

ALSO personas datu apstrādes noteikumi

1. NOTEIKUMOS LIETOTO TERMINU SKAIDROJUMI

Termins	Apraksts
ALSO	SIA "ALSO Latvia", reģ. Nr.: 40003274889, juridiskā adrese Liliju iela 29, Mārupe, LV-2167, kas šo Noteikumu ietvaros darbojas kā datu apstrādātājs.
Apstiprinājums	elektroniskā pasta saziņa vai saziņa caur E-komercijas vietni starp ALSO un KLIENTU
E-komercijas vietne	ALSO tīmekļa vietne <i>lv.also.com</i>
GDPR	Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula).
KLIENTS	Juridiskā persona, kas sadarbojas ar ALSO uz Sadarbības līguma (Līgums) pamata un šo Noteikumu ietvaros darbojas kā datu pārzinis.
Noteikumi	Šie ALSO personas datu apstrādes noteikumi, ieskaitot to pielikumus, kas KLIENTAM ir pieejami ALSO E-komercijas vietnē.
Puses	ALSO un KLIENTS.
Sadarbības līgums	rakstveida līgums, kas noslēgts starp ALSO un KLIENTU

GDPR 4. pantā lietotās definīcijas ir piemērojamas arī šiem Noteikumiem.

2. DATU APSTRĀDES VEIDS UN MĒRĶIS

2.1. Personas datu veidi

2.1.1. Personas identifikācijas dati (galvenie personas dati), kontaktinformācija, galvenie līguma dati (tiesiskās attiecības, intereses), personas vēsture, rēķinu un norēķinu informācija, iegūtā informācija (no trešajām personām, piemēram, kredītvēstures

- aģentūrām vai publiski pieejamiem avotiem), informācija par sistēmas konfigurāciju un klienta vidi, u.c. personas dati, kuru apstrādi KLIENTS uztic ALSO.
- 2.2. Noteikumi ir piemērojami Sadarbības līguma termiņā, un attiecībā uz konkrētiem pakalpojumiem – līdz konkrētā pakalpojuma izbeigšanas vai izbeigšanās brīdim.
- 2.3. Apstrādes mērķis
- 2.3.1. ALSO pakalpojumu un uzdevumu izpilde: tehniskais atbalsts, pasūtījumu apstrāde, IT pakalpojumi, klientu apkalpošana, mākoņpakalpojumi un citu KLIENTA pamatotu norādījumu izpilde, ja šādi norādījumi atbilst Noteikumiem.
- 2.4. Datu subjektu kategorijas
- 2.4.1. KLIENTA darbinieki, biznesa partneri, potenciālie klienti, lietotāji, pārdevēji, piegādātāji, ieinteresētās personas, u.c.
- 2.5. KLIENTS nodrošina, ka ir tiesīgs un tam ir nepieciešamās pilnvaras veikt personas datu nodošanu ALSO, tas ir iesniedzis nepieciešamos paziņojumus un saņēmis no fiziskām personām nepieciešamo piekrišanu. KLIENTS vienpersoniski atbild par ALSO nodoto personas datu atbilstību, tiesiskumu un precizitāti.
- 2.6. Personas datu apstrāde notiek tikai Eiropas Savienības (ES) dalībvalstī, Eiropas Ekonomikas zonas (EEZ) dalībvalstī vai valstī, kas pakļauta Eiropas Komisijas lēmumam. Katrai datu nodošanai uz valsti, kas nav ES vai EEZ dalībvalsts, ir nepieciešama iepriekšēja KLIENTA piekrišana, un tikai tad, ja ievēroti GDPR noteikumi attiecībā uz personas datu nosūtīšanu uz trešām valstīm vai starptautiskām organizācijām.

3. TEHNISKI ORGANIZATORISKIE PASĀKUMI

- 3.1. ALSO veic pasākumus atbilstoši GDPR 28. panta trešās daļas c) punkta un 32. panta nosacījumiem, it sevišķi – saistībā ar GDPR 5. panta pirmo un otro daļu. Veiktie pasākumi ir datu drošības pasākumi un pasākumi, kas garantē aizsardzības līmeni, kas ir atbilstošs riskam attiecībā uz sistēmu konfidencialitāti, integritāti, pieejamību un noturību. Jāņem vērā GDPR 32. panta pirmajā daļā minētais sistēmu stāvoklis, ieviešanas izmaksas, datu apstrādes daba, apmērs un mērķi, kā arī risku attiecībā uz personu tiesībām un brīvībām iestāšanās iespējamība un to smagums (detalizētāka informācija 1. pielikumā).
- 3.2. Tehniski organizatoriskie pasākumi ir pakļauti tehnikas attīstībai un tālākām pārmaiņām. Attiecīgi ALSO ir atļauts ieviest alternatīvus adekvātus pasākumus. To darot, aizliegts samazināt noteikto pasākumu drošības līmeni. Ievērojamas izmaiņas dokumentē.

4. DATU LABOŠANA, IEROBEŽOŠANA UN DZĒŠANA

- 4.1. ALSO nedrīkst pēc savas iniciatīvas labot, dzēst vai ierobežot to datu apstrādi, kas tiek apstrādāti KLIENTA labā. To atļauts darīt tikai pēc dokumentētu instrukciju saņemšanas no KLIENTA. Ja datu subjekts sazinās ar ALSO par datu labojumiem, dzēšanu vai to apstrādes ierobežošanu, ALSO nekavējoties pārsūta datu subjekta pieprasījumus KLIENTAM.

4.2. Tādā mērā, cik tas ir saprātīgi sagaidāms no ALSO, ALSO nodrošina datu dzēšanas politiku, „tiesības tikt aizmirstam”, labojumus, datu pārnēsamību un piekļuvi tiem atbilstoši dokumentētām KLIENTA instrukcijām bez nepamatotas kavēšanās.

5. KVALITĀTES NODROŠINĀŠANA UN CITI ALSO PIENĀKUMI

5.1. ALSO ievēro GDPR 28. - 33. pantā noteiktās prasības un nodrošina, ka:

5.1.1. Par kontaktpersonu ALSO vārdā tiek nozīmēta persona, kas norādīta ALSO e-komercijas tīmekļa vietnē *lv.also.com*. ALSO nav pienākuma iecelt datu aizsardzības speciālistu atbilstoši GDPR 37. līdz 39. pantam.

5.1.2. Noteikumos minēto datu apstrādi ALSO uztic tikai tādiem darbiniekiem, ar kuriem ir noslēgts konfidencialitātes līgums un kuri ir iepriekš iepazīstināti ar viņu darbam atbilstošajām datu aizsardzības metodēm. ALSO un jebkurai personai, kas darbojas ALSO pakļautībā un kurai ir pieeja personas datiem, nav tiesību apstrādāt šo informāciju, izņemot, ja tiek saņemtas tiešas instrukcijas no KLIENTA vai, ja tas tiek pieprasīts atbilstoši normatīvajiem aktiem; instrukcijas iekļauj arī piešķirtās pilnvaras.

5.1.3. Nepieciešamo tehnisko un organizatorisko pasākumu ieviešana un atbilstība tiem notiek saskaņā ar GDPR 28. panta trešās daļas otrā teikuma c) punktu un 32. pantu (detalizētāk 1. pielikumā).

5.1.4. KLIENTS un ALSO pēc pieprasījuma sadarbojas ar datu aizsardzības uzraudzības iestādi tās pienākumu veikšanas laikā.

5.1.5. Puses nekavējoties informē viena otru par pārbaudēm vai citiem pasākumiem, kurus veic uzraudzības iestāde, ja tās ir saistītas ar datu apstrādi, kas veikta Pušu starpā pastāvošo saistību ietvaros. Tas attiecas arī uz gadījumiem, ja kāda Puse tiek izmeklēta, vai ir iesaistīts atbilstošās iestādes veiktā izmeklēšanā attiecībā uz personas datu apstrādes pārkāpumiem starp Pusēm pastāvošo saistību ietvaros.

5.1.6. Ja kāda no Pusēm tiek pakļauts uzraudzības iestādes izmeklēšanai, vai uz to attiecas administratīvais vai kriminālprocess, tiek saņemts prasījums no datu subjekta vai trešās puses, vai jebkāds cits prasījums, kas attiecas uz starp Pusēm pastāvošo saistību ietvaros veikto datu apstrādi, Puses pieliek saprātīgas pūles, lai atbalstītu otru Pusi.

5.1.7. Puses regulāri uzrauga iekšējos procesus un tehniski organizatoriskos pasākumus, lai nodrošinātu, ka datu apstrāde uzņēmuma atbildības jomā notiek atbilstoši piemērojamiem datu aizsardzības normatīvajiem aktiem un datu subjekta tiesību aizsardzības principiem.

5.2. KLIENTA tehnisko un organizatorisko pasākumu pārbaudāmība ietilpst Noteikumu 7. punktā paredzētajās KLIENTA uzraudzības pilnvarās.

6. APAKŠLĪGUMS

6.1. Apakšlīgums ir vienošanās par tādiem pakalpojumiem, kas tieši saistīti ar galvenā pakalpojuma nodrošināšanu. Tajā neietilpst papildpakalpojumi, tādi kā

telekomunikācijas pakalpojumi, pasta vai transporta pakalpojumi, apkopes vai lietotāju atbalsta pakalpojumi vai atbrīvošanās no datu nesējiem, kā arī citi pasākumi, kas tiek veikti, lai nodrošinātu datu apstrādes aprīkojuma (gan aparatūras, gan programmatūras) konfidencialitāti, pieejamību, integritāti un noturību. ALSO slēdz nepieciešamos līgumus un veic atbilstošus uzraudzības pasākumus, lai nodrošinātu KLIENTA datu aizsardzību un drošību arī ārēji veiktu papildpakalpojumu gadījumā.

- 6.2. Pasūtījumus var nodot apakšuzņēmējiem, ja tiek ievērota pasūtījumā noteikto aktivitāšu struktūra. Izvēloties apakšuzņēmējus, ALSO ņem vērā to piemērotību, it sevišķi – attiecībā uz GDPR nosacījumiem, un tos uzrauga. ALSO noslēdz ar apakšuzņēmējiem līgums par pasūtījumu apstrādi atbilstoši Noteikumiem. ALSO laicīgi informē KLIENTU par plānotām izmaiņām attiecībā uz apakšuzņēmēju iesaisti vai to nomaiņu, sniedzot KLIENTAM iespēju iebilst pret izmaiņām. Ja 14 (četrpadsmit) dienu laikā pēc paziņošanas nav celti iebildumi, tiek uzskatīts, ka KLIENTS piekrīt konkrētajām izmaiņām.
- 6.3. Personas datu pārsūtīšanu apakšuzņēmējiem un datu apstrādes uzsākšanu apakšuzņēmēja uzņēmumā ir atļauts veikt tikai pēc tam, kad izpildīts 6.2. punktā noteiktais.
- 6.4. Ja apakšuzņēmējs nodrošina līgumā noteikto pakalpojumu ārpus ES, ALSO nodrošina atbilstību GDPR, izmantojot atbilstošus pasākumus. Tas pats attiecas uz gadījumiem, ja pakalpojumu sniedz atbilstoši 6.1. punkta otrajam teikumam.
- 6.5. Tālākai apakšuzņēmēju izmantošanai nepieciešama galvenā piegādātāja piekrišana (vismaz rakstveida formā, elektroniski). Uz otro apakšuzņēmēju attiecas Noteikumi un, arī citi līgumu ķēdē ievērojamie noteikumi.

7. KLIENTA UZRAUDZĪBAS TIESĪBAS

- 7.1. KLIENTAM ir tiesības, pēc konsultēšanās ar ALSO, veikt apskates, ja tās veic persona, kurai ir pienākums ievērot profesionālo konfidencialitāti un objektivitāti, vai auditors, kurš tiek iecelts katrā atsevišķā gadījumā. Šai personai ir tiesības pārliecināties par ALSO atbilstību Noteikumiem, veicot pārbaudes, par kurām KLIENTS paziņo ALSO vismaz 3 (trīs) nedēļas pirms pārbaudes dienas.
- 7.2. Pārbaudi veic standarta darba laikā, minimāli traucējot ALSO efektīvai komercdarbībai.
- 7.3. ALSO nodrošina KLIENTAM pieeju telpām, ko tas izmanto personas datu apstrādei, audita mērķim. ALSO apņemas pēc pieprasījuma sniegt KLIENTAM nepieciešamo informāciju un kopumā demonstrēt tehnisko un organizatorisko pasākumu izpildi.
- 7.4. Pierādījumi par šādu pasākumu, kas attiecas ne tikai uz konkrēto pasūtījumu vai līgumu, izpildi var tikt nodrošināti, ievērojot apstiprināto rīcības kodeksu atbilstoši GDPR 40. pantam; izmantojot sertifikāciju atbilstoši apstiprinātajai sertifikācijas procedūrai, kas noteikta GDPR 42. pantā; izmantojot pašreizējos auditoru sertifikātus, ziņojumus vai ziņojumu kopsavilkumus, ja tos nodrošinājušas neatkarīgas organizācijas (piemēram, auditori, atbildīgais par datu aizsardzību, IT drošības departaments, datu privātuma auditors vai kvalitātes auditors); izmantojot atbilstošu IT drošības vai datu

aizsardzības auditu (piemēram, atbilstoši *BSI-Grundschutz* (IT pamata aizsardzības sertifikācija, ko izstrādājis Vācijas Federālais birojs drošībai informācijas tehnoloģijās) vai ISO/IEC 27001).

7.5. ALSO var pieprasīt samaksu par KLIENTA pārbaūžu nodrošināšanu.

8. SADARBĪBA

- 8.1. Puses nodrošina viena otrai saprātīgu atbalstu un sadarbību saistību izpildes ietvaros.
- 8.2. ALSO atbalsta KLIENTU, nodrošinot atbilstību saistībām, kas saistītas ar personas datu drošību, datu aizsardzības pārkāpumu ziņošanu, datu aizsardzības ietekmes novērtējumu un sākotnējām konsultācijām, kas minētas GDPR 32. līdz 36. pantā. Tostarp:
 - 8.2.1. Nodrošina pietiekamu aizsardzības līmeni, izmantojot tehniskus un organizatoriskus pasākumus, kas ņem vērā datu apstrādes apstākļus un mērķus, kā arī drošības trūkumu rezultātā radušos iespējamu normatīvo aktu pārkāpumu plānoto varbūtību un smagumu, tādējādi nodrošinot attiecīgo pārkāpumu tūlītēju noteikšanu.
 - 8.2.2. nekavējoties ziņo KLIENTAM par personas datu aizsardzības pārkāpumiem.
 - 8.2.3. palīdz KLIENTAM attiecībā uz KLIENTA pienākumiem nodrošināt informācijas sniegšanu attiecīgajam datu subjektam, kā arī nekavējoties nodrošina KLIENTAM visu nepieciešamo informāciju par šo aspektu.
 - 8.2.4. atbalsta KLIENTU ar datu aizsardzības ietekmes novērtējumu.
 - 8.2.5. atbalsta KLIENTU attiecībā uz uzraudzības iestādes sākotnējo konsultāciju.
- 8.3. ALSO var pieprasīt kompensāciju par atbalsta pakalpojumiem, kuri nav iekļauti iepriekš minētajā pakalpojumu aprakstā, un, kuri nav saistīti ar ALSO problēmām.

9. KLIENTA TIESĪBAS IZDOT INSTRUKCIJAS

- 9.1. KLIENTS nekavējoties apstiprina mutiski sniegtas instrukcijas (rakstveida formā elektroniski).
- 9.2. KLIENTS sniedz norādījumus, kas atbilst piemērojamo tiesību aktu prasībām un neradīs ALSO piemērojamo tiesību aktu pārkāpumu.
- 9.3. ALSO nekavējoties informē KLIENTU, ja uzskata, ka instrukcijas pārkāpj datu aizsardzības normatīvos aktus. ALSO tādā gadījumā ir tiesības pārtraukt atbilstošo instrukciju izpildi, līdz KLIENTS tās apstiprina vai izmaina.

10. PERSONAS DATU DZĒŠANA UN ATGRIEŠANA

- 10.1. Ja KLIENTS par to nav informēts, nav atļauts veidot datu kopijas, izņemot rezerves kopijas, ja tās ir nepieciešamas savlaicīgai datu apstrādei, kā arī datu kopijas, kas nepieciešamas, lai nodrošinātu normatīvajos aktos noteiktās prasības datu uzglabāšanai.

- 10.2. Pēc Noteikumos paredzēto uzdevumu veikšanas vai agrāk, pēc KLIENTA pieprasījuma, bet ne vēlāk par pakalpojuma vai Līguma izbeigšanu vai izbeigšanos, ALSO nodod KLIENTAM, vai, ja par to ir bijusi iepriekšēja vienošanās, iznīcina ALSO rīcībā esošos dokumentus, datu apstrādes un izmantošanas rezultātus, kā arī datu kopas, kas attiecas uz Pušu starpā vairs nepastāvošām saistībām, un visus saistītos testa, izlietotos, nevajadzīgos un noraidītos materiālus. Pēc pieprasījuma ir jāsniedz pierādījumi iznīcināšanas vai izdzēšanas faktam, ja tas ir tehniski iespējams.
- 10.3. Dokumentāciju, kas tiek izmantota atbilstīgas datu apstrādes demonstrēšanā atbilstoši Noteikumiem, ALSO uzglabā ilgāk par Sadarbības līguma termiņu atbilstoši attiecīgajiem uzglabāšanas termiņiem. ALSO var nodot šādu dokumentāciju KLIENTAM Sadarbības līguma termiņa beigās, tādējādi atbrīvojoties no šī pienākuma.

11. ATBILDĪBA

- 11.1. ALSO kopējā atbildība par prasījumiem, kas izriet no konkrētajām datu apstrādes saistībām, ir ierobežota ar tiešajiem zaudējumiem, kas izriet no ALSO pieļautas rupjas neuzmanības un aprobežojas ar KLIENTA par pakalpojumiem (kas ir pārkāpuma pamatā) samaksāto summu pēdējo sešu mēnešu ietvaros.

Pielikums Nr. 1

Tehniski organizatoriskie pasākumi

1. KONFIDENCIALITĀTE (GDPR 32. panta pirmās daļas b. punkts)

1.1. Fiziskās pieejas kontrole:

- 1.1.1. aizliegta neautorizēta pieeja datu apstrādes iekārtām, ko iespējams nodrošināt, izmantojot, piemēram, magnētiskās vai čipa kartes, atslēgas, elektronisku durvju atvēršanu, ēkas drošības dienestu un/vai ieejas drošības darbiniekus, brīdinājuma sistēmas, video/CCTV sistēmas.

1.2. Elektroniskās pieejas kontrole:

- 1.2.1. aizliegta neautorizēta datu apstrādes un datu uzglabāšanas sistēmu izmantošana, ko iespējams nodrošināt, izmantojot, piemēram, (drošas) paroles, automatiskos bloķēšanas/slēgšanas mehānismus, divu faktoru autentifikāciju, datu nesēju un uzglabāšanas iekārtu šifrēšana.
- 1.3. Iekšējās pieejas kontrole (lietotāju piekļuves tiesību un datu mainīšanas tiesību nodrošināšana):
 - 1.3.1. sistēmā aizliegts neautorizētām personām lasīt, kopēt, rediģēt vai dzēst datus, ko iespējams nodrošināt, izmantojot, piemēram, piekļuves tiesību konceptu, vajadzībā balstītas, pieejas tiesības un sistēmas piekļuves reģistrēšanu.
- 1.4. Izolācijas kontrole:
 - 1.4.1. dažādiem mērķiem ievāktu datu izolēta apstrāde, piemēram, ja tiek apkalpoti vairāki klienti; to iespējams nodrošināt, izmantojot t.s. *sandboxing* konceptu (atdalot darbojošos programmu darbību).
- 1.5. Pseidonimizācija (GDPR 32. panta pirmās daļas a. punkts; GDPR 25. panta pirmā daļa):
 - 1.5.1. personas datu apstrāde tādā veidā, ka šos datus nevar saistīt ar konkrēto datu subjektu bez papildu informācijas, ja šī papildu informācija tiek uzglabāta atsevišķi un ir pakļauta atbilstošajiem tehniskajiem un organizatoriskajiem pasākumiem.

2. INTEGRITĀTE (GDPR 32. panta pirmās daļas b. punkts)

- 2.1. Datu nodošanas kontrole:
 - 2.1.1. aizliegts datus lasīt, kopēt, rediģēt vai dzēst elektroniskās nodošanas vai transportēšanas laikā; to iespējams nodrošināt, izmantojot, piemēram, šifrēšanu, virtuālos privātos tīklus (VPN) vai elektroniskos parakstus.
- 2.2. Datu ievades kontrole:
 - 2.2.1. lietotāja apstiprināšana katrā gadījumā, kad personas dati tiek ievadīti datu apstrādes sistēmā, tajā rediģēti vai no tās dzēsti; to iespējams nodrošināt, izmantojot, piemēram, ierakstu sistēmas izveidi, un veicot dokumentu pārvaldību.

3. PIEEJAMĪBA UN NOTURĪBA (GDPR 32. panta pirmās daļas b. punkts)

- 3.1. Pieejamības kontrole:
 - 3.1.1. nejaušas vai plānotas iznīcināšanas vai zudumu novēršana; to iespējams nodrošināt, izmantojot, piemēram, datu kopiju saglabāšanas stratēģijas (tiešsaistes un vietējās kopijas, datu uzglabāšana uzņēmuma adresē un citur), nepārtrauktu elektrības padevi (UPS), aizsardzību no vīrusiem, ugunsdzēsības, ziņošanas procedūras un ārkārtas rīcības plānošanu.
- 3.2. Laicīga atjaunošana (GDPR 32. panta pirmās daļas c. punkts).

4. REGULĀRAS TESTĒŠANAS, NOVĒRTĒŠANAS UN PĀRBAUŽU PROCEDŪRAS (GDPR 32. panta pirmās daļas d. punkts un 25. panta pirmā daļa)

- 4.1. datu aizsardzības vadība;
- 4.2. negadījumu reaģēšanas vadība;
- 4.3. datu apstrāde pēc noklusējuma (GDPR 25. panta otrā daļa);
- 4.4. pasūtījuma vai līguma kontrole.
- 4.5. Ņemot vērā GDPR 28. pantu, ALSO neveic trešo personu datu apstrādi bez atbilstošām instrukcijām no KLIENTA; to iespējams nodrošināt, piemēram, izmantojot augsta līmeņa kontroli, kad tiek izvēlēts pakalpojumu sniedzējs, veicot sākotnējās novērtēšanas pienākumus un turpmākās pārbaudes.

Versija	Datums	Vieta	Izmaiņas veica/ Apstiprināja
1.0	23.05.2018	Mārupe	ALSO
2.0	07.03.2019	Mārupe	ALSO