Henkilötietojen käsittely FitnessBookerissa

21.5.2018

Tämän dokumentin tarkoitus on kuvata henkilötietojen käsittelyperiaatteet FitnessBooker-järjestelmää käytettäessä.

1. Terminologia

Tietojärjestelmä	FitnessBooker
Ohjelmistotoimittaja	Tooltip Oy
Liikuntakeskus	Tooltipin asiakas kuten liikuntakeskus.
Asiakas	Käyttää tietoärjestelmää ylläpito/back-office url:n kautta.
Henkilökunta	Liikuntakeskuksen henkilökunta, jolla pääsyoikeus tietojärjestelmään.
Loppukäyttäjä	Liikuntakeskuksen asiakas, joka käyttää palvelua esimerkiksi liikuntakeskuksen verkkosivujen kautta.

2. Asiakastietoihin pääsy

Tietojärjestelmässä säilytettäviä asiakastietoja pääsevät käsittelemään vain ne henkilöt, joilla on liikuntakeskuksen myöntämä käyttöoikeus asiakastietoihin. Ohjelmistotoimittajan edustajista asiakastietoihin on pääsy vain valituilla henkilöillä, jotka toimivat asiakasrajapinnassa. Pelkästään kehitystyöhön osallistuvilla henkilöillä on pääsy asiakasdataan ainoastaan niissä määrin ja siksi aikaa mitä mahdollisten tuotanto-ongelmien selvittely vaatii. Loppukäyttäjät näkevät ja voivat ylläpitää vain omia tietojaan. He eivät näe mitään tietoa toisistaan.

3. Tiedon käsittely, kerääminen ja luovuttaminen

Loppukäyttäjistä kerätään tietoa ja tallennetaan Henkilötiedot–kappaleen mukaisesti.

Tietoja kysytään asiakkaalta itseltään tai syötetään henkilökunnan toimesta. Ulkoisista tietolähteistä tietoa ei haeta, muutoin kuin mitä loppukäyttäjä on suostumuksensa antanut. Ulkoisesta lähteestä kautta saatua tietoa voi olla esimerkiksi Facebook -tunnuksien hyödyntämisen kautta tulevat tiedot loppukäyttäjästä.

Tietoja ei luovuteta kolmansille osapuolille kuin niissä määrin mitä asiakas on suostumuksen antanut tai liiketoiminnallisesti on tarpeellista. Liiketoiminnallisesti pakollisia ovat laskutus (osoitetiedot) ja yhteydenpito asiakkaaseen (sähköpostiosoite ja puhelinnumero tekstiviestien toimittamiseksi).

Liikuntakeskus vastaa toimenpiteistä, joilla varmistetaan, että järjestelmää käyttävät henkilöt ovat tietoisia henkilötietojen käsittelyyn liittyvistä ohjeista ja niiden noudattamisesta. Ohjelmistotoimittajan asiakaspalvelurajapinnassa toimivat henkilöt eivät muuta dataa ilman liikuntakeskuksen nimenomaista pyyntöä tehdä muutoksia. Ohjelmistotoimittaja käsittelee tietoa ainoastaan vikaselvittelyyn tai asiakkaan niin erikseen pyytäessä. Ohjelmistotoimittajan henkilökuntaa koskee vaitiolovelvollisuus kaikkea asiakasdataa kohtaan, joita he mahdollisesti näkevät tai käyttävät.

Mikäli liikuntakeskuksen palvelu sisältää videovalvonnan, siitä syntyvät videovalvontatallenteet liitetään kulunvalvontalokin perusteella loppukäyttäjään, jolloin voidaan tarvittaessa päätellä kuka loppuasiakas on kyseessä. Videovalvontatallenteisiin pääsy voi olla ainoastaan niillä liikuntakeskuksen henkilöillä, jotka muutoinkin tietojärjestelmää käyttävät. Tietojärjestelmässä olevien käyttövaltuuksien avulla voidaan erikseen rajata mitä asiakastietoa on henkilökunnan käytettävissä.

4. Fyysinen ja tekninen tietoturva sekä laadun varmistus

Kulunvalvontapalvelin ja/tai kulunvalvonnan ohjainyksikkö sijaitsee fyysisesti asiakkaan tiloissa. Mikäli palveluun kuuluu videovalvonta, se perustuu yleensä liiketunnistukseen ja tiedot tallennetaan samassa kiinteistössä olevalle kulunvalvontapalvelimelle tai verkkotallennusasemalle. Jatkuvaa videotallennusta ei pääsääntöisesti tehdä. Muuta kulunvalvontapalvelimelle tallennettavaa tietoa ovat muun muassa loppuasiakkaan kulkutunnisteen id, jonka avulla voidaan sallia tai estää asiakkaan kulkeminen ovista. Osassa liikuntakeskuksia kulunvalvontapalvelin on korvattu ovenohjauksyksiköllä, joka toimii samalla periaatteella kuin kulunvalvontapalvelin ovia ja/tai portteja ohjaten. Niin sanotut lokaalit laitteet ovat teknisesti sisäverkossa, joka on suojattu palomuurilla.

Täydelliset asiakastiedot ovat tallennettuina pilvipalvelussa. Pääsy ylläpito/back-office käyttöliittymälle on suojattu SSL-yhteydellä, mikäli liikuntakeskus on niin halunnut. Pilvi- ja kulunvalvontapalvelimen välillä tieto kulkee TLS-salattuna suljetussa virtuaaliverkossa (VPN). Tähän verkkoon pääsy on ainoastaan liikuntakeskuksella ja liikuntakeskus valvoo, että verkkoa eivät voi käyttää muut kuin liikuntakeskuksen oma henkilökunta. Data varmuuskopioidaan salattuna vähintään 1krt/vrk ja järjestelmän toimintaa monitoroidaan järjestelmän ylläpitäjien toimesta. Varmuuskopiot ovat fyysisesti Amazon Web Services -palvelussa

Irlannissa ja data on salattu GPG-tekniikalla. Konesalin tekninen ratkaisu on kahdennettu ja liikennettä ohjataan molemmille instansseille niin sanottujen käyttäjäpiikkien tapahtuessa (käytettävyyden varmistaminen). Operatiivinen tieto on fyysisesti Suomessa sijaitsevassa konesalissa. Palveluntarjoajana toimii Upcloud, joka on auditoitu Viestintäviraston toimesta esimerkiksi Oikeusministeriön käyttöön, ja konesali täyttää VAHTI-perustason vaatimukset. Tarkemmat Upcloudin tietoturvakäytännöt on kuvattu liitteessä "Upcloud GDPR Liite.odf". Fyysisen konesalivian sattuessa palvelutarjoaja vastaa palautustoimista. Mikäli tietoa katoaa - se voidaan palauttaa varmuuskopioista. Mahdollinen konesalivika ei aiheuta katkoksia kulunvalvonnassa. Kiireellisiin vikaselvittelyihin voidaan käyttää ohjelmistotoimittajan maanlaajuisesti toimivaa yhteistyökumppania.

Tuotekehityksen aikana vikasietoisuus todennetaan tarvittaessa poikkeustilanne- ja stressitestien avulla. Kehityksen aikana ohjelmiston laatu varmistetaan sekä automatisoitujen, että manuaalisten testitapausten avulla. Manuaalitestauksessa pääpaino on kokeilevalla (ad-hoc) testauksella. Tietojärjestelmä on tietoturvatestattu tietoturva-asiantuntijan toimesta.

Loppukäyttäjä on velvollinen huolehtimaan käyttäjätunnuksistaan ja salasanoistaan, sekä oman päätelaitteensa ja/tai työasemansa ohjelmistojen tietoturvasta. Salasanat tallennetaan salattuna käyttäen kryptografisia tiivistefunktioita.

5. Virhetilanteista toipuminen

Tietojärjestelmässä olevan tiedon tuhoutuessa se voidaan palauttaa edellisen päivän tilanteeseen varmuuskopiosta. Mikäli asiakkaan ylläpito/back-office -tunnukset päätyvät tai niiden epäillään päätyneen väärien henkilöiden käyttöön, voidaan tunnukset poistaa käytöstä, ja tarvittaessa järjestelmän lokitiedostoista voidaan päätellä aiheutunut vahinko sekä suorittaa tarvittavat palautustoimet. Liikuntakeskus on velvollinen ilmoittamaan viipymättä ohjelmistotoimittajalle, mikäli epäillään tunnusten joutuneen ulkopuolisten henkilöiden tietoisuuteen.

6. Henkilötiedot

Kuvaus	Arvo/tietotyyppi	Tarkoitus
Asiakkuustyyppi	kuluttaja tai yritys	Tekniset laskun toimitustapaan liittyvät syyt, tilastointi liiketoiminnan kehittämistä ja seurantaa varten.
Etunimi	txt	Vain kuluttaja-asiakkaat.
Sukunimi	txt	Vain kuluttaja-asiakkaat.
Yrityksen nimi	txt	Vain yritysasiakkaat.
Y-tunnus	txt	Vain yritysasiakkaat.
Syntymäaika	pp.kk.vvvv. HeTun loppuosaa ei tallenneta.	Vain kuluttaja-asiakkaat.
Sukupuoli	Mies, Nainen, Ei määritelty	Vain kuluttaja-asiakkaat.
Profiilikuva	kuvatiedosto	Asiakkaan tunnistaminen.
Hintaryhmä	Liikuntakeskuksen määrittelemät vaihtoehdot. Dynaaminen lista.	Tuotteiden hinnoittelu, tilastointi.
Sähköposti	txt	Asiakkaan kontaktointi, ryhmäliikuntatuntimuutoksista ilmoittaminen, asiakkaan käyttäjätunnus oma profiiliin, vaaditaan ryhmäliikuntapaikan varaamiseen. a)
Salasana	Salattuna tietokannassa	Salasana asiakkaan oma profiliin.
Puhelinnumero	txt	Asiakkaan kontaktointi. SMS -ilmoitukset.
Lähiosoite	txt	Kontaktointi. Laskun toimitusosoite.
Postinumero	txt	Kontaktointi. Laskun toimitusosoite.
Postitoimipaikka	txt	Kontaktointi. Laskun toimitusosoite.
Kulkutunnisteen id	txt	Kulunvalvonta.
Jäsynyyden tyyppi	aika / kerta	Laskutus, asiakkuuden hoito, kulunvalvonta
Jäsenyyden alkamispvm	pvm	Laskutus, asiakkuuden hoito, kulunvalvonta
Jäsenyyden päättymispvm	pvm / toistaiseksi	Laskutus, asiakkuuden hoito, kulunvalvonta
Sähköpostimarkkinointi	sallittu / kielletty	Asiakkuuden hoito ja kontaktointi.
Tekstiviestimarkkinointi	sallittu / kielletty	Asiakkuuden hoito ja kontaktointi.
Laskun toimitustapa	ei lähetetä, email, kirje, e-lasku	Laskun toimitustapa määräytyy asiakkaan itse tai henkilökunnan asettamana tai kolmannen osapuolen palvelusta saatuna (laskutusoperaattori välittää tiedon mikäli asiakas on aktivoinut e-laskutuksen).
Tilitysviite	txt	Millä kustannuspaikkaviitteellä kyseisen asiakkaan maksut tilittyvät Ropo tilitykseen.
Laskutussähköpostiosoite	txt	Erikseen määritelty sähköpostiosoite johon sähköpostitse toimitettavat laskut lähetetään.
Laskun saaja	txt	Erikseen määritelty laskutettava.
Laskutuslähiosoite	txt	Erikseen määritelty laskutuksen lähiosoite.
Laskutuspostinumero	txt	Erikseen määritelty laskutuksen postinumero.
Laskutustoimipaikka	txt	Erikseen määritelty laskutuksen toimipaikka.
Asiakasmerkinnät	txt	Vapaata liikuntakeskuksen syöttämää tekstiä asiakkuuden hoitamisesta.
Asiakasmerkinnät - sisäinen	txt	Vapaata liikuntakeskuksen syöttämää tekstiä asiakkuuden hoitamisesta.
Asiakkaan laskut, laskutushistoria, laskujen tilat	0 - n kpl	Sisältää järjestelmän kautta asiakkaalle luodut avoimet laskut seuraavilla tiedoilla; luontipäivä, tila (avoin, keskeytetty, lähetetty, maksettu käteisellä, maksettu tilisiirtona, muistutus, muu, perintä, vajaa suoritus, virheelliset tiedot), eräpäivä, eräajopäivä, laskun rivit (tuote id, selite,

		määrä, veroton euromäärä, alv-kanta, verollinen euromäärä, loppusumma). Koskee vain niitä liikuntakeskuksia, jotka käyttävät laskutusta ja vain niitä laskuja, jotka ovat muodostuneet järjestelmän luomina.
Asiakkaan ilmoittautumistieto tunnille tai tapahtumaan	Saapunut paikalle Kyllä/Ei	Palveluihin etukäteen ilmoittautuneiden lkm, käyttöaste, muutoksista informoiminen.
Asiakkaan kulku kulkuvalvonvonnan alaisesta ovesta tai portista	aikaleima	Asiakkaan yksiöivä tieto kulkutunnisteesta. Väärinkäytös- ja epäselvien tilanteiden selvittäminen.
Asiakkaan kulku kulunvalvonnan kosketusnäytön kautta	aikaleima	Asiakkaan yksiöivä tieto kulkutunnisteesta. Väärinkäytös- ja epäselvien tilanteiden selvittäminen. Ryhmäliikuntatuntien hallinta.
Asiakkaan tiedot: tietojen lisäys	txt	Kuka syötti asiakastiedot, ajankohta, mitä tietoa syötettiin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: tietojen muokkaus	txt	Milloin ja mikä tuote on myyty asiakkaalle. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: yhteystietojen muokkaus	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: laskutustietojen muokkaus	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: jäsen-/asiakkuustietojen muokkaus	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Mahdollisten duplikaattitilien yhdistäminen	txt	Mitkä tiedot on yhdistetty, kuka yhdistänyt. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskun lisäys	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskun muokkaus	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskun poisto	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskun yhdistäminen toiseen laskuun	txt	Mitkä laskut ja laskurivit on yhdistetty. Kuka toiminnon suoritti ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskun jakaminen	txt	Mi(t)kä lasku(t) on jaettu. Kenelle uudet laskut kohdistuu. Kuka toiminnon suoritti ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskurivien/hyvitysrivien lisäys	txt	Kuka on lisännyt laskurivin ja millä arvoilla. Sisältää myös järjestelmän lisäämät laskurivit, esim laskutuslisä kirjelaskuille. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskurivien poisto	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskun tilan vaihto	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskumallin lisäys	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskumallin lisäys	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskumallin muokkaus	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskumallin poisto	txt	Mitä tietoa on muutettu/lisätty/poistettu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Tuotteen myynti	txt	Kuka myi tuotteen, tuote, pvm tiedot, hinta, maksutapa, muodostetut laskut. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Ryhmäliikuntavarauksen lisäys	txt	Kuka teki, milloin ja mille tunnille. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Ryhmäliikuntakäynnin kirjaaminen	txt	Kuka teki, milloin ja mikä tunti oli kyseessä. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Ryhmäliikuntavarauksen poistaminen	txt	Kuka teki, milloin ja mikä tunti oli kyseessä. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Sähköpostin lähetys	txt	Viestin lähettäjä, aikaleima ja viestin sisältö. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Tekstiviestin lähetys	txt	Viestin lähettäjä, aikaleima ja viestin sisältö. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Tuotteen osto verkkokaupasta	txt	Kuka teki toiminnon, tuote, pvm tiedot, hinta, maksutapa, muodostetut laskut. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Asiakkuuden päättäminen	txt	Kuka teki toiminnon, milloin ja mistä päivästä lukien muutos astuu voimaan. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Asiakasmerkinnän lisäys	txt	Merkinnän sisältö, tekijä ja aikaleima. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Asiakasmerkinnän muokkaus	txt	Miten merkintää on muokattu, kenen toimesta ja milloin. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Asiakasmerkinnän poisto	txt	Merkinnän sisältö ja kuka merkinnän poisti sekä aikaleima. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Asiakkaan tilan muokkaus	txt	Merkinnän sisältö ja kuka merkintää muokkasi sekä aikaleima. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Asiakkaan salasanan vaihto	txt	Kuka muutti ja milloin. Salasanaa ei näytetä. Epäselvien tilanteiden selvittäminen.

Asiakkaan tiedot: Kuntosalikäynnin manuaalinen lisäys	txt	Kuka kirjauksen lisäsi ja aikaleima. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Laskun tila	txt	Ilmaisee laskutusoperaattoria käytettäessä laskun tilatiedon. Epäselvien tilanteiden selvittäminen.
Lunastamattomien varausten lunastus	txt	Kuka kirjannut? Milloin? Mikä tuntikyseessä? Asiakastietojen ylläpito.
Pankkiyhteystietojen muutokset	txt	Ei käytössä.
Asiakkaan tiedot: Tili lukittumistieto	txt	Ilmaisee jos asiakastili on lukittu lunastamattomista varauksista johtuen. Vain mikäli toiminto on käytössä. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Väärinkäytösepäily	txt	Kirjataan mikäli kulunvalvontalokista löytyy merkintä, mutta vastaavaa kirjausmerkintää ei kosketusnäytöllä näy. Edellyttää, että toiminto on käytössä. Epäselvien tilanteiden selvittäminen.
Asiakkaan tiedot: Päätöstoimenpiteiden poisto	txt	Mikäli tuotteeseen liitetty päätöstoimenpide on poistettu asiakkaalta. Epäselvien tilanteiden selvittäminen.
Lokimerkintä kulunvalvonnassa	txt	Aikaleima, kulkutunnisteen tiedot. Epäselvien tilanteiden selvittäminen.
Kosketusnäytön ohjaus	txt	Alkavat ryhmäliikuntatunnit ja niille ilmoittautuneet asiakkaat. Synkronointi pilvestä kosketusnäytölle (ja toisinpäin). Kosketusnäytön sujuva toiminta.
Tallenne	videotallenne	Liiketunnistukseen perustuva videotallenne. Pseudonymisoitu tieto eli tallenne ei sisällä faktuaalista tietoa kuka asiakas on kyseessä. Kulunvalvontalokitietoon yhdistämällä voidaan päätellä kuka asiakas on kyseessä. Epäselvien tilanteiden selvittäminen.
Kosketusnäytön loki-tiedosto, tunniste-id, nimi	txt	Epäselvien tilanteiden selvittely.
AccessManagement loki-tiedosto, tunniste-id, nimi	txt	Kulunvalvonnan luotettava toiminta ja epäselvien tilanteiden selvittely.
Loppuasiakkaan IP-osoite	txt	Lokitieto IP -osoitteista. Palvelimen lokitieto.

6. Liitteet

FiBo GDPR - Henkilötiedot laaja.pdf	Henkilötietojen laaja kuvaus.
Upcloud GDPR Liite.pdf	Upcloud palveluntarjoajan liite.