Turvalisuse ülevaade

Coresteads OÜ | Versioon 0.10 | 19. oktoober 2026

Kliendiprojekti kontrollide lähtekoht. Täpsed meetmed ja rakenduse tõend kinnitatakse DPA-s ning töökirjelduses enne töötlemist. See ülevaade ei ole audit ega vastavussertifikaat.

Coresteads ehitab AI-agente, oskusi, alamagentidega töövooge ja ajastatud käivitusi. Eesmärk on anda teie meeskonnale kontroll andmete, ligipääsude ja oluliste otsuste üle.

Andmevoog ja rollid	Võimalusel teie kontodel. Ka seal võivad andmed liikuda mudeli API-le ja teistele lubatud pakkujatele. DPA määrab rollid ja alamtöötlejad; kliendi otselepingulised teenused märgitakse eraldi.
Ligipääs ja saladused	Nimelised kontod, minimaalsed õigused, toetatud halduskontodel MFA, ligipääsu eemaldamine vajaduse lõppedes. Võtmed ja paroolid hoitakse saladuste hoidlas või paroolihalduris.
Andmekaitse	TLS, kontrollitud säilitus- ja seadmekrüpteerimine, kliendi andmete eraldamine ning võimalusel sünteetilised või anonüümsed testandmed. Rakendamine kontrollitakse projektis.
AI ja inimese kontroll	Coresteads ei treeni oma mudeleid kliendi andmetel. Teenusepakkuja treeningukasutus, säilitamine ja erandid kontrollitakse eraldi. Kõrge mõjuga toimingud vajavad kokkulepitud inimese kinnitust.
Säilitamine ja lahkumine	DPA lisa A määrab töökoopiate, logide ja varukoopiate tähtajad. Malli logide ülempiir on 90 päeva; lühem tähtaeg valitakse võimalusel. Lõpus andmed tagastatakse või kustutatakse üldjuhul 30 päevaga.
Testimine ja jälgitavus	Kokkulepitud kontrollid enne üleandmist ja oluliste muudatuste järel. Avalik metoodika: ülevaatus vähemalt 8/10, käivitustäpsus 85%, käitumistestid 80% ja blokeerivaid vigu pole. Need ei ole töökindluse garantii.
Intsidendid	DPA nõue on teavitada põhjendamatu viivituseta, hiljemalt 48 tunniga teadasaamisest. Teavet täiendatakse ja klienti abistatakse; kliendi seaduslik teavitamistähtaeg on eraldi kohustus.

Enne kasutust kinnitatakse vastutajad, tõendid, andmevoog, edastuse alus ja taastamine. Regulaarne hooldus, eelarvepiirid ning lisakontrollid lepitakse eraldi kokku. IKÜM-i ja AI määruse kohustusi hinnatakse lahenduse rolli ja riski järgi; asjakohased AI-suhtluse teavitused lisatakse. Kindlustust ega sertifikaati siin ei kinnitata.

Veebipäring on eraldi: Firebase Hosting -> Firestore (eur3) -> Trigger Email (europe-west1) -> Resend -> postkast. Google Analytics laaditakse nõusolekul. Täpsemalt: coresteads.com/et/privacy.

info@coresteads.com