



**Itslearning AS**  
PL 2686  
5836 Bergen  
Norja

**p:** + 47 55 23 60 70  
**s:** post@itslearning.com

---

# Henkilötietojen käsittelysopimus

---

OSAPUOLET:

[LISÄÄ ASIAKKAAN NIMI] \_\_\_\_\_  
ORG.NRO [LISÄÄ ORGANISAATIO NUMERO] \_\_\_\_\_  
(JÄLJEMPÄNÄ 'REKISTERINPITÄJÄ')

JA

ITSLEARNING AS, PALVELUN TILAUSSOPIMUKSEN MUKAISESTI  
(JÄLJEMPÄNÄ 'HENKILÖTIETOJEN KÄSITTELIJÄ')

---

## 1. Tarkoitus

Sopimuksen tarkoituksena on säännellä Euroopan tietosuojalainsäädännön, mukaan lukien yleisen tietosuoja-asetuksen (jäljempänä "sovellettava tietosuoja-lainsäädäntö") mukaisia oikeuksia ja velvollisuuksia, joita sovelletaan rekisterinpitäjään palvelun tilaussopimukseen (jäljempänä 'tilaussopimus') liittyen.

Sopimuksella varmistetaan, että tilaussopimuksen ehtojen (<https://itslearning.com/Global/terms-and-conditions>) mukaisesti käsiteltäviä henkilötietoja ei käytetä lainvastaisesti tai luovuteta valtuuttamattomalle kolmannelle osapuolelle.

Sopimuksesta aiheutuvat ilmoitukset on osoitettava tilauslomakkeessa mainitulle yhteyshenkilölle.

Mikäli rekisterinpitäjällä on kysyttävää tämän sopimuksen palveluista, ne voi osoittaa henkilötietojen käsittelijän tietosuojavastaavalle (DPO), [contact-dpo@itslearning.com](mailto:contact-dpo@itslearning.com).



## 2. Määritelmät

GDPR-asetuksella tarkoitetaan Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

Muilla tässä sopimuksessa käytetyillä tietosuojaan liittyvillä termeillä ja käsitteillä on sama sisältö ja merkitys kuin yleisessä tietosuoja-asetuksessa.

## 3. Käsittely ja ensisijainen vastuu

Sopimuksessa säännellään henkilötietojen käsittelijän suorittamaa henkilötietojen käsittelyä rekisterinpitäjän lukuun, mukaan lukien tietojen kerääminen, tallentaminen, yhteensovittaminen, säilyttäminen ja luovuttaminen tai niiden yhdistäminen. Käsiteltävien henkilötietojen aihe ja yksityiskohdat on eritelty liitteessä 1.

Henkilötietojen käsittelijällä itsellään ei ole henkilötietojen käyttöoikeutta, eikä se saa käsitellä henkilötietoja omiin tarkoituksiinsa. Henkilötietoja on käytettävä yksinomaan tilaussopimuksen tarkoituksiin rekisterinpitäjän määrittämissä rajoissa.

Jos henkilötietojen käsittelijä on lain mukaan velvollinen käsittelemään henkilötietoja muulla tavoin kuin rekisterinpitäjän ohjeiden mukaisesti, henkilötietojen käsittelijän on ilmoitettava siitä rekisterinpitäjälle ennen käsittelyn aloittamista, ellei sovellettava lainsäädäntö tai oikeusmenettely estä sitä tekemästä ilmoitusta.

## 4. Rekisterinpitäjän rooli ja vastuut

Rekisterinpitäjän vastuulla on varmistaa, että henkilötietojen käsittelylle on lainmukainen peruste, ja että varsinainen käsittely on sovellettavan tietosuojalainsäädännön mukaista.

Tähän vastuuseen liittyy, että rekisterinpitäjä varmistaa järjestelmänvalvojen riittävät valtuudet ennen henkilötietojen käsittelemistä rekisterinpitäjän puolesta.

Rekisterinpitäjän on myös suoritettava tarvittavat yksityisyyden suoja ja tietosuojaa koskevat vaikutustenarvioinnit, eli arvioitava ennen käsittelyn aloittamista suunniteltujen käsittelytoimien vaikutukset henkilötietojen suojaamiseen.

Rekisterinpitäjä on vastuussa loppukäyttäjien esittämistä pyynnöistä saada käyttöönsä henkilötietoja, joita rekisterinpitäjä tai henkilötietojen käsittelijä sopimuksen nojalla säilyttää. Mikäli henkilötietojen käsittelijä vastaanottaa tällaisia pyyntöjä, henkilötietojen käsittelijä neuvoo loppukäyttäjää esittämään pyyntönsä rekisterinpitäjälle, joka on vastuussa näihin pyyntöihin vastaamisesta.

Tilaussopimuksen mukaisesti rekisterinpitäjällä on mahdollisuus asentaa ja ottaa käyttöön lisätuotteita ulkopuolisilta kolmansilta osapuolilta (mukaan lukien laajennukset). Rekisterinpitäjä tiedostaa, että jos se asentaa, käyttää tai ottaa käyttöön tällaisia kolmannen osapuolen tuotteita, jotka voivat käyttää henkilötietoja, tämä henkilötietojen käsittelysopimus ei koske kyseisiin ulkoisiin kolmannen osapuolen tuotteisiin siirrettyjen tai niistä peräisin olevien tietojen käsittelyä. Rekisterinpitäjä voi ottaa käyttöön tai poistaa

käytöstä ulkoisia kolmannen osapuolen tuotteita, ja tilaussopimus ei edellytä siltä tällaisten tuotteiden käyttöä.

## 5. Henkilötietojen käsittelijän rooli ja velvollisuudet

Henkilötietojen käsittelijä saa käsitellä tietoja ainoastaan rekisterinpitäjän puolesta ja ainoastaan rekisterinpitäjän määräysten mukaisesti. Henkilötietojen käsittelijän suorittamaa satunnaista henkilötietojen käsittelyä, jolla varmistetaan tilaussopimuksen mukaisten palvelujen turvallisuus, toiminnan ylläpito, analysointi tai arviointi ja jolla ei ole haitallisia vaikutuksia rekisteröityjen tietosuojan tasoon, ei katsota henkilötietojen käsittelyksi henkilötietojen käsittelijän omiin tarkoituksiin.

Henkilötietojen käsittelijä sitoutuu antamaan rekisterinpitäjän käyttöön kaikki tiedot, jotka ovat välttämättömiä sovellettavan tietosuojalainsäädännön noudattamisen dokumentoimiseksi, ja avustamaan rekisterinpitäjää sen lain ja asetusten mukaisten velvollisuuksien täyttämässä-

Ellei toisin sovita tai laissa toisin määrätä, rekisterinpitäjällä on oikeus saada pääsy henkilötietoihin, joita henkilötietojen käsittelijä käsittelee rekisterinpitäjän puolesta, sekä kaikkiin järjestelmiin, joita käytetään tähän tarkoitukseen. Henkilötietojen käsittelijä sitoutuu avustamaan edellä mainitussa. Henkilötietojen käsittelijä ei kuitenkaan ole velvollinen paljastamaan liikesalaisuuksia tai kaupallisesti arkaluontoisia tietoja rekisterinpitäjälle. Rekisterinpitäjällä ei myöskään ole pääsyoikeutta, jos siitä voi aiheutua riski henkilötietojen turvallisuudelle tai eheydelle.

Henkilötietojen käsittelijällä, myös työntekijöillä, on niiden asiakirjojen ja henkilötietojen salassapitovelvollisuus, joihin henkilötietojen käsittelijällä on pääsy tämän sopimuksen nojalla. Tätä sopimuksen kohtaa sovelletaan myös sopimuksen päättymisen jälkeen. Kaikki tarvittavat salassapitosopimukset on tehtävä, mikäli työntekijät eivät jo ole laillisen salassapitovelvollisuuden piirissä. Salassapitovelvollisuus koskee myös henkilötietojen alikäsittelijöiden työntekijöitä, jotka suorittavat niiden järjestelmien ylläpitotehtäviä (tai vastaavia tehtäviä), joita henkilötietojen käsittelijä käyttää palvelun tarjoamiseen tai hallinnointiin.

Henkilötietojen käsittelijän sisäiset tietojen käyttöprosessit ja -menettelyt on suunniteltu estämään luvattomia henkilöitä ja/tai järjestelmiä käyttämästä järjestelmiä, joita käytetään henkilötietojen käsittelyyn. Henkilötietojen käsittelijä suunnittelee järjestelmänsä niin, että ne sallivat vain valtuutettujen henkilöiden pääsyn tietoihin, joita heillä on oikeus käyttää. Henkilötietojen käsittelijä varmistaa myös, että henkilötietoja ei voida lukea, kopioida, muuttaa tai poistaa ilman lupaa käsittelyn ja käytön aikana ja tallennuksen jälkeen. Hyväksyntöjä hallitaan työnkulun valvonnalla, joka rekisteröi kaikki muutokset. Kaikki järjestelmien käyttö kirjautuu seurantalokiin osoitusvelvollisuuden mukaisesti. Henkilötietojen käsittelijän on säilytettävä lokit vähintään kolmen kuukauden ajan. Rekisterinpitäjälle on pyydettyessä annettava pääsy tällaisiin seurantalokeihin.

## 6. Tietosuojavaltuutettu

Henkilötietojen käsittelijä on nimennyt sovellettavan tietosuojalainsäädännön mukaisesti tietosuojavastaavan.

## 7. Alikäsittelijöiden käyttäminen ja tietojen siirto

Mikäli henkilötietojen käsittelijä käyttää alihankkijoita henkilötietojen käsittelyyn, siitä on sovittava kirjallisesti rekisterinpitäjän kanssa ennen kuin alikäsittelijä aloittaa käsittelyn, paitsi jos alihankkijan käyttö on jo tilaussopimuksen mukaista. Henkilötietojen käsittelijän on varmistettava, että kaikki alikäsittelijät pääsevät käsiksi ja käyttävät henkilötietoja vain tämän henkilötietojen käsittelysopimuksen ehtojen mukaisesti ja että alihankkijoita sitovat kirjalliset sopimukset, joissa edellytetään vähintään sovellettavassa tietosuojalainsäädännössä määrättyä tietosuojan tasoa. Rekisterinpitäjä voi kohtuullisista ja perustelluista syistä kieltäytyä hyväksymästä uusia alikäsittelijöitä.

Rekisterinpitäjä on hyväksynyt seuraavalla verkkosivustolla luetellut alikäsittelijät: <https://itslearning.com/Global/gdpr/subprocessors> . Jos rekisterinpitäjä vaatii tarkempia tietoja käsittelypaikoista noudattaakseen lakisääteisiä vaatimuksia tai tietosuojaviranomaisten pyyntöjä, henkilötietojen käsittelijän on avustettava rekisterinpitäjää näiden vaatimusten noudattamisessa edellyttäen, että rekisterinpitäjä on ennen tällaisten tietojen antamista solminut asianmukaiset salassapitosopimukset tapauksissa, joissa henkilötietojen käsittelijä katsoo ne tarpeellisiksi.

Edellä mainitun luettelon yksiköiden lisäykset tai korvaamiset on saatettava rekisterinpitäjän tietoon esimerkiksi ilmoittamalla niistä rekisterinpitäjälle automaattisilla ilmoituksilla tai muilla keinoilla tarvittaessa. Rekisterinpitäjä voi neljän viikon kuluessa tällaisen ilmoituksen vastaanottamisesta vastustaa kyseistä muutosta tai lisäystä ainoastaan kohtuullisin perustein.

Henkilötietojen käsittelijä on vastuussa rekisterinpitäjälle alikäsittelijöiden toimista ja laiminlyönneistä samalla tavalla kuin henkilötietojen käsittelijän omista toimista ja laiminlyönneistä. Henkilötietojen käsittelijän vastuulla on varmistaa, että alikäsittelijä on perehtynyt henkilötietojen käsittelijän sopimusvelvoitteisiin ja lakisääteisiin tehtäviin ja että alikäsittelijä suorittaa ne samalla tavalla kuin henkilötietojen käsittelijä.

Henkilötietojen käsittelijä ja mahdollinen alikäsittelijä eivät voi siirtää henkilötietoja EU:n/ETA:n alueen tai ennalta hyväksytyjen kolmansien maiden ulkopuolelle ilman rekisterinpitäjän etukäteen antamaa kirjallista suostumusta. Rekisterinpitäjä voi käyttää henkilötietoja kolmannessa maassa tai sellaisesta käsin, eikä henkilötietojen käsittelijä tai alikäsittelijä voi pitää tällaista käyttöä henkilötietojen siirtämisenä kyseiseen kolmanteen maahan.

Mikäli henkilötietojen siirtoa tapahtuu joko henkilötietojen käsittelijän yksiköihin tai muille kolmansien osapuolten alikäsittelijöille EU:n/ETA:n alueen ulkopuolisiin maihin, kyseisiin siirtoihin on sovellettava sitovia ja asianmukaisia siirtomekanismeja, jotka ovat riittävän turvallisia sovellettavan tietosuojalainsäädännön mukaisesti.

## 8. Turvallisuus

### a. Turvatoimet ja dokumentointi

Henkilötietojen käsittelijän on täytettävä sovellettavassa tietosuojalainsäädännössä määrätyt vaatimukset turvatoimista. Henkilötietojen käsittelijä on velvollinen dokumentoimaan turvatoimensa. Liitteessä 3 on tiivistelmä henkilötietojen käsittelijän turvatoimista. Rekisterinpitäjälle voidaan toimittaa tarkemmat asiakirjat pyynnöstä.

Henkilötietojen käsittelijän on pantava täytäntöön ja ylläpidettävä asianmukaiset tekniset ja organisatoriset turvatoimet, joilla varmistetaan riskitason mukainen turvallisuustaso ja arvioidaan esimerkiksi henkilötietojen käsittelijälle tarjottavien pilvipalveluiden luonne. Näiden toimenpiteiden on suojattava siirrettyjä, tallennettuja tai muutoin käsiteltyjä henkilötietoja vahingossa tapahtuvalta tai laittomalta tuhoamiselta, häviämiseltä, muutoksilta, luvottomalta luovuttamiselta ja henkilötietoihin pääsystä. Henkilötietojen käsittelijän on toimenpiteiden suunnittelussa otettava huomioon kyky taata tietojen ja käsittelyjärjestelmien ja palvelujen luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus.

Henkilötietoja käsiteltäessä asianmukaisia turvatoimia ovat mm. seuraavat soveltuvien osin:

- henkilötietojen pseudonymisointi ja salaus;
- kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;
- kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;
- menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän määräysten mukaisesti, ellei sovellettavassa tietosuojalainsäädännössä tai muussa lainsäädännössä toisin vaadita.

#### **b. Käsittelytoimien yleiskuvaus**

Henkilötietojen käsittelijän ja tarvittaessa henkilötietojen käsittelijän edustajan on ylläpidettävä selostetta rekisterinpitäjän lukuun tehtävistä käsittelytoimista, joka sisältää seuraavat tiedot:

- a) henkilötietojen käsittelijän ja tietosuojavastaavan nimi ja yhteystiedot;
- b) rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät;
- c) tarvittaessa tiedot henkilötietojen siirtämisestä EU:n/ETA:n ulkopuoliseen maahan, mukaan lukien tieto siitä, mikä kolmas maa on kyseessä ja tarvittaessa asianmukaisia suojatoimia koskevat asiakirjat;
- d) mahdollisuuksien mukaan yleiskuvaus sovellettavista teknisistä ja organisatorisista turvatoimista.

Selostetta on päivitettävä jäljempänä olevan sopimuskohdan 9 mukaisesti. Henkilötietojen käsittelijän on pyydettäessä saatettava seloste valvontaviranomaisen saataville.

#### **c. Henkilötietojen tietoturvaloukkauksesta ilmoittaminen**

Henkilötietojen turvallisuuden tai yksityisyyden vaarantavasta tietoturvaloukkauksesta on ilmoitettava sopimuksen kohdassa 1 mainittuun yhteyspisteeseen. Ilmoitus on tehtävä ilman aiheetonta viivytystä ja ehdottomasti 72 tunnin kuluessa siitä, kun tietoturvarikkomus on tullut henkilötietojen käsittelijän tietoon.

Ilmoituksessa on oltava:

- Henkilötietojen kuvaus ja mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja lukumäärät sekä henkilötietotyyppien ryhmät ja lukumäärät
- Mahdollisen tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyshenkilö
- Kuvaus tietoturvaloukkauksen todennäköisistä seurauksista
- Kuvaus toimenpiteistä, jotka on toteutettu tai ehdotettu tietoturvaloukkauksen ratkaisemiseksi, sekä tarvittaessa toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Rekisterinpitäjä vastaa relevanttien tietoturvaloukkausten virallisesta ilmoittamisesta valvontaviranomaiselle ja tarvittaessa niille henkilöille, joihin henkilötietojen tietoturvaloukkaus vaikuttaa.

#### **d. Käytön hallinta ja laitteet**

Henkilötietojen käsittelijän on varmistettava, että sen palvelu on tietoturvallinen esimerkiksi palvelinten, tietokantojen ja muiden asiaankuuluvien laitteiden tai ohjelmistojen osalta niin, että kukaan ei pääse luvatta henkilötietoihin. Sama pätee kaikkiin tulosteisiin ja muihin fyysisiin asiakirjoihin.

Henkilötietojen käsittelijällä on lisäksi oltava käytössä tietosuojan valvontamenettelyt sovellettavan tietosuojasetuksen mukaisesti. Menettelyssä on oltava muun muassa seuraavat rutiinit:

- Toimenpiteet epäyhdenmukaisuuksien käsittelemiseen, esimerkiksi ilmoitusten tekeminen tietojärjestelmän väärinkäytöstä, kuten tietoturvaloukkauksista
- Tietosuojaa koskevat tarkastukset

Henkilötietojen käsittelijän on laadittava sellaiset turvallisuustoimenpiteet, jotka on havaittu tarpeellisiksi turvallisuuden ja teknologiaan liittyvässä riskienarvioinnissa, sekä ylläpidettävä niitä.

### **9. Käsittelytoimien päivittäminen ja turvallisuustarkastukset**

Käsittelytoimien luettelo (ks. edellä kohta 8 b) on tarkastettava ja päivettävä vähintään kerran vuodessa tai sen jälkeen, kun käsittelytoimiin on tehty huomattavia muutoksia.

Henkilötietojen käsittelijän on säännöllisesti, vähintään kerran vuodessa tai merkittävien muutosten tai eroavuuksien jälkeen, tarkastettava järjestelmien turvallisuus ja tarkastettava myös kaikki muu, mikä on olennaista henkilötietojen käsittelyn kannalta tämän sopimuksen mukaisesti. Turvallisuustarkastuksessa on varmistettava, että laadittuja teknisiä, fyysisiä ja organisatorisia turvallisuustoimenpiteitä noudatetaan ja että ne toimivat suunnitelmien mukaisesti sekä selvitettävä mahdolliset parannustarpeet.

Turvallisuustarkastuksen tulokset on dokumentoitava ja saatettava rekisterinpitäjän saataville esimerkiksi rekisterinpitäjän turvallisuustarkastusta varten.

Henkilötietojen käsittelijän järjestelmät ja prosessit tarkastetaan ja sertifioidaan säännöllisesti, ja kaikki sovellettavat sertifikaatit toimitetaan pyynnöstä rekisterinpitäjän saataville.

Rekisterinpitäjän pyynnöstä tehtävien erityistarkastusten kustannuksista vastaa rekisterinpitäjä.

## 10. Sopimuksen kesto

Sopimus on voimassa 25.5.2018 alkaen tai siitä päivästä lähtien, jona osapuolet ovat hyväksyneet sopimusehdot, jos kyseinen päivämäärä on 25.5.2018 jälkeen. Sopimus on voimassa niin kauan kuin tilaussopimus on voimassa ja korvaa kaikki aiemmat osapuolten välille solmitut henkilötietojen käsittelysopimukset.

Tämän sopimuksen tai sovellettavan tietosuoja-asetuksen rikkomuksen jälkeen rekisterinpitäjä voi määrätä henkilötietojen käsittelijän lopettamaan henkilötietojen käsittelyn.

## 11. Palauttaminen ja poisto sopimuksen päättymisen jälkeen

Tämän sopimuksen päättyessä henkilötietojen käsittelijän on palautettava, päällekirjoitettava tai poistettava liitteessä 2 mainituilla poistomenettelyillä ja/tai hävitettävä asianmukaisesti kaikki asiakirjat, tallennusvälineet ja muu henkilötietoja sisältävä aineisto, joka kuuluu tämän sopimuksen piiriin. Tämä pätee myös mahdollisiin varmuuskopioihin. Henkilötietojen käsittelijän on esitettävä kirjallisesti, että nämä toimenpiteet on suoritettu tämän sopimuksen mukaisesti kohtuullisen ajan kuluessa sopimuksen päättymisen jälkeen.

Rekisterinpitäjä vastaa kaikista tämän lausekkeen täyttämisen yhteydessä aiheutuvista kustannuksista, ellei tilaussopimuksessa toisin määrätä.

## 12. Lainvalinta ja oikeuspaikka

Lainvalintaa ja oikeuspaikkaa säännellään tilaussopimuksessa tai muulla tämän sopimuksen osapuolten välillä sovitulla tavalla.

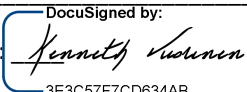
\*\*\*

Sopijana **itslearningin** puolesta  
(HENKILÖTIETOJEN KÄSITTELIJÄ)

Sopijana **asiakkaan** puolesta  
(REKISTERINPITÄJÄ)

itslearning-yksikön nimi:

Asiakkaan yksikön nimi:

Allekirjoitus:   
3E3C57F7CD634AB...

Allekirjoitus: \_\_\_\_\_

Kenneth Vuorinen  
Nimi: \_\_\_\_\_

toimitusjohtaja  
Nimike: \_\_\_\_\_

4/12/2018  
Päiväys: \_\_\_\_\_

Nimi: \_\_\_\_\_

Nimike: \_\_\_\_\_

Päiväys: \_\_\_\_\_



## LIITE 1

### Käsiteltävien henkilötietojen aihe ja yksityiskohdat Käsittelyn alkuperä ja tarkoitus

Henkilötietojen käsittelijänä itslearning käsittelee palvelun (eli itslearning-ohjelmiston, SkoleIntra- tai Fronter-alustojen), asiakkaan puolesta isännöidyn palvelun, yhteistyökumppaneiden sovellusten ja sivuston (<http://www.itslearning.com>) kautta saatuja henkilötietoja rekisterinpitäjän puolesta seuraaviin tarkoituksiin:

- Henkilötietojen käsittelysopimuksen ja tilaussopimuksen mukaisten palvelujen tarjoamiseen
- Palveluihin liittyvän perustuen ja teknisen tuen tarjoamiseen henkilötietojen käsittelysopimuksen ja tilaussopimuksen mukaisesti
- Rekisterinpitäjän tietojen turvalliseen varmuuskopiointiin.
- Henkilötietojen käsittelijä voi kerätä tietoja rekisterinpitäjän palvelun käytöstä sisäistä tilastointia ja laskutusta varten.

### Käsittelyn kesto

Tilaussopimuksen voimassaoloaika sekä ajanjakso sopimuksen päättymisestä siihen asti, kunnes henkilötietojen käsittelijä on poistanut kaikki asiakkaan tiedot voimassaolon mukaisesti.

### Henkilötietoryhmät

Henkilötietojen käsittelijä käsittelee henkilötietoja, jotka on lähetetty, säilytetty, tuotu, lähetetty tai vastaanotettu palvelun kautta rekisterinpitäjän ja sen valtuuttamien käyttäjien toimesta (tai rekisterinpitäjän käskystä). Tietojen laajuuden määrittävät ja sitä valvovat edellä mainitut oman harkintansa mukaan. Tiedot sisältävät seuraavat ryhmät:

- Yhteystiedot (nimi, sähköpostiosoite, puhelinnumero, osoite, käyttäjänimi jne.),
- Vanhempien tai huoltajien yhteystiedot
- Viestintä (viestit käyttäjien välillä, keskustelut, kommentit viesteihin, ilmoitukset, jne.)
- Kurssimateriaalit
- Arviointitulos ja arvosanat
- Kalenterimerkinnät ja tapahtumatiedot
- Asiakirjat, esitykset, kuvat, kotitehtävät, tehtävät jne.

### Rekisteröidyt

Henkilötietojen käsittelijän suorittama henkilötietojen käsittely palvelun kautta rekisterinpitäjän puolesta voi sisältää esimerkiksi henkilötietoja, jotka koskevat seuraavia rekisteröityjen ryhmiä:

- Asiakkaan työntekijät mukaan lukien opettajat, ylläpitäjät, lehtorit, mentorit ja muut
- Asiakkaan muut työntekijät ja toimeksisaajat sekä kaikki muut asiakkaan valtuuttamat käyttäjät, jotka lähettävät henkilötietoja palvelun kautta, mukaan lukien opiskelijat ja vanhemmat.

## LIITE 2 | POISTOMENETTELYT

### Tietojen poisto sopimuksen päättymisen jälkeen

Kuuden kuukauden kuluessa rekisterinpitäjän ja henkilötietojen käsittelijän välisen sopimuksen päättymisestä kaikki rekisterinpitäjän puolesta käsitellyt tiedot mukaan lukien varmuuskopiot on poistettava pysyvästi.

### Käytöstä poistetut tallennusvälineet ja tyhjennyskäytäntö

Tietoja sisältäviin tallennusvälineisiin/levyihin (mukaan lukien kiintolevyt, SSD-asetat, muistitikut ja nauhat) saattaa tulla toimintaongelmia, virheitä tai laitteistovikoja, joiden vuoksi ne on poistettava käytöstä. Jokainen käytöstä poistettu tallennusväline käy läpi erilaisia tietojen hävitysprosesseja, ennen kuin se viedään pois henkilötietojen käsittelijän tiloista joko uudelleenkäyttöä tai hävittämistä varten. Nämä prosessit on määritetty yrityksen tallennusvälineiden hävittämistä koskevassa menettelyssä (Company policy – Disposal of Storage Media), jolla varmistetaan, että kaikki tiedot hävitetään ja tuhoetaan täysin ja turvallisesti. Poistotulokset kirjataan seurantaan ottamalla ylös käytöstä poistetun tallennusvälineen sarjanumero.

## LIITE 3 | TURVATOIMET

itslearning on toteuttanut tässä liitteessä esitetyt turvatoimet, sekä organisatoriset että tekniset toimenpiteet, alan standardien mukaisesti. itslearning voi ajoittain päivittää tai muuttaa näitä turvatoimia edellyttäen, että päivitykset ja muutokset eivät heikennä palvelujen yleistä turvallisuutta. Ajantasainen versio on osoitteessa <https://itslearning.com/global/gdpr/securitymeasures/>.

### Organisatoriset toimenpiteet

Itslearningin johtoryhmä on osallistunut aktiivisesti tietoturvakulttuurin kehittämiseen yrityksessä meneillään olevan tiedotusohjelman kautta, ja sillä on organisaatiossa käytössä hallintorakenne, jonka selkeillä rooleilla ja vastuilla hallitaan tietoturvan täytäntöönpanoa palveluissa.

### Operatiivinen hallinta

Alan parhaita käytäntöjä ja menettelyitä noudattamalla varmistetaan alustan paras mahdollinen luottamuksellisuus, käytettävyys ja eheys. Menettelyt sisältävät tiukkoja vaatimuksia eri alueilla, joita ovat esimerkiksi:

- Tietoturva
- Hosting-ympäristön turvallisuus
- Kolmannen osapuolen käyttöoikeudet
- Kapasiteetin hallinta
- Muutosten hallinta
- Varmuuskopiointi ja palauttaminen
- Käytön valvonta
- Dokumentointi
- Kirjaaminen ja seuranta
- Tapahtumiin reagoiminen
- Julkaisuersioiden hallinta

### Tietoturvatiimi

itslearningillä on tietoturva-asiantuntijoista koostuva tiimi, joka vastaa organisaation tietoturvasta. Tiimin roolina on vastata seuraavista:

- Tietoturvaan liittyvien tehtävien koordinointi
- Yrityksen ympäristön, verkon ja laitteiden suojaaminen
- Sovelluksen tietoturva (sisäiset penetraatiotestit ja sovellustarkastukset)
- Seuranta ja kirjaaminen
- Prosessin ja menettelyn hallinta (palautussuunnitelma, polun hallinta jne.)
- Työntekijöiden tietoturvakoulutus
- Kolmannen osapuolen turvatarkastusten koordinointi ja mahdollisten havaintojen mukainen toiminta
- Koodin tarkkailu mahdollisten tietoturvaavaoittuvuuksien varalta.

## Roolit ja vastuut

Kaikilla työntekijöillä on selkeät roolit yrityksessä, ja heillä on pääsy vain oman roolinsa edellyttämiin tietoihin. Rajallisella määrällä työntekijöitä on ylläpitäjän roolissa pääsy tuotantoympäristöömme, ja heidän oikeuksiaan säännellään voimakkaasti ja tarkistetaan tietyin väliajoin. Kaikki merkittävät muutokset sovellukseen, ympäristöön tai tuotantoympäristön laitteistoon hyväksyy aina vähintään kaksi henkilöä.

## Henkilöstön turvallisuus

Koko itslearningin henkilöstöltä edellytetään tiukan salassapitosopimuksen allekirjoittamista. Koko henkilökunnan on noudatettava salassapitoa, liiketoiminnan etiikkaa ja ammatillisia standardeja koskevia yrityksen menettelytapoja. Asiakkaiden tietojen turvaamiseen, käsittelemiseen ja prosessoimiseen osallistuvien työntekijöiden on käytävä rooliaan vastaava koulutus.

## Käytön valvonta

Tiukat vaatimukset koskevat kaikkia työntekijöitä, konsultteja tai kolmansia osapuolia, jotka pyytävät pääsyä itslearningin tietojärjestelmiin. Käyttöä valvotaan todennusjärjestelmällä. Käyttäjältä vaaditaan:

- Johdon hyväksyntä pyydetylle käyttöoikeudelle
- Vahvat, yrityksen salasanakäytännön mukaiset salasanat
- Salasanan vaihtamista säännöllisin väliajoin
- Asiakirjaa, jossa todetaan pyydetyn käytön olevan oman roolin/tehtävän suorittamista varten
- Sen varmistamista, että laite (PC, tabletti, matkapuhelin) on turvassa ja lukittuna, kun käyttäjä on poissa.

itslearningin päätelaitteet lukittuvat automaattisesti väliaikaisesti, jos niitä ei käytetä.

Henkilötietojen käyttöä koskevat sisäiset prosessit ja menettelyt on suunniteltu estämään luvattomia henkilöitä ja/tai järjestelmiä käyttämästä järjestelmiä, joita käytetään henkilötietojen käsittelyyn. Kaikki tietojen muutokset kirjautuvat seurantalokiin osoitusvelvollisuuden mukaisesti.

## Fyysinen turvallisuus

### a. Palvelinkeskukset

itslearning toteuttaa kaikki asiakaspalvelunsa yrityksen toimistotiloista erillään olevissa palvelinkeskuksissa. Pääsy palvelinkeskuksiin on tiukasti valvottua ja suojattua, mikä vähentää luvattoman pääsyn, tulipalon, tulvien tai muiden fyysisen ympäristön vaurioiden todennäköisyyttä. Palvelinkeskusten fyysinen käyttö on rajattu pienelle joukolle itslearningin ja/tai sen isännöintikeskuksen palveluntarjoajien työntekijöitä. Palvelinkeskukseen tulijalla on ehdottomasti oltava turvallisuusjohdon hyväksymä kulkulupa.

### b. Toimistotilat

Kaikissa itslearningin toimistotiloissa on käytössä kulunvalvonta. Vain kutsutut kävijät ja työntekijät pääsevät itslearningin työtiloihin. Käytössä on useita toimenpiteitä, joilla voidaan välttää IT-laitteiden varastamisesta tai häviämisestä johtuvia tietoturvaongelmia. Näitä ovat mm. turvallisuusohjeet ja hyväksyttävät käyttömenettelyt, sekä tarvittaessa säilytysyksiköiden todennusjärjestelmät ja salaus.

## Tekniset toimenpiteet

### Järjestelmän käytettävyys

itslearningillä on käytössä alalla vakiintuneet toimenpiteet, joilla suojataan henkilötietoja vahingossa tapahtuvalta tuhoamiselta tai häviämiseltä. Näitä ovat mm.:

- Varainfrastrukturi (mm. verkon, virransyötön, jäähdytyksen, tietokantojen, palvelinten ja tallennustilan täydet varajärjestelmät)
- Varmuuskopioiden tallentaminen vaihtoehtoiseen kohteeseen, josta ne ovat palautettavissa ensisijaisen järjestelmän vikaantuessa.
- Asianmukainen suojaus palvelunestolta
- Henkilöstö töissä 365/24/7 järjestelmän seurantaa ja vianmäärittystä varten.

### Henkilötietojen suojaaminen

itslearningillä on käytössä useita alalla vakiintuneita toimenpiteitä, joilla estetään henkilötietojen luvaton lukeminen, kopiointi, muuttaminen tai poistaminen kuljetuksen tai säilytyksen aikana. Tämä toteutetaan alalla vakiintuneilla toimenpiteillä, joita ovat esimerkiksi:

- Monikerroksiset palomuurit, VPN-verkot ja salaustekniikat, joilla suojataan yhdyskäytäviä ja putkia
- HTTPS-salaus (tunnetaan myös nimellä SSL- tai TLS-yhteys) ja suojatut salausavaimet
- Palvelinkeskusten etäkäyttö on suojattu useilla verkon suojauskerroksilla
- Eriyisen arkaluontoiset asiakastiedot on suojattu salaamalla ja/tai hajauttamalla (pseudonymisointi)
- Jokainen käytöstä poistettu kiintolevy käy läpi poistoprosessin (Disk erase policy), ja käytöstä poisto kirjataan ottamalla ylös levyn sarjanumero
- Säännölliset kolmannen osapuolen turvatarkastukset (vähintään vuosittain), joihin liittyy penetraatiotestaus. Tarkastustiedot ovat asiakkaiden saatavilla.

### Palvelinkeskukset

itslearning käyttää vain alan uusinta tekniikkaa käyttäviä palvelinkeskuksia, joissa on aina paikalla henkilöitä huolehtimassa tuvallisuudesta ja seurannasta, 365/24/7. Palvelinkeskukset sijaitsevat uudenaikaisissa palonkestävissä tiloissa, joissa on sähköinen kuluvalvonta ja hälyttimet, jotka on kytketty kohteen turvajärjestelmään. Vain valtuutetut työntekijät ja toimeksiannon saaneet voivat pyytää sähköistä kulkulupaa tiloihin.

### Järjestelmäkehitys

itslearningin alusta perustuu alan standarditeknologiaan tunnetuilta toimittajilta (esim. Microsoft, Linux, Dell, Fujitsu, Amazon, Cloudflare, F5 ja Cisco). Järjestelmiin asennetaan säännöllisesti

uusimmat päivitykset, joten tietoturva on aina ajan tasalla. Alustaa päivitetään yleensä useita kertoja neljännesvuoden aikana, ja korjauksia julkaistaan nopeaan tahtiin tärkeysjärjestyksessä tiukan laadunvarmistusprosessin mukaisesti.

itslearningillä on käytössä toimenpiteitä, joilla minimoidaan sellaisen koodin tuominen alustaan, joka voi heikentää asiakaspalveluiden tai käsiteltävien henkilötietojen tietoturvaa tai eheyttä. Toimenpiteitä ovat mm.:

- Henkilöstön säännöllinen koulutus
- Tietoturva-arkkitehtien suorittama koodin tarkistus
- Laadunvarmistusprosessi, jolla testataan muutokset perusteellisesti ennen käyttöönottoa.

### **Alikäsittelijöiden tietoturva**

Ennen kuin itslearning käyttää alikäsittelijöitä, niiden turvallisuus- ja tietosuojakäytännöt tarkistetaan sen toteamiseksi, että ne ovat riittävällä tasolla niiden tietojen käytön ja tarjoamien palveluiden laajuuteen nähden. itslearning tarkistaa säännöllisesti alikäsittelijöidensä menettelyiden ja toiminnan turvallisuuden.