Andmetöötlusleping

Coresteads OÜ | Versioon 0.10 | 19. oktoober 2026

Kliendipõhiselt täidetav mall. Versioon juriidiliseks ja korralduslikuks ülevaatuseks; ei ole allkirjastatud leping. Nurksulgudes väljad ja lisad A-C tuleb täita ning meetmed enne isikuandmete töötlemist kontrollida.

1. Pooled, rollid ja ulatus

1.1 [Kliendi ärinimi], registrikood [kood], aadress [aadress] ("Vastutav töötleja") ja Coresteads OÜ, registrikood 17617785, Varju tee 8, Pirita linnaosa, Tallinn, Eesti ("Volitatud töötleja") sõlmivad käesoleva andmetöötluslepingu ("DPA"). Kontaktid: [kliendi kontakt] ja info@coresteads.com.

1.2 DPA on [kuupäev] sõlmitud teenuste raamlepingu ("Leping") lisa. Kui raamlepingut ei ole, määrab teenuse ulatuse poolte kinnitatud töökirjeldus [viide]. Lahendus tähendab selles kirjeldatud AI-agente, oskusi, alamagentidega töövooge, integratsioone või ajastatud käivitusi.

1.3 Vastutav töötleja määrab eesmärgid ja olulised vahendid ning tagab õigusliku aluse, andmesubjektide teavitamise ja õiguspärased juhised. Coresteads töötleb andmeid kliendi nimel ainult kokkulepitud teenuse osutamiseks. Kui Coresteads määrab ise töötlemise eesmärgid ja vahendid, hinnatakse tema rolli eraldi; veebipäringuid käsitleb eraldi privaatsuspoliitika.

1.4 Töötlemise ese, laad, eesmärk, kestus, isikuandmete liigid ja andmesubjektide kategooriad määratakse lisas A. Kohaldatakse määruse (EL) 2016/679 (IKÜM) mõisteid. Töötlemist ei alustata enne lisade ja vajalike teenusepakkujate kinnitamist.

2. Juhised ja põhilised kohustused

2.1 Dokumenteeritud juhised on DPA, Leping, töökirjeldus ja hilisemad kirjalikud juhised, sealhulgas juhised EMP-välisteks edastusteks. Õigusaktist tulenevast muust töötlemisest teavitab Coresteads enne töötlemist, kui õigus seda ei keela. Õigusvastasena näivast juhisest teavitatakse viivitamata ning vaidlusalust toimingut ei tehta enne selgitust.

2.2 Andmetele pääsevad ligi ainult volitatud ja konfidentsiaalsuskohustusega seotud isikud. Coresteads rakendab lisa C meetmeid, piirab ligipääsu ja andmehulka ning ei kasuta kliendi isikuandmeid oma eesmärkidel ega oma AI-mudelite treenimiseks.

2.3 Mudeliteenust võib kasutada ainult dokumenteeritud juhise alusel kontrollitud äritingimuste ja seadistustega, mis välistavad kliendi sisu kasutamise üldmudeli treenimiseks ilma kliendi eraldi kirjaliku juhiseta. Enne kasutamist hinnatakse eraldi säilitamist, turvakontrolli ja võimalikke tagasiside- või kuritarvituste seire erandeid. Treenimiskeeld ei tähenda andmete mittesäilitamist.

3. Abi, alamtöötlejad ja edastused

3.1 Coresteads aitab mõistlikult täita andmesubjektide õigusi ning IKÜM artiklite 32-36 kohustusi, arvestades töötlemise laadi ja talle kättesaadavat teavet. Otse saadud taotlus edastatakse kliendile põhjendamatu viivituseta, hiljemalt viie tööpäevaga; vastust kliendi nimel ei anta ilma juhiseta, kui seadus ei nõua teisiti. Coresteads peab nõutavat töötlemistoimingute registrit.

3.2 Üldine kirjalik luba hõlmab üksnes lisas B täpselt nimetatud alamtöötlejaid. Lisamisest või asendamisest teatatakse vähemalt 14 kalendripäeva ette. Klient võib selle aja jooksul põhjendatud andmekaitselisel alusel vastu vaielda; vaidlusalusele uuele töötlejale andmeid enne lahendust ei anta. Kokkuleppe puudumisel võib klient mõjutatud töökirjelduse leppetrahvita lõpetada.

3.3 Coresteads paneb alamtöötlejale kirjalikult sisuliselt samad andmekaitsekohustused ja jääb tema kohustuste täitmise eest kliendi ees vastutavaks. Kliendi enda lepinguline teenusepakkuja ei muutu üksnes Coresteadsi seadistustöö tõttu tema alamtöötlejaks; tegelik roll, lepingupool ja juhiste ahel dokumenteeritakse lisas B.

3.4 Väljapoole Euroopa Majanduspiirkonda edastamine, sh asjakohane kaugjuurdepääs, eeldab kliendi juhist ja IKÜM V peatüki alust. Standardsed andmekaitseklauslid valitakse tegelike rollide järgi; vajadusel hinnatakse edastuse mõju ja rakendatakse lisameetmeid. Piisavusotsusele võib tugineda ainult selle kehtivuse ja vastuvõtja hõlmatuse ulatuses. Kliendi konto või ELi andmebaas ei tõenda kogu andmeahela jäämist EMPsse.

4. Turvalisus, rikkumised ja audit

4.1 Lisa C meetmed peavad olema riskile vastavad ning enne töötlemist rakendatud. Neid võib ajakohastada kaitsetaset vähendamata. Muutunud riskist või olulisest kaitsepuudusest teavitatakse klienti ja lepitakse kokku parandused.

4.2 Coresteads teatab kliendi andmeid puudutavast isikuandmetega seotud rikkumisest põhjendamatu viivituseta, igal juhul hiljemalt 48 tunni jooksul teadasaamisest. 48 tundi on lepinguline ülempiir, mitte õigus teavitamist edasi lükata. Esmane teade ei oota täielikku uurimist: selles antakse teadaolev kirjeldus, mõjutatud andmed ja isikud, tõenäolised tagajärjed, kontakt ning võetud või kavandatud meetmed; teavet täiendatakse viivituseta.

4.3 Klient otsustab järelevalveasutuse ja andmesubjektide teavitamise ning vastutab oma seaduslike tähtaegade eest. Coresteads säilitab asjakohase tõendi ja aitab teadete ning rikkumise lahendamisega.

4.4 Coresteads annab vastavuse tõendamiseks vajaliku teabe ning võimaldab kliendi või tema määratud sõltumatu audiitori auditeid, sealhulgas kontrolle. Tavakontrolli planeeritakse üldjuhul kord aastas 30-päevase etteteatamisega; see ei piira põhjendatud lisakontrolli, rikkumisjärgset kiiret kontrolli ega järelevalveasutuse õigusi. Kulud ja konfidentsiaalsus lepitakse mõistlikult kokku, tegemata seaduslikku kontrolli võimatuks.

5. Lõpetamine, vastutus ja allkirjad

5.1 Teenuse lõppemisel tagastab või kustutab Coresteads kliendi valikul isikuandmed ja olemasolevad koopiad üldjuhul 30 kalendripäevaga, kui lisas A ei ole kokku lepitud lühemat tähtaega. Tagastamine toimub levinud masinloetavas vormingus; pärast tagastamist kustutatakse allesjäänud koopiad. Täitmine kinnitatakse kirjalikult.

5.2 Kui seadus kohustab andmeid säilitama, dokumenteeritakse alus ja tähtaeg, piiratakse töötlemist ning kustutatakse andmed kohustuse lõppedes. Varukoopiate kustutustsükkel ja ligipääsupiirangud määratakse enne töötlemist lisas A; varukoopiaid ei või säilitada tähtajatult ega võtta tavakasutusse. Taastamisel rakendatakse kustutamisjuhised uuesti.

5.3 Vastutuse jaotus järgib Lepingut, piiramata IKÜMist tulenevaid andmesubjektide või asutuste õigusi. Isikuandmete töötlemist puudutava vastuolu korral on DPA ülimuslik; kohustuslik õigus ja kohaldatavad standardsed andmekaitseklauslid jäävad ülimuslikuks. Kohaldatakse Eesti õigust.

5.4 ET- ja EN-mall on sisult paralleelsed. Kahekeelse allkirjastamise korral lepivad pooled kokku ülimusliku keele: [ET / EN]. DPA ei ole iseenesest nõusolek uueks töötlemise eesmärgiks.

Allkirjad

Vastutav töötleja: [ärinimi, nimi, amet, kuupäev, allkiri]

Volitatud töötleja: Coresteads OÜ; [esindaja nimi, esindusõigus, kuupäev, allkiri]

Lisa A. Töötlemise kirjeldus - täita enne algust

Töökirjeldus ja eesmärk: [viide; konkreetne äriprotsess ja lubatud tulemus].

Laad ja sagedus: [lugemine, liigitamine, väljavõte, mustandi koostamine, edastamine, kustutamine; pidev / projekti ajal / ajastatud].

Andmesubjektid ja andmeliigid: [täpsed kategooriad ja väljad; allikad ning süsteemid]. Eriliigilised ja süüteoandmed on välistatud, kui siin ei ole eraldi õiguslikku alust ja kaitset kokku lepitud.

Kestus ja tähtajad: [algus/lõpp; töökoopiate ja logide eesmärk ning tähtaeg; varukoopiate kustutustsükkel]. Logide kavandatav ülempiir on 90 päeva, kui põhjendatud lühemat tähtaega või muud kohaldatavat nõuet ei ole siin kinnitatud. See on lepinguline nõue, mitte tõend olemasolevast seadistusest.

Andmevoog ja kinnitused: [allikas -> tööriist -> mudeliteenus -> väljund; asukohad ja kaugjuurdepääs; inimese kinnitust nõudvad toimingud; kliendi ja Coresteadsi vastutajad].

Lisa B. Teenusepakkujate register - täita iga projekti jaoks

Ükski teenusepakkuja ei ole selle tühja malli alusel automaatselt heaks kiidetud. Lisage iga tegelikult kasutatav alamtöötleja eraldi kirjena ning kliendi otse hangitud teenused eraldi rollimärkega.

Iga kirje peab sisaldama: [täpne juriidiline nimi ja kontakt]; [teenus ja töödeldavad andmed]; [Coresteadsi alamtöötleja / kliendi otsetöötleja]; [lepingu ja DPA viide]; [andmete asukohad ja kaugjuurdepääsu riigid]; [edastuse alus, SCC moodul ja vajadusel mõjuanalüüs]; [säilitamine, kustutamine ja treeningukasutuse seadistus]; [kinnitaja ja kuupäev].

Vajaduse järgi kontrollitavad teenused võivad olla Anthropic Claude API, Google Workspace või muu e-posti/dokumenditeenus, töövoo majutaja ja muud integratsioonid. See on näidete loend, mitte luba neid kasutada. Tootenimi ei asenda lepingupoole juriidilist nime.

Coresteadsi avaliku veebivormi Firebase/Firestore/Resend ahelat ei loeta automaatselt kliendiprojekti andmeahelaks. Kui samu teenuseid kasutatakse kliendi nimel, tuleb need siin eraldi hinnata ja nimetada.

Lisa C. Tehnilised ja korralduslikud nõuded

Meetmed on lepingu nõuded. Vastutaja, rakenduse tõend ja erandid dokumenteeritakse enne töötlemist; rakendamata meedet ei tohi kirjeldada olemasoleva kaitsena.

1. Ligipääs ja saladused. Nimelised kontod, minimaalsed õigused, MFA toetatud halduskontodel, ligipääsude ülevaatus ning viivitamatu eemaldamine vajaduse lõppedes. Saladused hoitakse selleks mõeldud hoidlas või paroolihalduris; neid ei lisata lähtekoodi, avalikesse promptidesse ega e-kirjadesse.

2. Eraldatus ja krüpteerimine. Kliendi andmed, konfiguratsioon ja ligipääsutunnused eraldatakse. Kasutatakse TLS-i; säilitatavate andmete ja tööseadmete krüpteerimine ning teenusepakkuja rakendus kontrollitakse. Seadmetel on ekraanilukk, turvauuendused ja riskile vastav kaitse.

3. Minimeerimine ja AI. Arenduses kasutatakse võimalusel sünteetilisi või anonüümseid andmeid; pseudonüümitud andmed on endiselt isikuandmed. Tööriistu ja andmeallikaid piiratakse; mudeli väljund ei ole usaldatud käsk. Kõrge mõjuga saatmised, maksed, õiguste või lepingute muudatused nõuavad kokkulepitud inimese kinnitust.

4. Logid, taastamine ja kustutamine. Logitakse vajalikud toimingud, vead, kinnitused ja kasutus; täielikku sisu ja saladusi välditakse. Säilitamine järgib lisa A. Riskist sõltuv varundus, taastamise kontroll ja käideldavuse meetmed määratakse ning testitakse enne tootmiskasutust.

5. Testid ja intsidendid. Enne üleandmist ja olulise muudatuse järel tehakse kokkulepitud kontrollid, sh ligipääsu- ja piirangutestid. Dokumenteeritakse intsidendi kontakt, avastamine, piiramine, tõendite kaitse, teavitamine ja järelparandused. Kontrollide tõhusust hinnatakse regulaarselt riskile vastavalt.