svoje uređaje za obradu podataka na reviziju aktivnosti obrade koje Odredbe pokrivaju koje će izvršiti izvoznik podataka ili organ inspekcije koji je sastavljen od nezavisnih članova i koji imaju potrebne profesionalne kvalifikacije i obavezu povjerljivosti, a koje bira izvoznik podataka, gdje je moguće, u dogovoru sa nadzornim organom;
- (g) da će dati na raspolaganje na osnovu zahtjeva nosioca podataka kopiju Odredbi, ili bilo kojeg postojećeg ugovora o pod-obradivanju, osim ako Odredbe ili ugovor sadrže komercijalne informacije, i u tom slučaju može ukloniti te komercijalne informacije, osim Dodatka 2 koji će zamijeniti kratkim opisom mjera sigurnosti u slučajevima u kojim nosilac podataka ne može da dobije kopiju od izvoznika podataka;
- (h) da je, u slučaju pod-obrade podataka, prethodno obavijestio izvoznika podataka i dobio njegovu prethodnu pismenu saglasnost;
- (i) da će usluge obrade od strane pod-obradivača biti izvršene u skladu s Odredbom 11;
- (j) da će odmah poslati kopiju bilo kojeg ugovora o pod-obradi koji zaključi po Odredbama izvoznika podataka.

Odredba 6 Odgovornost

1. Strane prihvataju da bilo koji nosilac podataka, koji je pretrpio štetu zbog bilo kojeg prekršaja obaveza iz Odredbi 3 ili 11 od strane bilo koje strane ili pod-obradivača ima pravo da dobije nadoknadu od izvoznika podataka zbog pretrpljene štete.
2. Ukoliko nosilac podataka ne može da podnese zahtjev za nadoknadu u skladu s odlomkom 1 protiv izvoznika podataka, zbog prekršaja od strane uvoznika podataka ili njegovog pod-obradivača bilo kojih njihovih obaveza iz Odredbi 3 ili 11, zato što je izvoznik podataka nestao ili prestao da zakonski postoji ili je postao nesolventan, uvoznik podataka prihvata da nosilac podataka izda zahtjev protiv uvoznika podataka kao da je izvoznik podataka, osim ako bilo koji nasljednik preuzme sve zakonske obaveze izvoznika podataka putem ugovora ili primjene zakona, i u tom slučaju nosilac podataka može ostvariti svoja prava protiv te cjeline. Uvoznik podataka ne može se osloniti na prekršaj obaveza od strane pod-obradivača da bi izbjegao svoju odgovornost.
3. Ukoliko nosilac podataka ne može da podnese zahtjev u skladu s odlomcima 1 i 2 protiv izvoznika ili uvoznika podataka, zbog prekršaja od strane pod-obradivača bilo kojih njihovih obaveza iz Odredbi 3 ili 11, zato što je izvoznik ili uvoznik podataka nestao ili prestao da zakonski postoji ili je postao nesolventan, pod-obradivač prihvata da nosilac podataka izda zahtjev protiv pod-obradivača podataka vezano za njegove aktivnosti obrade po Odredbama kao da je izvoznik ili uvoznik podataka, osim ako bilo koji nasljednik preuzme sve zakonske obaveze izvoznika ili uvoznika podataka putem ugovora ili primjene zakona, i u tom slučaju nosilac podataka može ostvariti svoja prava protiv te cjeline. Odgovornost pod-obradivača biće ograničena na njegove aktivnosti obrade u skladu s Odredbama.

Odredba 7 Posredovanje i nadležnost

1. Uvoznik podataka prihvata da ako se nosilac podataka poziva protiv njega na prava trećeg lica kao korisnika i/ili zahtjeva nadoknadu šteta u skladu s Odredbama, uvoznik podataka će prihvatiti odluku nosioca podataka:
 - (a) da podnese spor na posredovanje od strane nezavisnog lica ili, gdje je izvodivo, nadzornog organa;

- (b) da podnese spor sudovima u zemlji članici u kojoj je osnovan izvoznik podataka.
2. Strane prihvataju da izbor nosioca podataka neće biti štetan po njegova materijalna ili proceduralna prava da traži sredstva po ostalim odredbama državnog ili međunarodnog zakona.

Odredba 8

Saradnja sa nadzornim organima

1. Izvoznik podataka prihvata da deponuje kopiju ovog Ugovora kod nadzornog organa ukoliko to zatraži ili ukoliko je to deponovanje potrebno po važećem zakonu o zaštiti podataka.
2. Strane prihvataju da nadzorni organ ima pravo na reviziju uvoznika podataka, i bilo kojeg pod-obrađivača, koji ima isti djelokrug i podložan je istim uslovima koji bi se primijenili na reviziju izvoznika podataka po važećem zakonu o zaštiti podataka.
3. Uvoznik podataka će odmah obavijestiti izvoznika podataka o zakonima koji su primjenljivi ili bilo kojem pod-obrađivaču koji sprječava reviziju uvoznika podataka, ili bilo kojeg pod-obrađivača, u skladu s odlomkom 2. U tom slučaju izvoznik podataka imaće pravo da preduzme mjere iz Odredbe 5 (b).

Odredba 9

Vladajući zakon

Na Odredbe će se primjenjivati zakon zemlje članice u kojoj je osnovan izvoznik podataka.

Odredba 10

Promjena ugovora

Strane prihvataju da neće mijenjati ili modifikovati Odredbe. To ne sprječava strane da dodaju odredbe o poslovnim pitanjima kada zatreba sve dok nisu kontradiktorne Odredbama.

Odredba 11

Pod-obrada podataka

1. Uvoznik podataka neće izvršiti pod-ugovaranje bilo koje svoje aktivnosti obrade koja je obavljena u ime izvoznika podataka po Odredbama bez prethodne pismene saglasnosti izvoznika podataka. Ako uvoznik podataka pod-ugovori svoje obaveze iz Odredbi, uz saglasnost izvoznika podataka, uradiće to samo putem pismenog sporazuma sa pod-obrađivačem koji nameće iste obaveze za pod-obrađivača koje su nametnute uvozniku podataka u skladu s Odredbama. Ako pod-obrađivač ne izvrši svoje obaveze zaštite podataka po tom pismenom sporazumu uvoznik podataka ostaće potpuno odgovoran izvozniku podataka za izvršenje obaveza pod-obrađivača iz tog sporazuma.
2. Prethodni pismeni ugovor između uvoznika podataka i pod-obrađivača će imati i odredbu o trećoj strani kao korisniku iz Odredbe 3 za slučajeve u kojim nosilac podataka ne može da podnese zahtjev za nadoknadu iz odlomka 1 Odredbe 6 protiv izvoznika ili uvoznika podataka jer su nestali ili prestali da postoje po zakonu ili su postali nesolventni ili ni jedan nasljednik ne preuzme sve zakonske obaveze izvoznika ili uvoznika podataka putem ugovora ili primjene zakona. Ta odgovornost pod-obrađivača prema trećoj strani biće ograničena na njegove aktivnosti obrade u skladu s Odredbama.

3. Za odredbe o aspektima zaštite podataka za pod-obradu ugovora iz odlomka 1 biće mjerodavan zakon zemlje članice u kojoj je osnovan izvoznik podataka.
4. Izvoznik podataka će imati spisak ugovora o pod-obradi podataka koji su zaključeni po Odredbama i o kojim je uvoznik podataka obavijestio u skladu s Odredbom 5 (j), a koji će biti ažurirani bar jedanput godišnje. Spisak će biti na raspolaganju nadzornom organu izvoznika podataka za zaštitu podataka.

Odredba 12

Obaveza nakon raskida usluga obrade ličnih podataka

1. Strane prihvataju da će po raskidu davanja usluga obrade podataka, uvoznik podataka i pod-obrađivač, po izboru izvoznika podataka, vratiti izvozniku podataka sve dostavljene lične podatke i njihove kopije ili će uništiti sve lične podatke i potvrditi izvozniku podataka da je to uradio, osim ako zakon koji je nametnut uvozniku podataka spriječi da isti vrati ili uništi sve ili dio dostavljenih ličnih podataka. U tom slučaju uvoznik podataka izjavljuje da će garantovati povjerljivost dostavljenih ličnih podataka i da više neće aktivno obrađivati dostavljene lične podatke.
2. Uvoznik podataka i pod-obrađivač garantuju da će na osnovu zahtjeva izvoznika podataka i/ili nadzornog organa dostaviti svoje uređaje za obradu podataka na reviziju mjera u skladu s odlomkom 1.

Dodatak 1 Standardnih ugovornih odredbi

Ovaj Dodatak čini dio odredbi i strane ga moraju izvršiti i potpisati.

Zemlje članice mogu definisati, u skladu sa njihovim državnim procedurama, sve dodatne informacije koje trebaju biti u ovom Dodatku.

Izvoznik podataka: Korisnik koji je definisan u UOP-u je izvoznik podataka.

Uvoznik podataka: Uvoznik podataka je AO Kaspersky Lab, Bldg. 3, 39A, Leningradskoe Shosse, Moskva, 125212, Ruska Federacija, međunarodna firma koja se bavi razvojem rješenja softverske sigurnosti i davalac softverskog rješenja Kaspersky Endpoint Security Cloud ("Proizvod").

Nosioci podataka: Dostavljeni lični podaci odnose se na korisnike Softvera po definiciji iz Pod-dijela 1 Aneksa 1 ovog UOP-a.

Kategorije podataka: Djelokrug i kategorije podataka definisani su u Pod-dijelu 1 Aneksa 1 ovog UOP-a.

Specijalne kategorije podataka (ako je prikladno): Prenos specijalnih kategorija podataka nije predviđen.

Aktivnosti obrade: Dostavljeni lični podaci biće podložni aktivnostima obrade u skladu s Ugovorom i UOP-om, naročito s Pod-dijelom 1 Aneksa 1 ovog UOP-a.

Dodatak 2 Standardnih ugovornih odredbi

Opis mjera tehničke i organizacione sigurnosti koje je primijenio uvoznik podataka po Odredbama 4 (d) i 5 (c):

1. Tehničke i organizacione mjere. Uvoznik podataka je primijenio i primjenjivaće odgovarajuće mjere tehničke i organizacione sigurnosti, internet kontrole i standardne procedure po pitanju sigurnosti informacija u svrhu zaštite Korisničkih podataka, što je definisano u Pod-dijelu 2 Aneksa 1 ovog UOP-a, od slučajnog gubitka, uništenja ili zamjene, neovlaštenog otkrivanja ili pristupa, ili nezakonitog uništenja.
2. Kontakti. Za sva pitanja o obradi Korisničkih podataka molimo da kontaktirate predstavnika Kaspersky Lab-a u EU putem e-maila ili broja: Kaspersky Lab GmbH, Ingolstadt, Njemačka, info@kaspersky.de, +49 (0) 841 98 18 90.