Tietojenkäsittelysopimus (DPA)

Edudata.io (3460068-8) — Cloudpoint Oy (Y-tunnus 2325703-6, ALV-tunnus FI23257036) • Malminkaari 17–19 B, 00700 Helsinki, Suomi • DPO: tietosuoja@cloudpoint.fi

[VIRALLINEN JULKAISTU · H-AI-H] Ihmisen vahvistama virallinen kieliversio (H-AI-H Human–AI–Human -prosessi; tulkintaristiriidoissa EN-pääversio on ensisijainen).
Verification Role: LEGAL_COUNSEL_AND_RELEASE_OWNER | **Verified UTC:** 2026-11-25T08:36:41Z

Asiakirjatunnus	`edudata.dpa.fi.v2.0.0-r01`	**Versio**	**v2.0** (`v2.0.0-r01`)
Voimassaolo	2026-11-10	**Seuraava katselmus**	2027-11-10
Kieli	Suomi (fi-FI)	**Tietoturvasertifiointi**	ISO/IEC 27001:2022 (#123522, Prescient Security LLC)
Laadintaprosessi	**H-AI-H (Human–AI–Human)**	**Kielirooli / Pääversio**	Lokalisoitu käännös (EN-pääversiosta)
Kanoninen verkko-osoite	`https://www.edudata.io/fi/trust-center#dpa`		
Sisällön SHA-256 (UTF-8 NFC)	`7747efbbbda4e38fd3d020387fe19277bdccef590dd81315269515fbacfdddf0`		

Oikeudellisesti sitova tietojenkäsittelysopimus, joka säätelee henkilötietojen käsittelyä Edudata.io-alustan rekisterinpitäjän ja käsittelijän välillä.

EDUDATA.IO TIETOJENKÄSITTELYSOPIMUS

Tämä lokalisoitu versio on tekoälyavusteinen käännös
alkuperäisestä englanninkielisestä versiosta
, ja se on tarkoitettu ainoastaan tiedoksi ja viitteeksi. Ristiriitatilanteissa englanninkielinen versio on ensisijainen.

Versio 2.0 | Voimassaolo: 10.11.2026 alkaen

Tämä tietojenkäsittelysopimus ("DPA", Versio 2.0) koskee EDUDATA-palvelua ("Palvelu"), jonka tarjoaa Cloudpoint Oy. Sopimus täydentää pääsopimusta (mukaan lukien käyttöehdot) ja muodostaa sen kiinteän osan. Ristiriitatilanteissa tämän DPA:n ehdot ovat ensisijaisia henkilötietojen käsittelyn osalta.

Sopijapuolet:

Henkilötietojen käsittelijä: Cloudpoint Oy (2325703-6) / Edudata.io (3460068-8), joka on osa Cloudpoint Oy:tä (2325703-6, ALV-tunnus FI23257036), Malminkaari 17-19B, 00700 Helsinki, Suomi (Tietosuojavastaava / DPO: Jasse Tenko, tietosuoja@cloudpoint.fi, ISM-johtaja: Hesham Abboud, asiakaspalvelu: info@edudata.io, puh. +358 9 4257 9280)
Rekisterinpitäjä: Asiakas (Kunta / Koulutuksen järjestäjä)

1. Määritelmät

- **Rekisterinpitäjä:** Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot (GDPR 4 artiklan 7 kohta).
- **Henkilötietojen käsittelijä (Käsittelijä):** Luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (GDPR 4 artiklan 8 kohta).
- **GDPR:** Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (yleinen tietosuoja-asetus).

- **Henkilötiedot:** Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (GDPR 4 artiklan 1 kohta).
- **Käsittely:** Kaikki sellaiset toimenpiteet tai toimenpidesarjat, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin, joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti.

Muilla tässä käsittelysopimuksessa (DPA) määrittelemättömillä termeillä on sama merkitys kuin GDPR:ssä.

2. Tausta ja tarkoitus

Rekisterinpitäjä on valinnut Palveluntarjoajan (Cloudpoint Oy) toimimaan henkilötietojen käsittelijänä EU:n yleisen tietosuoja-asetuksen (GDPR) artiklan 28(3) mukaisesti.

Tämä DPA on kiinteä osa Osapuolten välillä solmittua Pääsopimusta, jonka nojalla Käsittelijä toimittaa Rekisterinpitäjälle Edudata-palvelun (ensisijaisesti *Edudata Compliance* ja *Edudata Compliance Service* sekä erikseen tilattaessa valinnaiset moduulit *Edudata Privacy* ja *Edudata Security*), ellei Pääsopimuksessa ole toisin sovittu.

Käsittelijä käsittelee tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja Rekisterinpitäjän lukuun. Yksityiskohtaiset käsittelytoimet on kuvattu tämän sopimuksen Liitteessä 1 (Versio 2.0 — 10.11.2026).

Tämän sopimuksen tarkoituksena on sopia osapuolten oikeuksista ja velvollisuuksista henkilötietojen käsittelyssä GDPR:n vaatimusten mukaisesti ja turvata rekisteröidyn oikeudet ja vapaudet käsittelyn aikana.

3. Roolit ja vastuut

Käsittelijä käsittelee henkilötietoja ainoastaan tämän DPA:n ja Rekisterinpitäjän kirjallisten ja dokumentoitujen ohjeiden mukaisesti. Käsittelijä sitoutuu olemaan käyttämättä henkilötietoja mihinkään muihin tarkoituksiin kuin tässä DPA:ssa ja Rekisterinpitäjän ohjeissa on sovittu. Rekisterinpitäjän ohjeiden tulee olla sovellettavan tietosuojalainsäädännön ja tämän DPA:n mukaisia.

Jos Käsittelijä huomaa, että jokin Rekisterinpitäjän antama ohje on sovellettavan lain vastainen tai puutteellinen, Käsittelijä ilmoittaa tästä Rekisterinpitäjälle viipymättä.

Rekisterinpitäjä vastaa laillisen käsittelyperusteen olemassaolosta, rekisteröityjen informoinnista henkilötietojen käsittelystä sekä muista GDPR:n mukaisista rekisterinpitäjän velvoitteista.

Rekisterinpitäjä on velvollinen ilmoittamaan Käsittelijälle tietosuojavastaavansa (DPO) ja nimetyn yhteyshenkilönsä yhteystiedot ja varmistamaan, että yhteystiedot pidetään ajan tasalla. Yhteystiedot ovat välttämättömiä, jotta Käsittelijä voi täyttää suorat kirjalliset ilmoitusvelvollisuutensa alikäsittelijämuutoksissa, sopimusmuutoksissa ja mahdollisessa tietoturvaloukkaustilanteessa.

4. Tekniset ja organisatoriset turvatoimet

Käsittelijä toteuttaa ja ylläpitää asianmukaisia teknisiä ja organisatorisia turvatoimia (GDPR 32 artikla ja Cloudpoint Oy:n ISO/IEC 27001:2022 -sertifioitu tietoturvan hallintajärjestelmä) suojatakseen henkilötietoja luvattomalta tai lainvastaiselta käsittelyltä ja pääsyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Turvatoimia valitessaan Käsittelijän on otettava huomioon uusin tekniikka, toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Yksityiskohtainen kuvaus käytetyistä suojatoimista on esitetty tämän DPA:n Liitteessä 2 (Versio 2.0 — 10.11.2026).

5. Avustamisvelvollisuus ja rekisteröityjen pyyntöjen (DSAR) vasteaika

Käsittelijä käsittelee henkilötietoja tämän DPA:n, Rekisterinpitäjän ohjeiden ja tietosuojalainsäädännön mukaisesti. Käsittelijä sitoutuu varmistamaan, että sen lukuun työskentelevät henkilöt noudattavat tämän DPA:n ehtoja ja ovat tietoisia asiaankuuluvasta lainsäädännöstä. Käsittelijä tukee Rekisterinpitäjää GDPR:n 28 ja 32–36 artiklojen mukaisten velvollisuuksien täyttämisessä (mukaan lukien tietosuojavaikutusten arvioinnit [DPIA], ennakkokuulemiset ja rekisteröityjen oikeuksien toteuttaminen).

Ei lisäkustannuksia lakisääteisestä avustamisesta: Kaikki GDPR 28 artiklan ja 32–36 artiklojen mukainen tavanomainen avustaminen sisältyy Palvelun tilausmaksuun ilman erillistä korvausta. Vain sellaisista Asiakkaan nimenomaisesti tilaamista räätälöidyistä kehitys- tai integraatiotöistä, jotka ylittävät GDPR:n lakisääteiset vaatimukset, sovitaan kirjallisesti etukäteen.

Viiden (5) arkipäivän vasteaika (DSAR SLA): Käsittelijä ilmoittaa Rekisterinpitäjälle ilman aiheetonta viivytystä ja **viimeistään viiden (5) arkipäivän kuluessa** kaikista vastaanottamistaan rekisteröityjen pyynnöistä (DSAR) sekä toimittaa pyynnön täyttämiseen tarvittavan teknisen avun ja tietojen viennin viimeistään 5 arkipäivän kuluessa Rekisterinpitäjän pyynnöstä.

6. Kansainväliset tiedonsiirrot, HubSpot EU1 -hallinta ja ohjelmistokehityksen eriyttäminen

Käsittelemme kaikkia Palvelun tuotannollisia henkilötietoja ja tietokantoja yksinomaan Euroopan unionin ja Euroopan talousalueen (EU/ETA) sisällä sijaitsevissa Google Cloud -palvelinkeskuksissa (ensisijaisesti `europe-north1` Hamina, Suomi sekä EU-monialue). Tuotantotietoja ei siirretä säännöllisesti EU/ETA-alueen ulkopuolelle.

HubSpot Ireland Ltd (EU1 Frankfurt -tietojen sijainti ja 5 kategorian tukitikettikielto): Asiakaspalvelun tukitiketti- ja yhteystietojen hallintaan käytettävä HubSpot-järjestelmä on lukittu EU-palvelinkeskukseen (`dataHostingLocation = eu1` , `app-eu1.hubspot.com` , AWS `eu-central-1` Frankfurt, Saksa; varajärjestelmä Dublin, Irlanti). HubSpotissa on pakotettuna GDPR Compliance Toolkit (mukaan lukien pysyvä GDPR-poisto [*GDPR Permanent Delete*] 90 päivän kuluessa sopimuksen päättymisestä tai pyynnöstä) sekä tekoälyestot (`customer_data_training_enabled = False` , `crm_sensitive_pii_access_enabled = False`). Siltä osin kuin yhdysvaltalaisella emoyhtiöllä (HubSpot, Inc.) on teoreettinen alikäsittelijärooli, siirto on suojattu EU–US Data Privacy Framework (DPF) -sertifioinnilla, EU:n mallisopimuslausekkeilla (SCC 2021/914) ja siirtojen vaikutustenarvioinnilla (TIA). Lisäksi Cloudpointin tietojen käsittelypolitiikka (*Data Management Policy v1.1.0*) kieltää ehdottomasti viiden (5) tietokategorian syöttämisen tai siirtämisen HubSpot-tukitiketteihin: (1) oppilas- ja opiskelijatiedot, (2) erityiset henkilötietoryhmät (arkaluonteiset tiedot), (3) tietoturvapoikkeamien yksityiskohdat, (4) tunnistautumistunnukset ja salaisuudet sekä (5) tietoturvalokit.

Ohjelmistokehityksen tekninen eriyttäminen (Aimpulse, Egypti — GDPR 25 ja 32 artikla): **Aimpulse** on Cloudpoint Oy:n dedikoitu tuotekehitysyksikkö / kumppaniyhtiö (Kairo, Egypti), joka toimii yksinomaan Cloudpoint Oy:n operatiivisessa määräysvallassa ja ISO/IEC 27001:2022 -sertifioidun ISMS-hallintajärjestelmän alaisuudessa. Egyptissä työskentelevät ohjelmistokehittäjät osallistuvat aktiivisesti Edudata.io-ohjelmistokoodin kehittämiseen **yksinomaan eristetyissä kehitys- ja testiympäristöissä (`edudata-compliance-staging`) käyttäen 100 % synteettistä testiaineistoa** (*Test Data & Production Data Separation Policy CP-ISMS-DLP-001 v1.2*), eikä heillä ole **lainkaan pääsyä operatiiviseen asiakasdataan tai henkilötietoihin tuotantoympäristössä (`edudata-compliance-prod`)**. Asiakastuki ja tuotannollisten henkilötietojen ylläpito suoritetaan yksinomaan EU/ETA-alueella (Suomi). Sopimussuhde on katettu EU:n vakiosopimuslausekkeilla (SCC, päätös (EU) 2021/914, Module 3: käsittelijästä käsittelijään), dokumentoidulla siirtojen vaikutustenarvioinnilla (TIA) sekä muuttumattomalla 400 päivän tarkastuslokituksella.

7. Salassapitovelvollisuus

Käsittelijän ja kaikkien sen lukuun työskentelevien luonnollisten henkilöiden on noudatettava luottamuksellisuutta ja salassapitovelvollisuutta henkilötietojen käsittelyn aikana. Käsittelijä varmistaa, että kaikki sen lukuun työskentelevät luonnolliset henkilöt ovat sitoutuneet salassapitosopimukseen.

Käsittelijä varmistaa, että sen alihankkijoiden kanssa on voimassa salassapitosopimus (NDA) ja että alihankkijan ja kaikkien sen lukuun käsittelyyn osallistuvien luonnollisten henkilöiden välillä on voimassa salassapitosopimus. Salassapitovelvollisuus säilyy voimassa myös Pääsopimuksen ja tämän käsittelysopimuksen päättymisen jälkeen.

8. Auditointioikeus

Rekisterinpitäjällä on oikeus kohtuullisessa määrin auditoida Käsittelijän tiloja ja käsittelytoimia tarkastaakseen tämän DPA:n mukaisen suojan ja tietoturvan tason sekä arvioidakseen Käsittelijän vaatimustenmukaisuutta tämän DPA:n ehtojen kanssa. Käsittelijä toimittaa Rekisterinpitäjälle pyynnöstä ajantasaisen ISO/IEC 27001:2022 -auditointidokumentaation (Prescient Security) ja auditointiyhteenvedot.

Kumpikin osapuoli vastaa omista auditointikustannuksistaan (tai kuten Pääsopimuksessa on sovittu). Rekisterinpitäjän on ilmoitettava auditoinnista Käsittelijälle kirjallisesti vähintään 30 arkipäivää (tai kunta- ja julkishallinnon JIT-sopimuksissa vähintään 14–30 päivää) ennen auditoinnin suorittamista.

Rekisterinpitäjän auditointioikeutta voidaan käyttää enintään kerran kahdessatoista (12) kuukaudessa, ellei yksilöity tietoturvaloukkaus, valvontaviranomaisen määräys tai perusteltu huoli edellytä aikaisempaa auditointia.

Mikäli auditointi saattaa johtaa Käsittelijän liike- tai yrityssalaisuuksien paljastumiseen tai vaarantaa Käsittelijän immateriaalioikeudet, auditoinnin suorittamiseen on käytettävä riippumatonta asiantuntijaa, joka ei ole Käsittelijän kilpailija ja jonka on sitouduttava salassapitosopimukseen.

9. Alihankkijat (Alikäsittelijät)

Käsittelijällä on oikeus käyttää alihankkijoita (alikäsittelijöitä) henkilötietojen käsittelyssä Palvelun tarjoamisen yhteydessä edellyttäen, että tämä ei johda Käsittelijän tämän DPA:n mukaisten velvoitteiden rikkomiseen. Hyväksytyt alikäsittelijät on yksilöity Liitteessä 1.

Käsittelijä varmistaa, että käytetyt alihankkijat toimivat kirjallisen tietojenkäsittelysopimuksen (GDPR 28 artiklan 4 kohta) alaisina ja noudattavat vähintään yhtä tiukkoja tietosuoja- ja tietoturvavelvoitteita kuin mitä tässä sopimuksessa on määrätty. Käsittelijä vastaa alikäsittelijöidensä toiminnasta kuin omastaan.

Suora kirjallinen ennakkoilmoitus (vähintään 30 kalenteripäivää): Käsittelijä ilmoittaa Rekisterinpitäjän nimetylle yhteyshenkilölle suoraan kirjallisesti (sähköpostitse) **vähintään kolmekymmentä (30) kalenteripäivää etukäteen** ennen uuden alikäsittelijän käyttöönottoa tai olemassa olevan alikäsittelijän vaihtamista. Rekisterinpitäjällä on kolmekymmentä (30) kalenteripäivää aikaa ilmoituksen vastaanottamisesta vastustaa muutosta kirjallisesti perustellusta tietosuojasyystä. Mikäli osapuolet eivät löydä ratkaisua 30 kalenteripäivän neuvotteluajan kuluessa, Rekisterinpitäjällä on oikeus irtisanoa Palvelu ilman irtisanomisseuraamuksia.

10. Tietoturvaloukkaukset (Kaksivaiheinen 24/7-valvonta ja NIS2 / GDPR 33 artiklan ilmoitusmalli)

Käsittelijä noudattaa dokumentoitua poikkeamienhallintamenettelyä (*Security Incident Management Procedure CP-ISMS-IR-002 v1.0* sekä VPM-38 4-portaista vasteaikamallia: P1 < 1 h, P2 < 4 h, P3 < 24 h, P4 < 72 h) ja ilmoittaa Rekisterinpitäjälle henkilötietojen tietoturvaloukkauksista kaksivaiheisesti:

- **Vaihe 1 — Automaattinen 24/7/365-valvonta ja alustava ennakkovaroitus (≤ 24 tuntia):** Tuotantoinfrastruktuuria (`edudata-compliance-prod`) valvotaan ympäri vuorokauden 24/7/365 (mukaan lukien viikonloput ja arkipyhät) automaattisilla tietoturva- ja poikkeamahälytyksillä. Saatuaan tiedon todetusta tai perustellusti epäillystä henkilötietojen tietoturvaloukkauksesta Käsittelijä lähettää Rekisterinpitäjän nimetylle yhteyshenkilölle kirjallisen tai automaattisen **alustavan ennakkovaroituksen (Early Warning) viimeistään 24 tunnin kuluessa** havainnosta (sisältäen havaintoajan, kohdejärjestelmän, käynnistetyt tekniset rajoittamistoimet ja yhteyshenkilön).
- **Vaihe 2 — Tietosuojavastaavan (DPO) arviointi ja yksityiskohtainen 8-kohtainen raportti (seuraavana arkipäivänä / ≤ 72 tuntia):** Asiantuntijoiden suorittama juurisyyanalyysi ja tietosuojavastaavan (DPO Jasse Tenko / ISM-johtaja Hesham Abboud, `tietosuoja@cloudpoint.fi`) vaikutustenarviointi suoritetaan virka-aikana ja toimitetaan Rekisterinpitäjälle **seuraavana arkipäivänä** (ja aina GDPR 33 artiklan mukaisen 72 tunnin enimmäismääräajan puitteissa). Raportti sisältää kaikki kahdeksan (8) pakollista tietopistettä:
  1. Tietoturvaloukkauksen tapahtuma- ja havaintoajankohta (aikaleimat);
  2. Kuvaus loukkauksen luonteesta sekä kohdejärjestelmistä ja -tiedoista;
  3. Asianomaisten rekisteröityjen ryhmät ja arvioitu lukumäärä sekä henkilötietietueiden ryhmät ja arvioitu lukumäärä;
  4. Mahdolliset alikäsittelijät tai kolmannet maat, joita poikkeama koskee;
  5. Kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista;
  6. Kuvaus välittömistä teknisistä rajoittamis- ja korjaustoimenpiteistä sekä toimenpiteistä haittavaikutusten lieventämiseksi;
  7. Tietosuojavastaavan (DPO) ja tietoturvavastaavan (ISM) suorat yhteystiedot (`tietosuoja@cloudpoint.fi`, puh. +358 9 4257 9280);
  8. Aikataulu seuraavalle tilanneraportille ja lopulliselle juurisyyanalyysille (RCA).

11. Henkilötietojen palauttaminen ja poistaminen (30 päivää ensisijainen data / 90 päivää varmuuskopiot)

Ennen sopimuksen päättymistä Rekisterinpitäjällä on oikeus viedä (export) kaikki kunnan arvioinnit, päätökset, metatiedot ja tarkastuslokit rakenteisessa ja yleisesti käytetyssä koneluettavassa muodossa (JSON/CSV/PDF).

Tämän DPA:n ja Pääsopimuksen päätyttyä Käsittelijä poistaa henkilötiedot seuraavien sitovien enimmäismääräaikojen mukaisesti, ellei pakottava EU:n tai jäsenvaltion lainsäädäntö velvoita säilyttämään tietoja:

- **Ensisijaiset tuotantotiedot (enintään 30 päivää):** Kaikki aktiiviset asiakas- ja henkilötiedot poistetaan tuotantotietokannoista (Cloud SQL `edudata-comp-db`, `edudata-ai-db` ja Firestore) **viimeistään kolmenkymmenen (30) päivän kuluessa** sopimuksen päättymisestä.
- **Varmuuskopiot (enintään 90 päivää ensisijaisesta poistosta):** Kaikki salatut varmuuskopiot (Cloud SQL `edudata-comp-db` 21 päivän automaattiset varmuuskopiot + 7 päivän PITR-loki, `edudata-ai-db` 7 päivän varmuuskopiot + 7 päivän PITR-loki, Firestore 7–90 päivän palautuspisteet sekä Cloud Storage 7 päivän soft-delete `604800s`) poistetaan ja ylikirjoitetaan peruuttamattomasti **viimeistään yhdeksänkymmenen (90) päivän kuluessa** ensisijaisesta poistosta (yhteensä enintään 120 päivää sopimuksen päättymisestä). Muuttumattomat tietoturva- ja tarkastuslokit (`_Required` 400 päivää / `_Default` 365 päivää), jotka eivät sisällä asiakkaan sisältödataa, poistuvat automaattisesti kiinteän säilytysaikansa päättyessä.
- **Poistokuittaus pyydettäessä ja suojaus poistoikkunan aikana:** Koko poisto- ja varmuuskopioiden kiertokulun ajan tietoja suojataan AES-256-salauksella ja tiukalla käyttökielolla. Toimittaja toimittaa Asiakkaalle pyydettäessä kirjallisen poistokuittauksen (esim. sähköpostitse), kun poistaminen on suoritettu.

Lisäksi passiiviset käyttäjätilit poistetaan käyttäjätietokannasta automaattisesti, kun 366 päivää on kulunut viimeisimmästä kirjautumisesta.

12. Tekoälyavusteinen käsittely (Vertex AI / Gemini & Document AI) ja vastuunrajoitus

Tekoälykäsittelyn rajoitukset (EU/ETA-lukitus ja koulutuskielto): Siltä osin kuin Rekisterinpitäjä hyödyntää Palvelun valinnaisia tekoälyavusteisia toimintoja (kuten tietosuojadokumenttien, sopimusten tai DPIA-arviointien alustavaa analysointia), käsittely suoritetaan yksinomaan **Google Cloud Vertex AI (Gemini Enterprise -mallit)** ja **Google Cloud Document AI** -palveluilla EU/ETA-alueella (`europe-north1` Suomi ja `eu` -monialue, tietokanta `edudata-ai-db`, poisto 30 päivää / varmuuskopiot 7 päivää). Asiakkaan tietoja, syötteitä (prompts), dokumentteja tai tulosteita **ei koskaan käytetä yleisten tai asiakkaiden välisten tekoälymallien kouluttamiseen, hienosäätöön tai parantamiseen** (*Data Management Policy v1.1.0*). Palvelu ei suorita GDPR 22 artiklan mukaista automaattista päätöksentekoa tai profilointia, vaan toimii aina asiantuntijan päätöksenteon tukena (*Human-in-the-Loop*).

Vastuunrajoitus: Käsittelijä ei vastaa mistään tämän DPA:n alaisista epäsuorista tai välillisistä vahingoista. Käsittelijän enimmäisvastuu Rekisterinpitäjää kohtaan tämän DPA:n perusteella määräytyy Pääsopimuksen mukaisesti (tai mikäli Pääsopimuksessa ei ole toisin sovittu, rajattuna summaan, joka vastaa 100 % Rekisterinpitäjän Käsittelijälle Palvelusta edeltävän 12 kuukauden aikana maksamista maksuista). Käsittelijä ei rajoita vastuutaan siltä osin kuin tällainen vastuunrajoitus olisi pakottavan lainsäädännön tai GDPR 82 artiklan vastainen.

13. Voimassaolo

Tämä DPA (Versio 2.0, voimassa 10.11.2026 alkaen) ja Edudata.io:n Käyttöehdot (Versio 3.1) allekirjoitetaan ja saatetaan voimaan samanaikaisesti joko sähköisesti **Cloudpoint Portalissa (`portal.cloudpoint.fi`)** (käyttäen vahvaa sähköistä tunnistautumista `Bink.fi` FTN / `Swedish BankID` ja muuttumatonta kryptografista `SHA-256` -arkistointia Google Cloud Storage WORM -tallennustilaan alueella `europe-north1`) tai Pääsopimuksen / Tilaussopimuksen ulkoisella sähköisellä allekirjoituksella, joka rekisteröidään `portal.cloudpoint.fi` -portaaliin keskitettyä sopimus-, moduuli- ja tietosuojavastaavan (DPO) yhteystietohallintaa varten. Tämä DPA pysyy voimassa, kunnes Käsittelijä on lopettanut Rekisterinpitäjän henkilötietojen käsittelyn ja suorittanut kohdan 11 mukaiset poistotoimenpiteet, tai kunnes se korvataan toisella Osapuolten välisellä tietojenkäsittelyä koskevalla sopimuksella.

14. Riitojen ratkaiseminen ja lainkäyttöalue

Tähän sopimukseen sovelletaan Pääsopimuksen mukaisia riitojenratkaisu- ja lainkäyttöalueen ehtoja (Helsingin käräjäoikeus ja Suomen laki, ellei kunnan kanssa solmitussa Pääsopimuksessa ole nimenomaisesti sovittu paikallisesta tuomioistuimesta ja laista).

15. Muutosten hallinta (3-portainen Trust Center- ja DPA-muutosmalli)

Tämän DPA:n ja Trust Center -dokumentaation päivityksiin sovelletaan kolmiportaista muutoshallintamallia:

- **Taso 1 — Ei-olennaiset, selkeyttävät ja tietoturvaa parantavat päivitykset (0 päivän ennakkoilmoitus, kielto heikentää tietosuojaa):** Käsittelijä voi päivittää Trust Center -dokumentaatiota ja teknisiä kuvauksia ilman ennakkoilmoitusta silloin, kun kyse on kielellisistä tai teknisistä täsmennyksistä, uusista tietoturvasertifioinneista (kuten ISO/IEC 27001:2022) tai tietoturvatoimien vahvistamisesta, **edellyttäen, etteivät päivitykset koskaan muuta sovittuja käsittelyn tarkoituksia tai heikennä Palvelun tietoturva- tai tietosuojasitoumuksia (*No Material Degradation Guarantee*)**.
- **Taso 2 — Alikäsittelijämuutokset ja operatiiviset ennakkoilmoitukset (vähintään 30 kalenteripäivän suora kirjallinen ennakkoilmoitus ja vastustusoikeus):** Alikäsittelijöiden lisäyksistä tai vaihdoista (GDPR 28 art. 2 kohta, ks. kohta 9) sekä vastaavista operatiivisista päivityksistä ilmoitetaan kirjallisesti (sähköpostitse) suoraan Rekisterinpitäjän nimetylle yhteyshenkilölle **vähintään kolmekymmentä (30) kalenteripäivää etukäteen**, jolloin Rekisterinpitäjällä on 30 kalenteripäivän oikeus vastustaa muutosta perustellusta tietosuojasyystä.
- **Taso 3 — Olennaiset muutokset henkilötietojen käsittelytapaan ja asiakaskohtaiset Pääsopimuksen muutokset (vähintään 30 kalenteripäivän ennakkoilmoitus + Rekisterinpitäjän nimenomainen sähköinen hyväksyntä):** Käsittelijä ei tee olennaisia muutoksia siihen, miten henkilötietoja käsitellään (kuten käsittelyn tarkoituksiin, henkilötieto- tai rekisteröityryhmiin, tietojen säilytysalueisiin, säilytysaikoihin tai tämän DPA:n ydinsitoumuksiin GDPR 28 art. 3 kohdan mukaisesti) ilman Rekisterinpitäjän hyväksyntää. Tällaiset muutokset toimitetaan vähintään 30 kalenteripäivää etukäteen Rekisterinpitäjän pääkäyttäjän tai päättäjän sähköisesti hyväksyttäväksi **Edudata.io-palvelussa tai Cloudpoint Portalissa (`portal.cloudpoint.fi`) (sisältäen mahdollisuuden välittää hyväksyntäpyyntö suoraan organisaation nimenkirjoitusoikeutetulle henkilölle)**.

Allekirjoitukset

Osapuolet ovat hyväksyneet ja allekirjoittaneet tämän DPA:n (Versio 2.0) sekä Käyttöehdot (Versio 3.1) samanaikaisesti joko sähköisesti **Cloudpoint Portalissa (`portal.cloudpoint.fi`)** (vahvalla sähköisellä tunnistautumisella `Bink.fi` / `Swedish BankID` ja kryptografisella `SHA-256`-tiivisteellä, joka arkistoidaan muuttumattomasti `GCS WORM` -tallennustilaan alueella `europe-north1`) tai Pääsopimuksen / Tilaussopimuksen ulkoisella sähköisellä allekirjoituksella, joka on rekisteröity `portal.cloudpoint.fi`-portaaliin keskitettyä sopimus-, moduuli- ja DPO-yhteystietohallintaa varten.

Cloudpoint Oy / Edudata.io

Tietosuojavastaava (DPO) ja nimenkirjoitusoikeutettu edustaja, Cloudpoint Oy (Käsittelijä)

Versio 2.0 | Päivämäärä: 10.11.2026

[Asiakkaan edustajan allekirjoitus]

Valtuutettu allekirjoittaja (Rekisterinpitäjä)

Päivämäärä: [Pääsopimuksen hyväksymispäivä]

LIITE 1: Käsittelyn kuvaus (Versio 2.0 — 10.11.2026)

1. Henkilötietojen käsittelyn tarkoitukset

Käsittelijä käsittelee henkilötietoja Rekisterinpitäjän lukuun Edudata-palvelun toimittamiseksi, käyttäjien vahvan federoidun tunnistautumisen (SSO) ja roolipohjaisen käyttöoikeushallinnan (RBAC) toteuttamiseksi, digitaalisten oppimisympäristöjen ja järjestelmien tietosuoja- ja riskiarviointien (DPIA) hallinnoimiseksi

sekä tietoturvallisuuden ja auditointiketjujen ylläpitämiseksi Pääsopimuksen, tämän DPA:n ja Rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti.

2. Rekisteröityjen ryhmät ja moduulikohtainen rajaus

Henkilötietojen käsittely jakautuu asiakkaan tilaamien Palvelun moduulien mukaisesti seuraavasti:

- **Kunnan henkilöstö ja hallinnon käyttäjät (*Edudata Compliance* & *Edudata Compliance Service* — ydinalusta):** Kunnan hallintohenkilöstö, rehtorit, opettajat, IT- ja järjestelmävastaavat, valmistelijat, päättäjät sekä tietosuojavastaavat (DPO), jotka käyttävät alustaa järjestelmien ja oppimateriaalien vaatimustenmukaisuuden ja tietosuojan arviointiin.
- **Oppilaat, opiskelijat ja huoltajat (VAIN valinnaisissa *Edudata Privacy*- ja *Edudata Security*-moduuleissa):** Oppilaiden, opiskelijoiden tai huoltajien henkilötietoja **ei käsitellä** perusmuotoisessa *Edudata Compliance* -hallintamoduulissa. Oppilas- tai opiskelijatietoja käsitellään ainoastaan silloin, jos Rekisterinpitäjä on erikseen ottanut käyttöön valinnaiset oppilasrajapinta- tai lokimoduulit (*Edudata Privacy* tai *Edudata Security*).
- **Vapaa tekstikenttä -suojalauseke (Free-Text Safeguard):** Mikäli Rekisterinpitäjän käyttäjä syöttää arviointilomakkeen vapaaseen tekstikenttään tai liitetiedostoon oppilaan tai huoltajan henkilötietoja, kyseisiä tietoja suojataan täysimääräisesti tämän DPA:n mukaisilla suojatoimilla (AES-256-salaus, TLS 1.2/1.3, asiakaskohtainen eriyttäminen ja RBAC), ja Rekisterinpitäjän pääkäyttäjä tai Käsittelijä (Rekisterinpitäjän pyynnöstä) voi poistaa tiedot välittömästi.

3. Henkilötietoryhmät ja tunnistautuminen (Zero Passwords — CP-ISMS-AUTH-001 v1.1)

Käsittelijä käsittelee seuraavia henkilötietoryhmiä käyttäjärooleissa (*Opettaja, Opettaja+, Valmistelija, Päättäjä, Asiakkaan pääkäyttäjä* sekä valinnaisissa moduuleissa *Oppilas/Opiskelija*):

- **Identiteetti- ja organisaatiotiedot:** Yksilöllinen käyttäjätunniste (Edudata UID), etu- ja sukunimi (näyttönimi), työsähköpostiosoite, organisaatio-/kuntayksikkö ja verkkotunnus, käyttäjärooli (RBAC), kielivalinta ja valinnainen profiilikuva.
- **Federoidut SSO-tunnistautumistiedot (ei salasanoja):** Palvelu käyttää yksinomaan federoidun kertakirjautumisen (SSO) tunnistautumista (Microsoft Entra ID / M365 tai Google Workspace) Firebase Authentication -palvelun kautta (`edudata-compliance-prod`). Käsiteltäviä teknisiä attribuutteja ovat IdP-tunniste, OAuth 2.0 / OIDC JWT -istuntotunnisteet, tilin luontiaika, viimeisin kirjautumisaika, istunto-ID, IP-osoite sekä selaimen/laitteen perustiedot. **Edudata.io ei koskaan vastaanota, käsittele tai tallenna käyttäjien salasanoja tai henkilökohtaisia tunnistautumissalaisuuksia** (*Authentication & Token Security Standard CP-ISMS-AUTH-001 v1.1*).
- **Valinnainen kolmannen osapuolen sovellusten metatieto (OAuth App Discovery):** Kolmansien osapoolten sovellusten kirjautumis- ja käyttöoikeusmetatietoja (OAuth-sovelluksen nimi, client ID ja myönnetyt luvat) käsitellään vain, jos Asiakas on ottanut käyttöön valinnaisen Google Workspace / M365 OAuth -sovelluskartoituksen.

4. Google Cloud -vastuumatriisi (7 kohtaa), säilytysajat (CP-ISMS-LOG-001 v1.2) ja kunnallinen arkistointi

7-kohtainen Google Cloud -vastuumatriisi: Poiketen vanhentuneista pilvikuvauksista Edudata-palvelun tuotantoympäristö toimii seuraavan selkeän vastuunjaon mukaisesti:

1. **Tuotantoprojektin omistajuus: Cloudpoint Oy** omistaa ja hallinnoi kokonaisuudessaan Edudata-tuotantoympäristön Google Cloud -projektia (`edudata-compliance-prod`).
2. **Google CDPA -sopimussuhde:** Cloudpoint Oy:llä on voimassa oleva Google Cloud Data Processing Addendum (CDPA) -sopimus **Google Cloud EMEA Limitedin / Google Ireland Ltd:n** kanssa.
3. **Aluelukitus ja tietokannat (v1/v2-yhteensopiva tallennusarkkitehtuuri):** Kaikki perustilit, arvioinnit ja relaatiotietokannat tallennetaan EU/ETA-alueelle (`europe-north1` Suomi ja `eu` -monialue) Cloudpoint Oy:n keskitettyihin Cloud SQL -tietokantoihin (`edudata-comp-db` ja `edudata-ai-db`) sekä erilliseen Firestore-tietokantaan. (Nykyisten v1-tallennusmallin asiakkaiden osalta valinnaisen SSO- ja sovelluslokimoduulin lokitiedot voivat sijaita asiakaskohtaisissa Google Cloud Firestore -projekteissa, kun taas uudet käyttöönotot käyttävät keskitettyä, tiukasti eristettyä EU-moniasiakasarkkitehtuuria v2; `TenantStorageRouter` tukee molempia malleja rinnakkain täydellä taaksepäin yhteensopivuudella.)

4. **IAM-käyttöoikeushallinta:** Cloudpoint Oy hallinnoi pilvi-infrastruktuurin IAM-käyttöoikeuksia pakotetun laitteistopohjaisen monivaiheisen tunnistautumisen (Yubico YubiKey 2SV) ja vähimmän oikeuden periaatteen (Least Privilege) mukaisesti.
5. **Salaus ja avaintenhallinta:** Cloudpoint Oy vastaa AES-256-lepotilasalauksesta (Google-Managed Encryption Keys, GMEK) ja sovellussalaisuuksien hallinnasta Google Cloud Secret Managerissa.
6. **Tekninen poistaminen:** Cloudpoint Oy suorittaa tietojen ja varmuuskopioiden teknisen poistamisen tämän DPA:n kohdan 11 mukaisesti (30 päivää ensisijainen data / 90 päivää varmuuskopiot).
7. **Auditointi- ja tietoturvalokitus:** Cloudpoint Oy vastaa keskitetystä ISO/IEC 27001 -lokituksesta EU-alueen BigQuery-lokiarkistoon (`edudata_compliance_logging`).

3-portainen ISO/IEC 27001 -lokien ja tietojen säilytysmatriisi (*Logging & Retention Standard CP-ISMS-LOG-001 v1.2*):

- **Taso 1 — Hallinnon ja järjestelmätapahtumien tarkastuslokit (400 päivää):** Muuttumattomat Google Cloud `_Required` Admin Activity- ja System Event -tarkastuslokit sekä EU BigQuery -lokiarkisto (`edudata_compliance_logging`) säilytetään **400 päivää**.
- **Taso 2 — Sovellus-, tietokanta- ja verkkotietoturvalokit (365 päivää / APM 15–30 päivää):** Google Cloud `_Default` -lokit, Cloud Run -sovelluslokit, Cloud SQL -tietokantalokit (`cloudsql_mysql_audit`) ja VPC-tietoturvalokit säilytetään **365 päivää**. Datadog APM -suorituskyky- ja virhejäljityslokit (joista henkilötiedot on maskattu) säilytetään **15–30 päivää**.
- **Taso 3 — Sovellustason elinkaariajat:** Passiiviset käyttäjätilit poistetaan automaattisesti **366 päivän** kuluttua viimeisimmästä kirjautumisesta; vastaamattomat tai hylätyt roolipyynnöt poistetaan **30 päivän** kuluessa; valinnaisen OAuth-sovelluskartoituksen lokit säilytetään enintään **18 kuukautta**.

Arvioinnit, päätökset ja pyynnöt (säilytys koko sopimuskauden ajan + 30 päivän poistoaika sopimuksen päätyttyä): Rekisterinpitäjän Palvelussa laatimia tietosuoja-arviointeja, DPIA-dokumentteja, päätöksiä ja pyyntöjä **ei poisteta ennen kuin asiakkaan sopimus Edudata.io-palvelun kanssa päättyy** (ellei Rekisterinpitäjä itse poista niitä). Rekisterinpitäjällä on koko sopimuskauden ajan täysi vientioikeus (export) kaikkiin arviointeihin, metatietoihin, versiohistoriaan ja tarkastuslokeihin. Sopimuksen päätyttyä noudatamme **30 kalenteripäivän poistoaikaa** ja tietojen poistumista ensisijaisista tietovarastoista (sekä varmuuskopioiden kiertopoistoa 90 kalenteripäivän kuluessa).

5. Hyväksytyt alihankkijat (Alikäsittelijät)

Käsittelijä käyttää Palvelun tuottamisessa seuraavia hyväksyttyjä alikäsittelijöitä:

Alihankkijan nimi	Käsittelyn tarkoitus, sijainti ja suojatoimet
Google Ireland Ltd (Google Cloud EMEA Limited)	Tuotannon pilvi-infrastruktuuri (`edudata-compliance-prod`), Cloud SQL, Firestore, Firebase Auth SSO sekä valinnainen Vertex AI (Gemini) & Document AI. Sijainti: **EU/ETA (`europe-north1` Suomi & `eu` -monialue)**. Koskee kaikkia Palvelun käyttäjiä (Google CDPA, EU SCC & DPF).
HubSpot Ireland Ltd	Asiakaspalvelun tukitikettijärjestelmä ja nimetyt asiakasyhteyshenkilöt (ei oppilastietoja; 5 kategorian tikettikielto). Sijainti: **EU/ETA (`dataHostingLocation = eu1` , AWS `eu-central-1` Frankfurt, Saksa)** (EU SCC, DPF & TIA).
Datadog, Inc.	Infrastruktuurin 24/7-suorituskyky-, viive- ja virhehälytysvalvonta (APM). Henkilötiedot maskataan (ei arviointien sisältödataa). Säilytys: **15–30 päivää** (EU SCC & DPF).

Alihankkijan nimi	Käsittelyn tarkoitus, sijainti ja suojatoimet
Aimpulse (Cloudpoint Oy:n dedikoitu tuotekehitysyksikkö / kumppaniyhtiö, Kairo, Egypti)	Ohjelmistokehitys yksinomaan Cloudpoint Oy:n operatiivisessa määräysvallassa ja ISO/IEC 27001:2022 -sertifioidun ISMS-hallintajärjestelmän alaisuudessa. Kehitys tapahtuu **eristetyssä ei-tuotantoympäristössä (`edudata-compliance-staging`) 100 % synteettisellä testidatalla** (`CP-ISMS-DLP-001 v1.2`); **ei pääsyä operatiiviseen asiakasdataan tai henkilötietoihin tuotantoympäristössä (`edudata-compliance-prod`)**. Sijainti: Egypti (EU SCC Module 3, TIA & 400 päivän audit-loki).
Online Partner AB	**Ehdollinen kumppani (Ruotsi):** Koskee **ainoastaan** sellaisia asiakkaita, jotka ovat solmineet sopimuksen Online Partner AB:n kautta paikallisena jälleenmyyjänä tai 1. tason tukikumppanina. Ei käsittele suoraan Cloudpoint Oy:n kanssa sopimuksen tehneiden kuntien tietoja. Sijainti: Ruotsi (EU/ETA).
Visma AB	**Vain Cloudpointin oma B2B-taloushallinto:** Käytetään yksinomaan Cloudpoint Oy:n lakisääteiseen B2B-laskutukseen ja sopimuslaskutukseen Cloudpointin toimiessa itsenäisenä rekisterinpitäjänä. Visma AB ei koskaan käsittele Edudata-alustan arviointitietoja tai loppukäyttäjätietoja. Sijainti: EU/ETA.

6. Kansainväliset tiedonsiirrot

Kaikki Palvelun tietokannat ja asiakassisällöt säilytetään EU/ETA-alueella (`europe-north1` Suomi ja `eu`-monialue). Mikäli alikäsittelijän käytön yhteydessä syntyy GDPR V luvun mukainen siirtotilanne ETA:n ulkopuolelle, siirto perustuu EU-komission tietosuojan riittävyyttä koskevaan päätökseen (kuten EU–US Data Privacy Framework) ja/tai EU-komission hyväksymiin vakiolausekkeisiin (SCC 2021/914) täydennettynä siirtojen vaikutustenarvioinnilla (TIA) ja teknisillä suojatoimilla.

LIITE 2: Tekniset ja organisatoriset turvatoimet (Versio 2.0 — 10.11.2026)

Käsittelijä toteuttaa ja ylläpitää GDPR 32 artiklan sekä ISO/IEC 27001:2022 -sertifioidun tietoturvan hallintajärjestelmän (ISMS) mukaisia teknisiä ja organisatorisia turvatoimia henkilötietojen luottamuksellisuuden, eheyden, käytettävyyden ja vikasietoisuuden varmistamiseksi.

Kaikkia Käsittelijän lukuun henkilötietoja käsitteleviä henkilöitä sitoo kirjallinen salassapitovelvollisuus, ja henkilöstö suorittaa säännölliset tietosuoja- ja tietoturvakoulutukset.

- **Cloudpoint Oy:n ISO/IEC 27001:2022 -sertifioitu ISMS (Prescient Security LLC, #123522) ja jatkuva Vanta-valvonta:** Cloudpoint Oy (2325703-6) ylläpitää **ISO/IEC 27001:2022 -sertifioitua** tietoturvan hallintajärjestelmää (ISMS, *Statement of Applicability v1.2* 20.10.2026; sertifikaatti `#123522` Issue 1, myönnetty 18.11.2026, voimassa 17.11.2029 asti; myöntäjä IAS-akkreditoitu **Prescient Security LLC**, MSCB-267, IAF MLA; päätoimipaikka Malminkaari 17-19 B, Helsinki). Sertifioitu soveltamisala kattaa julkisen sektorin, opetuksen ja yritysten pilviekosysteemien käyttöönoton, hallinnan ja optimoinnin, GCP- ja Google Workspace -infrastruktuurin sekä IT-, ohjelmistokehitys-, HR-, tietoturva-, laki- ja talousosastot. Vaatimustenmukaisuutta valvotaan jatkuvasti automaattisella Vanta-alustalla, mukaan lukien hallintakeinot VPM-38 (verkkokovennus, päivitysten ja poikkeamien hallinta), VPM-3 (haavoittuvuuksien ja riskien hallinta) sekä AST-4 – AST-9 (omaisuuserien ja päätelaitteiden elinkaaren hallinta).
- **Looginen moniasiakaseriyttäminen (Multi-Tenancy) ja kryptografinen suojaus (AES-256 & TLS 1.3):** Jokaisen kunta-asiakkaan tiedot on eristetty tiukalla organisaatiotunnisteeseen perustuvalla loogisella moniasiakaseriyttämisellä (multi-tenancy) sovellus- ja tietokantatasolla. Kaikki asiakastiedot, tietokannat ja varmuuskopiot salataan lepotilassa AES-256-algoritmilla (Google-Managed Encryption Keys, GMEK) ja siirron aikana TLS 1.3 -suojaprotokollalla (vähintään TLS 1.2). Tuotannon Cloud SQL -tietokantayhteydet pakottavat mTLS-varmenteet (`TRUSTED_CLIENT_CERTIFICATE_REQUIRED`).
- **Pääsynhallinta (Access Control Policy v1.1.0) ja laitteistopohjainen YubiKey (U2F/FIDO2) MFA:** Kaikki pääsy tuotantoympäristöihin on roolipohjaisen IAM-pääsynhallinnan ohjaamaa (vähimmän

oikeuden periaate) ja muuttumattomasti lokitettua. Kaikki ylläpitäjien kirjautumiset vaativat pakotetun monivaiheisen tunnistautumisen laitteistopohjaisilla Yubico YubiKey (U2F/FIDO2) -suojausavaimilla sekä työasemien koko levyn salauksen (Full Disk Encryption, FDE). Käyttöoikeudet katselmoidaan neljännesvuosittain, ja pääsyoikeudet poistetaan 24 tunnin kuluessa työsuhteen tai tehtävän päättymisestä.

- **Riippumaton penetraatiotestaus (kesäkuu 2026) ja haavoittuvuuksien hallinta (7 vrk / 14 vrk SLA):** Edudata.io-sovellukselle ja pilvi-infrastruktuurille on suoritettu riippumaton ulkopuolinen penetraatiotestaus kesäkuussa 2026 (*CP-ISMS-VSR-002 v1.0*), ja kaikki havainnot on korjattu ja todennettu **16.8.2026** mennessä. Haavoittuvuuksien hallintamenettelyn (*Vulnerability Management Procedure v2.1*) mukaisesti kriittiset haavoittuvuudet (Critical CVEs) korjataan **7 päivän** kuluessa ja korkean riskin haavoittuvuudet (High CVEs) **14 päivän** kuluessa (jatkuva Bitbucket Pipelines- ja Google Artifact Registry -skannaus).
- **Toipumisaika (RTO), palautuspiste (RPO) ja todennetut palautustestit (CP-ISMS-BIA-001 v1.1 & CP-ISMS-BCDR-002 v1.1):**
- Cloud Run -sovellusrajapinnat ja Firebase Auth SSO: **RTO < 15 minuuttia, RPO = 0** (monivyöhykkeinen korkea käytettävyys).
- Cloud SQL -tuotantotietokannat (`edudata-comp-db` , `edudata-ai-db`): **RTO < 1 tunti**, RPO = 24 tuntia (päivittäiset automaattiset varmuuskopiot) ja **lähes nolla (near-zero RPO)** 7 päivän jatkuvan binäärilokin (Point-in-Time Recovery, PITR) avulla; koko alustan RTO < 4 tuntia.
- **Todennetut palautusharjoitukset:** Tuotantotietokannan täysi palautusharjoitus suoritettiin onnistuneesti **3.6.2026 (kokonaiskesto 26 minuuttia)** ja PITR-ajankohtapalautustesti **18.10.2026 (kokonaiskesto 9 minuuttia 52 sekuntia)**, molemmat 100 % tietojen eheydellä.
- **3-tasoinen tiedon luokittelu ja fyysinen turvallisuus (Malminkaari 17-19B, 00700 Helsinki):** Asiakasdata ja henkilötiedot luokitellaan tasoille Luottamuksellinen (Confidential) / Rajoitettu (Restricted) Google Cloud -ympäristössä (`europe-north1` Suomi). Toimitilat osoitteessa Malminkaari 17-19B, 00700 Helsinki, Suomi ovat kulunvalvotut, vartioidut ja 24/7 kameravalvotut, ja Google Cloudin EU-konesalit ovat ISO 27001-, ISO 27017-, ISO 27018- ja SOC 2/3 -sertifioituja.

Turvallisen ohjelmistokehityksen (SDLC) hallintakeinot:

- Eristetyt kehitys-, testi- (`edudata-compliance-staging`) ja tuotantoympäristöt (`edudata-compliance-prod`); kehityksessä käytetään 100 % synteettistä testiaineistoa (`CP-ISMS-DLP-001 v1.2`).
- Pakollinen vertaisarviointi (4-eyes peer review) ja vanhemman kehittäjän hyväksyntä kaikille koodimuutoksille ennen tuotantoonvientiä.
- Automaattinen CI/CD-tietoturva- ja riippuvuusskannaus (Bitbucket Pipelines & Google Artifact Registry).
- Paikallinen kehitys tapahtuu vain keskitetysti hallituilla (MDM) kannettavilla tietokoneilla, joissa on koko levyn salaus (FDE).
- Säännöllinen OWASP- ja Google Cloud -tietoturvakoulutus kehittäjille sekä kyberuhkien ja haavoittuvuustiedotteiden jatkuva seuranta.

Pilvi-infrastruktuurin ja Asiakkaan vastuunjako:

Cloudpoint Oy omistaa ja hallinnoi Palvelun Google Cloud -tuotantoympäristöä (`edudata-compliance-prod`) ja vastaa sen tietoturvasta tämän Liitteen 2 mukaisesti. Asiakas rekisterinpitäjänä vastaa omien käyttäjiensä käyttövaltuuksien hallinnasta omassa identiteetinhallintajärjestelmässään (Microsoft Entra ID / Google Workspace) sekä syöttämiensä tietojen lainmukaisuudesta.

Palvelu toimii Googlen pilvipalvelussa (Google Cloud, `europe-north1` Suomi). Lisätietoja Googlen konesali- ja alustatietoturvasta on saatavilla Google Cloud Security Whitepapers -dokumentaatiosta.