Tehtävänkäsittelynsopimus
(Artiklan 28 DS-GVO mukaan)

välillä

Käyttäjä (kuten pääsopimuksessa määritetty)

(jäljempänä ”**toimeksiantaja**”)

ja

TB Digital Services GmbH, Oskar-Schlemmer-Str. 19 - 21, 80807 München

(jäljempänä ”**toimeksisaaja**”)
(toimeksiantaja ja toimeksisaaja jäljempänä ”**osapuoli**” ja yhdessä ”**osapuolet**”).

Johdanto

(A) Tätä tehtävänkäsittelysopimusta (jäljempänä "**Sopimus**") sovelletaan kaikkiin toimiin, joissa toimeksisaaja on toimittanut toimeksiantajan henkilötietoja (kuten kohdassa 1.5 alla on määritetty), kolmansien osapuolten tai muiden asianomaisten osapuolten kanssa kohdassa 2 kuvatulla toiminnalla yleisistä puiteolosuhteista alustan käyttöön ja tarvittaessa tulee kosketukseen siitä johdettuihin yksittäissopimuksiin lisäpalveluista (seuraavassa "**Pääsopimus**").

(B) Tämän sopimuksen puitteissa toimeksiantaja toimii vastuullisena ja toimeksisaaja tehtävänkäsittelijänä tehtävänkäsittelyn puitteissa Art. 28 DS-GVO:n mukaan (kuten alla määritetty).

Sen vuoksi osapuolet sopivat seuraavan:

1 Määritykset ja tulkinta

1.1 ”**Eurooppalainen lainsäädäntö**” on Euroopan unionin lainsäädäntö, Euroopan unionin nykyisten jäsenvaltioiden sovellettavat lait sekä jokaisen sellaisen valtion sovellettavat lait, joista tulee myöhemmin Euroopan unionin jäsenvaltio.

1.2 ”**Eurooppalainen tietosuojalaki**” on Euroopan unionin henkilötietojen käsittelyä koskeva lainsäädäntö (ennen kaikkea tietosuoja-asetus), Euroopan unionin nykyisten jäsenvaltioiden henkilötietojen käsittelyä koskevat lait (ennen kaikkea Saksan tietosuojalain BDSG kulloinkin voimassa oleva versio) sekä jokaisen sellaisen valtion henkilötietojen käsittelyä koskevat lait, joista tulee myöhemmin Euroopan unionin jäsen.

1.3 ”**Tietosuoja-asetus**” on EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679, annettu 27. huhtikuuta 2017, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

1.4 ”**BDSG**” Saksan tietosuojalaki.

1.5 ”**Henkilötiedoilla**” on sama merkitys kuin BDSG:ssä ja tietosuoja-asetuksessa.

2 Tietojenkäsittelyn kohde / Toimeksiantajan velvollisuudet

2.1 Tämä sopimus määrittää osapuolten velvoitteet, jotka koskevat toimeksisaajan suorittamaa toimeksiantajan henkilötietojen käsittelyä liitteessä 1 mainitun pääsopimuksen puitteissa.

2.2 Käsittelyn kohde ja kesto, käsittelyn tapa ja tarkoitus, henkilötietojen tyyppi, henkilöiden luokitus sekä vastuullisen velvollisuudet ja oikeudet on määritetty tämän sopimuksen liitteessä 1 ja pääsopimuksen määrityksissä.

2.3 Toimeksiantaja pysyy edelleen DS-GVO:n mukaisesti vastuussa tietojenkäsittelystä ja takaa asianomaisten henkilöiden (kuljettajan ja tarvittaessa muiden henkilöiden) henkilötietojen käsittelyn hyväksyttävyyden. Erityisesti toimeksiantaja noudattaa laajaa tiedonantovelvollisuuttaan ja huolehtii siitä, että henkilötietojen käsittely perustuu tietosuojaa koskevaan oikeusperustaan (esimerkiksi yritysten välisen sopimuksen tekeminen, työsuhteen rajoittaminen työllistämisolosuhteen tarkoituksiin).

3 Toimeksisaajan velvollisuudet

3.1 Toimeksisaaja käsittelee toimeksiantajan henkilötietoja ainoastaan liitteessä 1 mainittuun tarkoitukseen ja pääsopimuksen puitteissa sekä liitteessä 1 dokumentoitujen toimeksiantajan ohjeistuksen mukaisesti; toimeksisaaja ei käsittele henkilötietoja mihinkään muuhun tarkoitukseen tämän sopimuksen puitteissa. Se ei vaikuta käsittelyyn tämän sopimuksen ulkopuolella omiin tarkoituksiin pääsopimuksen kohdan 8.3.4 mukaisesti. Henkilötietojen kopioita tai jäljennöksiä ei tehdä ilman toimeksiantajan tietoa. Se ei koske turvakopioita, sikäli kuin niitä tarvitaan asianmukaisen tietojenkäsittelyn turvaamiseen, eikä tietoja, joita tarvitaan laillisten säilytysaikojen noudattamiseen.

3.2 Käsittelypalvelujen tuottamisen jälkeen toimeksisaajan on toimeksiantajan valinnan mukaan palautettava ja/tai poistettava toimeksiantajan kaikki henkilötiedot, sikäli kuin siihen eivät vaikuta eurooppalaisen lainsäädännön säilytysajat, ja sikäli kuin toimeksisaaja ei käsittele niitä omiin tarkoituksiin tämän sopimuksen ulkopuolella pääsopimuksen kohdan 8.3.4 mukaisesti. Sama pätee testi- ja hylkymateriaaliin. Tietojen täydellinen poistaminen tai palauttaminen toimeksiantajalle on tämän vaatimuksesta vahvistettava kirjallisesti päivämäärällä varustettuna.

3.3 Mitä tulee palvelujen soveltamisalaan toimeksisaaja tukee toimeksiantajaa koskevien oikeuksien (tiedon, korjauksen, vastustuksen, poiston) täyttämistä toimeksiantajan ohjeiden mukaisesti.

3.4 Toimeksisaaja vahvistaa, että hän – mikäli laillisesti tarpeellista – on tilannut yrityksen tietosuojavaltuutetun (vrt. § 38 BDSG Art. 37 DS-GVO)

3.5 Toimeksisaaja sitoutuu ilmoittamaan toimeksiantajalle välittömästi tietosuojaviranomaisten tarkastusten tulokset, sikäli kuin ne koskevat toimeksiantajan tietojen käsittelyä. Toimeksisaaja korjaa mahdolliset huomautukset kohtuullisen ajan sisällä ja ilmoittaa siitä toimeksiantajalle.

3.6 Toimeksisaajan ja toimeksiantajan hyväksymien alihankkijoiden tietojenkäsittely tapahtuu ainoastaan Saksan liittotasavallan alueella, Euroopan unionin jäsenvaltiossa tai jossakin muussa Euroopan talousaluesopimukseen kuuluvassa valtiossa. Jokainen siirtäminen johonkin muuhun maahan (jäljempänä "**kolmas maa**") vaatii ennalta toimeksiantajan nimenomaisen hyväksynnän, ja sen saa tehdä vain, kun kolmansiin maihin vietävien tietojen erityiset edellytykset on täytetty (vrt. Art. 40 ff. DS-GVO) Hakemukseen täytyy tarvittaessa lisätä liitteessä 1 vaaditut (sopimus)dokumentit.

3.7 Toimeksisaajan täytyy tutustuttaa työt suorittavat työntekijät näiden osalta päteviin tietosuojamääräyksiin ja velvoittaa heidät noudattamaan vaitiolovelvollisuutta (vrt. Art. 28 DS-GVO Abs. 3 b)) samoin kuin asianmukaisin toimenpitein sen varmistamiseksi, että nämä työntekijät käsittelevät henkilötietoja vain toimeksiantajan ohjeiden mukaisesti.

3.8 Toimeksisaaja valvoo säännöllisesti tämän sopimuksen tietosuojaa koskevien määräysten ja toimeksiantajan ohjeistusten noudattamista sopimuksen koko keston ajan. Tarkastusten tulokset on esitettävä toimeksiantajalle pyynnöstä, sikäli kuin se on oleellista toimeksiantajan tietojen käsittelyn osalta. Valvontaa koskevat toimenpiteet on kuvattu tietosuojaperiaatteissa, jotka on esitettävä toimeksiantajalle pyynnöstä.

3.9 Toimeksisaajan on avustettava toimeksiantajaa käsittelyllä ja mahdollisuuksien mukaan sopivilla teknisillä ja organisatorisilla keinoilla tämän velvollisuudessa vastata osallisten henkilöiden asettamiin kysymyksiin tietosuoja-asetuksen luvussa III mainittujen oikeuksien hallinnoinnin mukaisesti. Toimeksiantajan on maksettava toimeksisaajalle tämän yhteydessä syntyvät kustannukset.

3.10 Toimeksisaajan on avustettava toimeksiantajaa käsittelyllä ja hänen käytössään olevilla tiedoilla tietosuoja-asetuksen artikloissa 32–36 mainittujen velvollisuuksien noudattamisessa.

4 Tietoturvallisuutta koskevat tekniset ja organisatoriset toimenpiteet

4.1 Toimeksisaaja huolehtii kohtuullisista tietoturvallisuutta koskevista teknisistä ja organisatorisista toimenpiteistä (vrt. Art. 32 DS-GVO). Toimeksisaaja on erityisesti velvoitettu toteuttamaan tämän sopimuksen liitteessä 2 sovitut tekniset ja organisatoriset toimenpiteet. Toimeksiantajan on sovitettava nämä toimenpiteet yhteistyösuhteen aikana teknisen ja organisatorisen kehityksen mukaisesti suojatasoa pienentämättä. Oleellisista muutoksista on sovittava kirjallisesti.

4.2 Toimeksisaaja todistaa toimeksiantajalle tämän pyynnöstä, että hän todella noudattaa teknisiä ja organisatorisia toimenpiteitä.

4.3 Toimeksiantaja on velvoitettu dokumentoimaan tietojen käsittelyn kohtuullisella tavalla, niin että toimeksiantaja pystyy todistamaan tietojen asianmukaisen käsittelyn. Todistus voi tapahtua myös tietosuoja-asetuksen artiklan 42 mukaisesti hyväksytyllä sertifioinnilla.

5 Alihankkijat

5.1 Toimeksisaajalle sallitaan liitteessä 1 mainittujen alihankkijoiden käyttö.

5.2 Muiden alihankkijoiden käyttö hyväksytään täten yleisesti. Toimeksisaaja tiedottaa kuitenkin toimeksiantajalle suunnitelluista muutoksista, jotka koskevat alihankkijoiden hankkimista tai korvaamista; toimeksiantaja voi esittää vastalauseen suunnitelluille muutoksille. Alihankkijasuhteena ei tämän määrityksen mukaan pidetä palveluja, jotka toimeksisaaja hankkii kolmannelta osapuolelta liitännäissuorituksena toimeksiannon suorittamisen tukemiseksi. Sellaisia ovat esimerkiksi telekommunikaatiopalvelut, siivoojat, tarkastajat tai tietoaineiston hävittäminen. Toimeksisaajan täytyy kuitenkin taata toimeksiantajan tietojen suoja ja turvallisuus myös ulkoistetuissa liitännäissuorituksissa asiaankuuluvilla ja lain mukaisilla sopimuksilla sekä huolehtia tarkastuksista.

5.3 Jos toimeksisaaja käyttää alihankkijaa, toimeksisaajan on varmistettava, että (i) alihankkijan ja toimeksisaajan välisessä sopimuksessa tai (ii) muissa eurooppalaisen tietosuojalain mukaisissa oikeudellisissa asiakirjoissa sovelletaan samoja tietosuojaa koskevia velvollisuuksia kuin tässä sopimuksessa on toimeksisaajalle määritetty. Toimeksisaajan on erityisesti varmistettava, että alihankkijalla on riittävät takuut sille, että tekniset ja organisatoriset toimenpiteet suoritetaan niin, että henkilötiedot käsitellään DS-GVO:n vaatimusten mukaisesti. Toimeksisaaja tiedottaa toimeksiantajan kirjallisesta pyynnöstä sopimuksen oleellisista kohdista ja tietosuojaa koskevien velvoitteiden toteutuksesta alihankkijasuhteessa ja antaa tarvittaessa luvan nähdä oleelliset sopimusasiakirjat. Toimeksiantaja saa tehdä kaupalliset ehdot näkymättömiksi. Toimeksiantaja on velvollinen noudattamaan vaitiolovelvollisuutta saamiensa tietojen osalta.

6 Tarkastusoikeudet

6.1 Toimeksiantajalla on oikeus tarkastaa itse tai toimeksiantajan nimeämän sopivan kolmannen osapuolen toimesta tämän sopimuksen velvoitteiden noudattaminen (annettu ohjeistus mukaan lukien).

6.2 Toimeksisaaja avustaa toimeksiantajaa tarkastuksissa kohtuullisella tavalla. Toimeksisaaja mahdollistaa erityisesti toimeksiantajan pääsyn tietojenkäsittelylaitteisiin ja antaa tietoja.

6.3 Mikäli tarkastuksen tuloksena on, että toimeksisaaja ja/tai käsittely ei noudata sopimuksen ja/tai eurooppalaisen tietosuojalain määrityksiä, toimeksisaaja suorittaa kaikki vaadittavat

korjaustoimenpiteet takaamaan tämän sopimuksen ja/tai eurooppalaisen tietosuojalain määritysten noudattamisen.

6.4 Toimeksiantaja maksaa itse tarkastuksesta aiheutuvat kustannukset. Toimeksisaaja voi vaatia, että toimeksiantaja maksaa hänelle toimeksiantajan tarkastuksesta aiheutuneet kustannukset, sikäli kuin toimeksiantaja suorittaa tai antaa suorittaa tarkastuksen useamman kerran kalenterivuoden sisällä.

6.5 Toimeksisaajan luona suoritettavista tarkastuksista on ilmoitettava hyvissä ajoin eivätkä ne saa vaikuttaa toimeksisaajan liiketoimintaan kohtuuttomalla tavalla.

7 Huomautusvelvollisuudet

Toimeksisaaja ilmoittaa toimeksiantajalle välittömästi, jos toimeksiantajan antama ohjeistus on toimeksisaajan mielestä eurooppalaisen tietosuojalain vastainen. Perustellusti kritisoitua ohjeistusta ei tarvitse noudattaa, niin kauan kuin toimeksiantaja ei ole muuttanut tai nimenomaisesti vahvistanut sitä. Toimeksisaaja ei ole velvollinen tarkastamaan ohjeistusten perusteltavuutta.

Toimeksisaaja on todetessaan tietojen käsittelyssä virheitä tai epäsäännöllisyyksiä tai epäillessään tietosuojan loukkaamista (jäljempänä yhdessä ”**tapahtuma**”) velvollinen ilmoittamaan siitä välittömästi toimeksiantajalle. Toimeksiantajan on dokumentoitava tapahtuma sekä kaikki olosuhteet, vaikutukset ja korjaavat toimenpiteet ja lähetettävä nämä dokumentoidut tiedot välittömästi toimeksiantajalle pyynnöstä kirjallisesti tai sähköisesti.

8 Vastuu ja vastuuvapaus

8.1 Toimeksisaaja vastaa vahingoista, jotka ovat aiheuttaneet toimeksisaajan tai tämän edustajan tahallinen teko ja/tai törkeä huolimattomuus. Toimeksisaaja vastaa vahingoista, jotka aiheuttaa toimeksisaajan tai tämän edustajien lievä huolimattomuus, sikäli kuin kyseessä ei ole olennaisen velvollisuuden loukkaaminen. Olennaiset velvollisuudet ovat sopimusvelvollisuuksia, jotka mahdollistavat sopimuksen asianmukaisen toteutuksen ja joiden täyttämiseen toimeksiantaja on luottanut ja sai luottaa. Tällaisten olennaisten velvollisuuksien loukkaaminen, kun kyseessä on lievä huolimattomuus, rajoittaa toimeksisaajan vastuuvelvollisuuden tavallisesti ennakoitaviin vahinkoihin.

8.2 Toimeksiantaja vapauttaa toimeksisaajan kaikista kolmatta osapuolta (asianomaiset henkilöt ja/tai tietosuojaviranomaiset mukaan lukien), vahinkoja ja kuluja koskevista vaatimuksista, jotka aiheuttaa toimeksiantajan tämän sopimuksen ja/tai eurooppalaisen tietosuojalain määräysten loukkaaminen; tämä ei päde, mikäli toimeksiantaja ei ole syyllistynyt tai myötävaikuttanut niihin.

9 Kesto

Tämän sopimuksen kestoaika on sama kuin pääsopimuksen kestoaika. Kun pääsopimus päättyy, mistä syystä tahansa, tämäkin sopimus päättyy aina automaattisesti. Irtisanominen tärkeästä syystä pysyy voimassa.

10 Muuta

10.1 Toimeksisaajan tämän sopimuksen mukaisten suoritukset on hyvitetty pääsopimuksessa sovittujen korvaussääntöjen mukaisesti.

10.2 Jos toimeksiantajan henkilötiedot ovat vaarassa toimeksisaajan luona kolmannen osapuolen toimenpiteiden (esimerkiksi ulosmittauksen tai takavarikoinnin), maksukyvyttömyyden tai sovittelumenettelyn tai muun vastaavan tapahtuman vuoksi, toimeksisaajan on ilmoitettava siitä toimeksiantajalle välittömästi.

10.3 Jos tämän sopimuksen jotkin määräykset ovat tehottomia tai muuttuvat tehottomiksi, se ei vaikuta muiden määräysten vaikuttavuuteen. Osapuolet sopivat tehottomalle lausekkeelle asiasisällön ja taloudellisuuden osalta sopimuksen tarkoituksen mukaisen vaihtoehtoisen säännöksen.

10.4 Siinä tapauksessa, että Britannia jättää Euroopan unionin, toimeksisaaja sitoutuu jo nyt solmimaan kaikki sopimukset ja suorittamaan kaikki toimenpiteet, jotka ovat tarpeellisia, jotta sopimuksen mukainen tietojenkäsittely voidaan hoitaa Britanniassa unionista lähtemisen ajankohdasta lukien tietosuojalain sallimalla tavalla. Sikäli kuin Euroopan komissio ei lähtöajankohtana ole antanut päätöstä tietosuojan tason riittävyydestä, kyseessä ovat tämän päivän näkökulmasta ennen kaikkea artiklan 46, kohdan 2 c) mukaiset vakiotietosuojalausekkeet, jotka koskevat henkilötietojen lähettämistä tietojen käsittelijöille, jotka toimivat kolmansissa maissa, joissa ei ole riittävää suojatasoa.

Jos toimeksisaaja ei toteuta näitä velvollisuuksia, toimeksiantajalla on oikeus vaatia toimeksisaajalta Britannian Euroopan unionista lähtemisen ajankohtana, että kyseiset palvelut suorittaa sidosyritys tai yrityksen yksikkö, jolla on pysyvä sijaintipaikka Euroopan unionin alueella, ilman että siitä aiheutuu toimeksiantajalle lisärasitetta tai lisäkustannuksia.

10.5 Tästä tehtävänkäsittelysopimuksesta on 18 erikielistä versiota, jolloin alkuperäisellä saksankielisellä versiolla on poikkeamien kohdalla etusija.

10.6 Tähän sopimukseen sovelletaan Saksan liittotasavallan lakia sulkien pois YK:n kauppalain soveltamisen. Toimivaltainen tuomioistuin on Münchenissä.

10.7 Seuraavat liitteet ovat sopimuksen olennaisia osia:

Liite 1 – Tehtävänkäsittelyn kuvaus
Liite 2 – Tekniset ja organisatoriset toimenpiteet

LIITE 1 – Tehtävänkäsittelyn kuvaus

1 Pääsopimus

Pääsopimus on sopimuksen pääosan kohdan 2.1 mukaisesti ”Alustan käytön yleiset ehdot”.

Nimitys/osapuolet: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19 - 21, 80807 München / **Käyttö**

2 Toimeksiannon sisältö ja kesto

Toimeksiannon sisältö on kuvattu pääsopimuksen kohdassa 1 (*Sisältö*) ja kohdassa 8 (*Käyttäjän tiedot ja tietosuoja*); toimeksiannon kesto on kuvattu pääsopimuksen kohdassa 7 (*Sopimuksen solmiminen, sopimuksen kesto ja irtisanomisoikeudet*).

3 Tietojenkäsittelyn laajuus, tapa ja tarkoitus / tietojenkäsittelytoimenpiteet

Henkilötietojen käsittelyn laajuus, tapa ja tarkoitus on kuvattu pääsopimuksen kohdassa 8.

Toimeksiannon sisällön yksityiskohtainen kuvaus koskien laajuutta, tapaa ja tarkoitusta:

Jotta toimeksiantajan tarjoamat palvelut (kuten pääsopimuksessa määritetty) voidaan suorittaa, toimeksiantajan täytyy kerätä toimeksiantajan henkilötiedot Connectec Vehicles- tai Mobile Devices -ratkaisun (ja tarvittaessa kolmannen osapuolen, jonka kanssa käyttäjä on sopinut kolmannen osapuolen palveluista, siirtämät tiedot) välityksellä palvelujen suoritukseen tarvittavissa määrin ja siirtää ne toimeksisaajan alustaan ja tallentaa ne sinne. Toimeksisaaja käsittelee alustaan tallennetut tiedot palvelujen suorittamiseen tarvittavissa määrin (esimerkiksi analysoi ja arvioi henkilötietojen perusteella kuljettajien ajokäyttäytymistä sekä Connected Vehiclen tai Mobile Devicen käyttöä ja tekee niihin perustuen toimeksiantajalle tälle räätälöityjä tarjouksia, kuten ajokoulutuksia, varusteita sekä ehdotuksia tehokkuuden parantamiseen). Tarkka laajuus, tapa ja tarkoitus määritetään lisäksi laadittavissa yksittäissopimuksissa.

4 Osalliset (osallisten henkilöiden kategoriat)

Tehtävänkäsittelyn piiriin kuuluvat seuraavat henkilöryhmät:

- **Kuljettaja ja muut työntekijät** (toimeksiantajan oman yhtiön työntekijät), esimerkiksi palkansaajat, oppisopimusopiskelijat, työnhakijat, entiset työntekijät,
- **Kuljettajat**, jotka eivät ole yrityksen työntekijöitä;
- Kuormaajien/purkajien tai toimeksiantajan muiden liikekumppanien **yhteyshenkilöt**; ja
- **Konsernin työntekijät** (toimeksiantajan jonkin toisen konserniin kuuluvan yhtiön työntekijät).

5 Henkilötietojen tyyppi

Tehtävänkäsittely käsittää seuraavan tyyppiset henkilötiedot:

- kuljettajan nimi ja kuljettajan tunnusnumero;
- ajoneuvon tunnistenumero;
- sijaintipaikkatiedot;
- ajo- ja lepoaikojen tiedot;
- tiedot ajokäyttäytymisestä;
- Connected Vehiclen tilatiedot;
- perävaunun tilatiedot;
- korien tai lisäasennusten, yksikköjen ja ajoneuvon muiden osien tilatiedot;
- muiden mahdollisesti yhdistettyjen IOT-laitteiden tilatiedot
- Mobile Device -laitteiden tilatiedot;
- lastaustiedot;
- tilaustiedot; ja
- kuormaajien/purkajien tai toimeksiantajan muiden liikekumppanien yhteyshenkilöt.

6 Dokumentoidut ohjeistukset

Toimeksiantaja antaa toimeksisaajalle ohjeistuksen käsitellä henkilötietoja, kuten pääsopimuksen kohdassa 8 on kuvattu. Se sisältää ennen kaikkea seuraavan käsittelyn:

- Henkilötiedot siirretään Connected Vehiclen tai Mobile Devicen välityksellä toimeksisaajan pilvipalvelussa toimivaan alustaan ja tallennetaan sinne.
- Henkilötietoja käsitellään tämän sopimuksen perusteella vain siinä määrin, kuin se on tarpeellista pääsopimuksen soveltamisen osalta; se ei vaikuta pääsopimuksen kohtaan 8.3.4.
- Toimeksisaaja siirtää henkilötiedot ulkopuoliselle palveluntarjoajalle (kuten pääsopimuksessa on määritetty), sikäli ja siinä määrin kuin tällainen siirtäminen ulkoiselle palveluntarjoajalle on tarpeellista, jotta tämä voi toimittaa toimeksiantajalle ulkoiset palvelunsa (kuten pääsopimuksessa on määritetty).
- Toimeksisaaja analysoi ja arvioi henkilötietojen perusteella kuljettajan ajokäyttäytymistä ja Connected Vehiclen käyttöä ja tekee niihin perustuen toimeksiantajalle tälle räätälöityjä tarjouksia, kuten ajokoulutuksia, varusteita sekä ehdotuksia tehokkuuden parantamiseen.

7 Käsittelypaikka

- Saksa.
- Yhdistynyt kuningaskunta; mikäli IT-hostingpalveluja ja/tai IT-tukipalveluja koskevia tietoja käsitellään Euroopan unionin sisällä, on solmittu niitä vastaavat tehtävänkäsittelysopimukset.

- Jos toimeksisaaja käyttää IT-hostingpalveluihin tai IT-tukipalveluihin alihankkijoita Euroopan unionin ulkopuolella (katso tämän liitteen 1 kohta 8), henkilötietojen siirto tapahtuu sopimuspuolen ja alihankkijan/vakiomuotoisten tietosuojalausekkeiden välillä, jotka koskevat henkilötietojen siirtämistä kolmansiin maihin jalostajille 46 artiklan 2 c alakohdan) DS-GVO: n mukaisesti.

8 Alihankkijat

Toimeksisaaja käyttää seuraavia alihankkijoita (jotka voivat osaltaan käyttää muita alihankkijoita):

Nro	Alihankkija (yritys, osoite, yhteyshenkilö)	Käsiteltyjen tietojen kategoriat	Käsittelyvaiheet / alihankintana tapahtuvan tehtävänkäsittelyn tarkoitus
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Alustan kaikki henkilötiedot, jotka ovat tekemisissä myyntiosan kanssa (eli siellä, missä asiakkaan rekisteröityy alustaan ja voi tehdä tilauksia)	Alustan hostingpalvelu
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	Alustan kaikki henkilötiedot, jotka ovat tekemisissä myyntiosan kanssa (eli siellä, missä asiakkaan rekisteröityy alustaan ja voi tehdä tilauksia)	Alustaa koskeva IT-tuki
3	Amazon Webservices, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	Kaikki muut henkilökohtaiset käyttäjätiedot, jotka välitetään toimeksisaajalle ajoneuvon välityksellä	Alustan hostingpalvelu / alustan hostingpalvelua koskeva IT-tuki
4	Tulevaisuudessa mahdollisesti nron 3 sijaan: Amazon Webservices (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA https://aws.amazon.com/de/compliance/contact/	Kaikki muut henkilökohtaiset käyttäjätiedot, jotka välitetään toimeksisaajalle ajoneuvon välityksellä	Alustan hostingpalvelu
5	MAN Service und Support GmbH Dachauer Straße 667	Kaikki henkilötiedot, joita tarvitaan asiakaskyselyjen käsittelyyn ensimmäisen ja toisen tason tuen	Ensimmäisen tason tuki

	80995 München Saksa	puitteissa	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	Kaikki henkilötiedot, joita tarvitaan laskujen/tilausten käsittelyyn	Alustan hostingpalvelu (EU:ssa – hosting: Amazon Web Services (EU) – katso kohta 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 München Saksa	Kaikki muut henkilökohtaiset käyttäjätiedot, jotka välitetään toimeksisaajalle Connected Vehiclen ja/tai Mobile Devicen välityksellä	Alustan hostingpalvelu
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Saksa	Kaikki muut henkilökohtaiset käyttäjätiedot, jotka välitetään toimeksisaajalle TBM1/2-ajoneuvon välityksellä	Alustan hostingpalvelu
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Ruotsi	Kaikki muut henkilökohtaiset käyttäjätiedot, jotka välitetään toimeksisaajalle ajoneuvon välityksellä	Alustan hostingpalvelu
10	Volkswagen Hyötyajoneuvot Mecklenheidestr. 74 30419 Hannover Saksa	Kaikki muut henkilökohtaiset käyttäjätiedot, jotka välitetään toimeksisaajalle ajoneuvon välityksellä	Alustan hostingpalvelu

LIITE 2 – Tekniset ja organisatoriset toimenpiteet
Toimeksisaajan suoritettavat tekniset ja organisatoriset toimenpiteet riskeille sopivan suojatason takaamiseksi on kuvattu RIO-alustan tietosuojaperiaatteissa, ja niihin kuuluvat ennen kaikkea:

1. Pseudonymisointi

Sikäli kuin henkilötietoja käytetään arviointeihin, jotka voidaan suorittaa myös pseudonymisoiduilla tiedoilla, käytetään pseudonymisointitekniikoita. Jokaiseen tietokenttään määritetään ennalta, täytyykö se pseudonymisoida, koska se voisi mahdollistaa henkilön tunnistamisen. Pseudonymisointiavaimet tallennetaan "Data Safeen", jolle määritetään suurin mahdollinen pääsyrajoitus.

2. Salaus

Mobiilipäätelaitteet kommunikoivat salattuina päätepisteen kanssa laitekohtaisella sertifikaatilla. Tiedot siirretään RIO-alustassa salattuina ("Ubiquitous encryption" tai "encryption everywhere").

3. Luottamuksellisuuden varmistaminen

Kaikille työntekijöille tiedotetaan heidän vaitiolovelvollisuudestaan ja heidät velvoitetaan kirjallisesti vaitiolovelvollisuuteen.

Käytetty IT-infrastruktuuri asetetaan käyttöön Amazon Web Services -palveluna (seuraavassa AWS) pilvipalvelun (IaaS ja PaaS) puitteissa. AWS-palvelinkeskus huolehtii kulunvalvonnasta: huipputurvalliset AWS-keskukset käyttävät uusimman tekniikan mukaisia elektronisia valvontajärjestelmiä ja monitasoisia kulunvalvontajärjestelmiä. Palvelinkeskuksissa on vuorokauden ympäri koulutetut turvahenkilöt, ja kulkua valvotaan tiukasti vähimpien oikeuksien periaatteella, ja se sallitaan ainoastaan järjestelmän ylläpitoa varten.

Pääsy laitteisiin (Clients) tapahtuu TB Digital Services GmbH:n tiloissa pätevillä, yksittäistapaukseen sopivilla vakiotoimenpiteillä. Niitä ovat esimerkiksi yhden henkilön läpipäästävät laitteet (kääntöportit), videovalvontalaitteet, hälytyslaitteet ja/tai vartiointi, elektronisesti ja mekaanisesti varmistetut ovet, luvatonta pääsyä vastaan suojatut rakennukset, dokumentoidut kulkuluvat (vierailijat, vierastyövoima) tai määritetyt turvallisuusalueet.

Kulunvalvonta käsittää toimenpiteet laitteiden varmistukseen, verkon varmistukseen ja sovellusten varmistukseen.

Ajoneuvojen laitteiden varmistuksessa käytetään erilaisia toimenpiteitä: Mobiilipäätelaitteet on asennettu pysyvästi ajoneuvoihin, ja niissä on Secure boot -toiminto, eli vierasta käyttöjärjestelmää ei voida ladata ja käynnistää. Mobiilipäätelaitteet kommunikoivat salattuina päätepisteen kanssa laitekohtaisella sertifikaatilla. Tiedot siirretään RIO-alustassa salattuina ("Ubiquitous encryption" tai "encryption everywhere"). Päätelaitteiden turvallisuustaso on aina ajan tasalla säännöllisten turvapäivitysten ansiosta (Patch management).

Verkon varmistukseen käytetään myös erilaisia vakiotoimenpiteitä: Käytössä on sopivat (tekniikan nykytason mukaiset) salasanamääritykset (salasanan pituus, kompleksisuus, kesto jne.). Käyttäjätunnus- ja salasanayhdistelmän toistuva virheellinen syöttö aiheuttaa käyttäjätunnuksen (väliaikaisen) eston. Yritysverkko on suojattu palomuurilla epäturvallisia avoimia verkkoja vastaan. Käytössä on prosessi, joka huolehtii mobiililaitteiden säännöllisistä turvapäivityksistä (OTA-prosessi). Käytössä on sopivat tekniset ratkaisut yrityksen verkkoon (Intranetiin) kohdistuvien hyökkäysten tunnistamiseen ja välttämiseen (esim. Intrusion Detection -järjestelmät). Työntekijöitä opastetaan säännöllisesti tunnistamaan vaarat ja riskit.

Sovellusten varmistukseen käytetään myös erilaisia vakiotoimenpiteitä:

Sovellukset on suojattu luvattomalta pääsyltä sopivilla tunnistus- ja vahvistusmekanismeilla. Käytössä on sopivat (tekniikan nykytason mukaiset) salasanamääritykset (salasanan pituus, kompleksisuus, kesto jne.). Erityistä suojausta tarvitsevissa sovelluksissa käytetään vahvoja tunnistusmekanismeja (esim. Token, PKI). Käyttäjätunnus- ja salasanayhdistelmän toistuva virheellinen syöttö aiheuttaa käyttäjätunnuksen (väliaikaisen) eston. Tärkeissä menetelmissä käytetyt tiedot ovat salatussa muodossa mobiilisti käytettävällä tallennusvälineellä. Sovelluksiin pääsyt ja pääsy-yritykset kirjataan lokiin. Lokitiedostoja säilytetään sopivan ajanjakson verran (väh. 90 päivää) ja tarkistetaan (satunnaisesti).

Käyttäjäoikeudet (pääsyä ja saantia varten) varmistetaan erilaisilla toimenpiteillä, joskin ne on kohdistettu tunnistettavissa olevaan henkilöön. Oikeuksien myöntäminen on alustasta vastaavan vastuulla, ja se tarkistetaan säännöllisesti. Pääsyoikeudet myönnetään vain määritetyssä ja dokumentoidussa prosessissa. Pääoikeuksien muutokset tehdään kahden käsittelijän periaatteella ja dokumentoidaan versioilla merkittyihin lokitiedostoihin.

Pääsyn tarkastuksessa tai hallinnassa käytetään erilaisia toimenpiteitä: Pääsyoikeudet määritetään ja dokumentoidaan rooli-/käyttöoikeusperiaatteiden puitteissa, ja ne on kohdistettu kunkin roolin tehtäväkohtaisten vaatimusten mukaisesti. Teknisille ylläpitäjille on määritetty erityiset roolit/oikeudet (jotka eivät, sikäli kuin teknisesti mahdollista, salli pääsyä henkilötietoihin). Sisältötuelle on määritetty erityiset roolit/oikeudet (jotka eivät sisällä teknisten ylläpitäjien oikeuksia).

Roolien/oikeuksien määritys ja roolien/oikeuksien kohdistus tehdään, mikäli teknisesti ja organisatorisesti mahdollista, ei-samojen henkilöiden toimesta ja tarkastusvarmassa (hyväksyntä)menettelyssä, ja se on ajallisesti rajoitettu. Suora pääsy tietokantoihin rooli-/oikeusperiaatteen ulkopuolella on mahdollista vain valtuutetuille tietokannan ylläpitäjille. Yksityisten tallennusvälineiden käyttöä varten on oma säännöstö tai yksityisten tallennusvälineiden käyttö on kielletty. Pääsy tietoihin ulkoisen huollon, etähuollon ja etätyön yhteydessä on säädelty sitovasti. Dokumentit ja tallennusvälineet hävitetään tietosuojaa noudattaen (esim. asiakirjasilppureilla, tietosuojasäiliöillä) luotettavissa jätehuoltoyrityksissä.

Rooli-/oikeusperiaate mukautetaan säännöllisesti muuttuviin organisaatiorakenteisiin (esim. uusilla rooleilla) ja kohdistetut roolit/oikeudet tarkistetaan säännöllisesti (esim. esimiesten toimesta), ja ne sovitetaan tai otetaan käytöstä tarvittaessa. Kohdistetut vakioprofiilit tarkistetaan säännöllisesti keskitetyillä tarkastuksilla. Muuttuvat

tapahtumat (kirjoittaminen, poistaminen) kirjataan lokiin, ja lokitiedostoja säilytetään sopivan ajanjakson verran (väh. 90 päivää) ja tarkistetaan (satunnaisesti).

Luovutusten varmistuksessa käytetään erilaisia vakiomenetelmiä:

Luovutuksista huolehtivat henkilöt tutustuvat ennalta sovellettaviin turvatoimiin. Vastaanottajat määritetään ennalta, niin että tarkastus (tunnistus) on mahdollista. Tietojen luovutuksen koko prosessi on määritetty ja dokumentoitu, ja konkreettisen luovutuksen suoritus kirjataan lokiin tai dokumentoidaan (esim. vastaanottovahvistuksella, kuittauksella). Luovutuksesta huolehtivat henkilöt tarkistavat ennalta, että tiedot ovat uskottavia, täydellisiä ja oikeita.

Ennen tietojen konkreettista luovutusta tarkistetaan vastaanottajan osoite (esim. sähköpostiosoite). Tiedot siirretään internetin kautta salattuina (esim. tiedoston salauksella). Luovutettujen tietojen integriteetti, mikäli mahdollista, varmistetaan allekirjoituksella (sähköisellä allekirjoituksella). Sähköiset vastaanottovahvistukset arkistoidaan sopivassa muodossa. E-toivotut tietojensiirrot internetissä estetään sopivalla tekniikalla (esim. Proxy, Palomuuri).

Tietojen erottaminen toisistaan on toteutettu seuraavilla vakiotoimenpiteillä:

Tietojen erottaminen toisistaan on säädelty sitovasti. Tiettyyn tarkoituksiin kerätyt tiedot tallennetaan erillään toisiin tarkoituksiin kerätyistä tiedoista. Käytetyt IT-järjestelmät mahdollistavat tietojen tallennuksen erikseen (useamman asiakkuuden ympäristössä tai pääsyperiaatteilla). Testi- ja tuotantojärjestelmät on erotettu toisistaan. Pseudonymisoitujen tietojen kohdalla jäljitettävyyden mahdollistavat digitaaliset avaimet tallennetaan tai säilytetään erikseen. Tehtävänkäsittelyssä tai toimintojen siirrossa eri toimeksiantajien tiedot käsitellään erikseen toimeksisaajalla. Rooli-/oikeusperiaatteet mahdollistavat käsiteltyjen tietojen loogisen erottamisen.

4. Integriteetin varmistaminen

Syöttöjen tallennuksessa käytetään erilaisia vakiomenetelmiä:

Pääsyoikeudet ja kaikki ylläpitäjän toimet kirjataan lokiin. Lokiin kirjataan kirjoitetut toimenpiteet (syötöt, muutokset, poistot) ja tietokenttiin tehdyt muutokset (esim. syötettyjen tai muutettujen tietojen sisältö). Lokiin kirjataan tietojen siirrot (esim. lataukset) ja sisäänkirjautumiset.

Käytetyt kirjausdokumentit kirjataan ja arkistoidaan syöttöjen seurattavuutta varten. Lokiin tallennetaan päivämäärä ja kellonaika, käyttäjä, toimenpide, sovellus ja tietueen järjestysnumero. Lokiasetukset dokumentoidaan.

Lokitiedot voidaan ainoastaan lukea. Lokitiedostoihin pääsevien määrä on rajoitettu (esim. ylläpitäjä, tietosuojavaltuutettu, tarkastaja). Lokitiedostoja säilytetään määritetyn ajanjakson verran (esim. 1 vuosi),

minkä jälkeen ne poistetaan tietosuojaa noudattaen. Lokitiedostot analysoidaan säännöllisesti automatisoidusti. Lokitiedostojen analyysit laaditaan mahdollisuuksien mukaan pseudonymisoituina.

5. Saatavuuden varmistaminen

Arkkitehtuuri on varmistettu tietojen häviämistä vastaan AWS-alustan sisäisillä replikointimekanismeilla. Lisäksi objektien varmistuksessa käytetään seuraavia AWS:n vakiotoimenpiteitä:

Käytössä on tulipalojen torjuntamenetelmiä (esim. palo-ovet, savunilmaisimet, paloseinät, tupakointikielto). Palvelimet on suojattu tulvilta (esim. palvelintila 1. kerroksessa, vedenilmaisin). Käytössä on menetelmiä tärinöiden ehkäisyyn (esim. palvelintila ei lähellä moottoriteitä, ratoja, konehuoneita). Palvelimet on suojattu sähkömagneettisia kenttiä vastaan (esim. teräslevyt ulkoseinissä). Käytössä on toimenpiteet vandalismia ja varkauksia vastaan (esim. kulunvalvonta). Palvelimet ovat ilmastoiduissa tiloissa (ilmastointi säätää lämpötilaa ja ilmankosteutta). Palvelimet on varmistettu ylijännitesuojalla ylijännitehuippuja vastaan. Käytössä on toimenpiteitä, jotka varmistavat vähähäiriöisen ja jatkuvan virransaannin (esim. katkottomalla tehonsyötöllä, hätävirtakoneistolla).

Tiedot varmistetaan säännöllisesti varmuuskopioilla AWS-alustassa. Varmuuskopioinnin periaatteet on dokumentoitu, ja ne tarkistetaan ja päivitetään säännöllisesti. Varmuuskopiot on suojattu luvattomalta pääsyltä. Käytetyt varmuuskopiointiohjelmat ovat nykyisten laatustandardien mukaisia, ja niitä päivitetään säännöllisesti. Käytettävissä on varapalvelinkeskus (kaukana käsittelypaikasta), jossa tietojen käsittely voi jatkua katastrofitilanteissa. Saatavuustarkastusten eri toimenpiteet on dokumentoitu AWS:n hätäsuunnitelmassa.

Ennen kuin toimeksianto tietojen käsittelyyn annetaan, toimeksisaaja tarkastetaan huolellisesti ja määritettyjen kriteerien mukaisesti (tekniset ja organisatoriset toimenpiteet). Sitä varten pyydetään ja tarkastetaan toimeksisaajan suorittamien teknisten/organisatoristen tietosuojatoimenpiteiden yksityiskohtainen kuvaus (kysymyksiin vastaaminen tai tietosuojaperiaatteet). Käsiteltyjen tietojen määrästä ja herkkyydestä riippuen tämä tarkastus voidaan tehdä myös toimeksisaajan tiloissa. Sopivat sertifioinnit (esim. ISO 27001) huomioidaan toimeksisaajien valinnassa. Toimeksisaajan sopivuuden toteaminen dokumentoidaan sopivassa ja ymmärrettävässä muodossa.

Toimeksiannon perusteeksi solmitaan tehtävänkäsittelysopimus toimeksiantajan ja toimeksisaajan välillä. Siinä määritetään yksityiskohtaisesti ja kirjallisesti molempien osapuolten vastuut, velvoitteet ja velvollisuudet. Mikäli toimeksiannon saaneen palveluntarjoajan toimipaikka on EU:n tai ETAn ulkopuolella, sovelletaan EU:n vakiosopimuslausekkeita. Sopimuksessa on määritetty, että toimeksisaajan suorittama tietojenkäsittely saa tapahtua ainoastaan toimeksiantajan ohjeistuksen mukaisesti. Toimeksisaaja on velvoitettu ilmoittamaan toimeksiantajalle välittömästi, jos toimeksiantajan antama ohjeistus on toimeksisaajan mielestä tietosuojasäädösten vastainen. Osallisten oikeuksien takaamiseksi tehtävänkäsittelysopimuksessa sovitaan, että toimeksisaajan on avustettava toimeksiantajaa kohtuullisella tavalla, sikäli kuin avustusta tarvitaan esimerkiksi osallisten tiedottamiseen.

Tehtävänkäsittelyn jatkovaiheessa toimeksiantaja tarkastaa toimeksisaajan työn tulokset muodon ja sisällön osalta. Toimeksisaajan teknisten ja organisatoristen toimenpiteiden noudattaminen tarkastetaan säännöllisesti. Siihen käytetään etupäässä ajankohtaisten testitietojen tai sopivien sertifiointien esittämistä tai todistetta suoritetuista IT-turvallisuus- tai tietosuojatarkastuksista. Alihankkijoita käytettäessä on myös sovittu, että nämä tarkastetaan samalla tavalla.

6. Järjestelmien kuormitettavuuden varmistaminen

AWS:n pilvipalvelun infrastruktuuri on yksi joustavimmista ja varmimmista pilvipalveluympäristöistä. Se on suunniteltu niin, että sen saatavuus on optimaalista, samalla kun asiakkaat erotetaan täydellisesti. Se on erittäin hyvin skaalattava, erittäin varmakäyttöinen alusta, jossa asiakkaat voivat jakaa sovelluksia ja sisältöjä nopeasti ja varmasti koko maailmassa. AWS-palvelut ovat sisällöstä riippumattomia siinä määrin, että ne tarjoavat kaikille asiakkaille saman turvallisuustason näiden sisällön tyypistä tai tallennettujen tietojen maantieteellisestä paikasta riippumatta.

Huipputurvalliset maailmanluokan AWS-keskukset käyttävät uusimman tekniikan mukaisia elektronisia valvontajärjestelmiä ja monitasoisia kulunvalvontajärjestelmiä. Palvelinkeskuksissa on vuorokauden ympäri koulutetut turvahenkilöt, ja kulkua valvotaan tiukasti vähimpien oikeuksien periaatteella, ja se sallitaan ainoastaan järjestelmän ylläpitoa varten.

7. Henkilötietojen saatavuuden palauttaminen fyysisen tai teknisen välikohtauksen jälkeen

AWS-palvelinkeskukset pystytetään klustereina maailman eri alueille. Kaikki palvelinkeskukset ovat verkossa ja palvelevat asiakkaita; yhtäkään palvelinkeskusta ei ole kytketty pois. Toimintahäiriössä automaattiset prosessit työntävät asiakastietojen lähetykset pois häiriöalueilta. Ydinsovellukset tarjotaan N+1-konfiguraatiossa, niin että palvelinkeskuksen toimintahäiriössä on riittävästi kapasiteettia jakamaan tietojen lähetyksen kuorma muihin toimipaikkoihin.

AWS tarjoaa joustavuuden käyttää instansseja ja tallentaa tietoja monilla maantieteellisillä alueilla sekä monilla saatavuusalueilla yhden alueen sisällä. Jokainen saatavuusalue on kehitetty riippumattomaksi toimintahäiriöalueeksi. Se tarkoittaa, että saatavuusalueet jaettu fyysisesti tyypillisen kaupunkialueen sisällä ja ovat esimerkiksi alueilla, joilla on vähäisempi tulvavaara (käytössä on tulva-alueiden erilaisia luokituksia alueesta riippuen). Itsenäisen katkottoman virransaannin ja paikallisten hätävirtakoneistojen lisäksi kaikki saatavuusalueet saavat virtaa riippumattomien sähkölaitosten sähköverkoista yksittäisten vikapaikkojen minimoimiseksi. Kaikki saatavuusalueet ovat redundantteja ja yhteydessä moniin Tier1-operaattoreihin.

Amazonin häiriöistä huolehtiva tiimi käyttää alalle tyypillistä diagnostiikkaa yrityskriittisten häiriöiden korjaamisessa. Käyttöhenkilöstö työskentelee kellon ympäri, seitsemän päivää viikossa ja 365 päivänä vuodessa havaitakseen häiriöt sekä hallitakseen niiden vaikutuksia ja korjauksia.

8. Teknisten ja organisatoristen toimenpiteiden vaikuttavuuden säännöllinen tarkastus, arviointi ja evaluointi

Yrityksen ohjesääntöjä ja ohjeita tai toteutettuja tietoturvallisuusstandardeja sovelletaan myös RIO-alustan käyttöönotossa ja toiminnassa. Yrityksessä on tietosuojasta ja -turvallisuudesta vastaavat toimet (tietosuojavastaava ja verkkoturva-asiamies). Työntekijät velvoitetaan vaitiolovelvollisuuteen ja heille tiedotetaan tietoturvallisuutta ja IT-turvallisuutta koskevista toimenpiteistä esitteillä, lehtisillä, intranetissä olevilla ohjeilla, jne.

Tarkastuksissa selvitetään, noudatetaanko sisäisissä prosesseissa tietoturvallisuutta ja tietosuojaa koskevia teknisiä toimenpiteitä.

Käsittelytoiminnot ja tietoturvallisuustoimenpiteet dokumentoidaan käsittelytapahtumien luettelossa. Toimenpiteiden vaikuttavuus tarkastetaan säännöllisesti (sisäisesti ja ulkoisesti).