TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Marek Kesküll

RAAMISTIK ANDMEBAASIDE MODELLEERIMISEKS VASTAVALT ISIKUANDMETE KAITSE ÜLDMÄÄRUSE NÕUETELE

Bakalaureusetöö

Juhendaja: Mart Roost
Magister

Tallinn 2019

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Marek Kesküll

20.05.2019

Annotatsioon

Lõputöö põhieesmärgiks oli analüüsida isikuandmete kaitse üldmäärusest tulenevaid subjekti õiguseid ning nendest tulenevaid protsesse ning luua raamistik uute andmebaaside modelleerimiseks vastavalt isikuandmete kaitse üldmääruse nõuetele.

Täna kannatavad andmetöötlejad selle all, kuidas leida üles süsteemidest isikuandmed, millele saab isik rakendada enda õiguseid ning murravad pead, kuidas korraldada andmetöötluse kaardistus vähese vaevaga. Antud hetkel puudub põhjalik ülevaade, kuidas peaksid olema organisatsioonide baasid modelleeritud vastavalt uute nõuete valguses.

Lõputöö tulemuseks on vastutavale töötlejale isikute poolt rakendatud õiguste vastuvõtmiseks ja täitmise korraldamiseks loodud raamistik, mis oleks aluseks ettevõtete infosüsteemide kohaldamisel uute isikuandmete töötlemise nõuete valguses.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 29 leheküljel, 7 peatükki, 14 joonist, 1 tabelit.

Abstract

A Framework For Modeling Databases According To The Requirements Of The General Data Protection Regulation

The main objective of the thesis was to analyze the subject's rights under the General Data Protection Regulation and the resulting processes, and to create a framework for modeling new databases according to the requirements of the General Data Protection Regulation.

Today, data controllers suffer from finding personal information from systems or databases that a person can apply to his / her own rights and also they don’t know how to map data processing with little effort. At this point, there is no comprehensive overview of how organizations' bases should be modeled in the light of new requirements.

The result of the thesis is a framework created for the data controller to receive and execute the rights implemented by the data subjects, which would serve as a basis for the enterprise information systems in the light of the new personal data processing requirements.
The thesis is in Estonian and contains 29 pages of text, 7 chapters, 15 figures, 1 tables.

Lühendite ja mõistete sõnastik

UML	Ühtne modelleerimiskeel[1]
Enterprise Architect	Modelleerimise tarkvara[2]
RUP	Iteratiivne tarkvaraarendus protsess[3]
UP	Iteratiivne ja inkrementaalne tarkvaraarendus protsess[4]
OO	Objekt-orienteeritud[5]
GDPR	Isikuandmete kaitse üldmäärus[6]
Andmesubjekt	Isik, kelle andmeid töödeldakse.

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Euroopa Liidu ja Eesti andmekaitseõigus uuenes 25.mai 2018. Alates sellest kuupäevast rakendatakse isikuandmete kaitse üldmäärust(*GDPR*). Isikuandmete kaitse üldmäärus rakendub väga paljudele ettevõtetele, kes töötlevad füüsilise isiku andmeid. GDPR lisas juurde nõudeid, mille järgi ettevõtted peavad oma süsteeme kohaldama. Määruse eesmärk on suurendada inimeste kindlustunnet, et nende kohta käivat andmehulka kasutatakse turvaliselt ning korrektselt. [6, lk 4]

Täna kannatavad andmetöötlejad selle all, kuidas leida üles süsteemidest/andmekogudest isikuandmed, milledele saab isik rakendada enda õiguseid ning murravad pead, kuidas korraldada andmetöötluse kaardistus vähese vaevaga.

Antud hetkel puudub põhjalik ülevaade, kuidas peaksid olema organisatsioonide baasid modelleeritud vastavalt uute nõuete valguses. Lõputöö eesmärgiks on analüüsida olemasolevat isikuandmete kaitse üldmäärust ning vastavalt sellele luua raamistik uute andmebaaside modelleerimiseks vastavalt isikuandmete kaitse üldmääruse nõuetele.

Töös käsitletud raamistik on vastutavale töötlejale isikute poolt rakendatud õiguste vastuvõtmiseks ja täitmise korraldamiseks.

1.1 Ülesande püstitus

Antud töö eesmärgid:

1. Luua raamistik uute süsteemide modelleerimiseks GDPR valguses.

    1.1. Koostada andmekaitse üldmääruse teksti analüüsides vastava valdkonna sõnastik ning tähtsamad toimimistaseme mudelid.

    1.2. Viia läbi andmesubjekti nõuete analüüs.

    1.3. Modelleerida raamistiku lahendus toetudes andmesubjekti nõuetele ning Fowleri osapoole mustrile.

    1.4. Hinnata loodud lahendust nõuete suhtes.

1.2 Metoodika

Käesoleva projekti eesmärkide saavutamiseks uuritakse olemasolevat uut isikuandmete üldmäärust, et saada põhjalik ülevaade selle toimimisest ja osadest. Defineerime, milline on süsteem kasutaja vaatepunktist hetkel.

Olemasolevaid nõudeid arvestades, modelleeritakse uus lahendus, mida hakatakse detailsemalt analüüsima.

Hinnatakse loodud lahendust: valideeritakse seadusest tulenevaid nõudeid.

Järgnevas peatükis käsitletakse töös kasutatud metoodikat täpsemalt.

2 Kasutatud metoodika

Käesolevas peatükis esitatakse süsteemi tutvustus ning kirjeldatakse tehnikaid, millele antud lõputöö toetus.

2.1 Süsteemi tutvustus

Ärisüsteemiks on isikuandmetega töötlemine, täpsemalt üldmäärusega kehtestatud subjekti õigustega seotud teenuste komplekt, mida teenusepakkuja peab võimaldama subjektile.

2.1.1 Tarkvara ja lühikirjeldus

Tarkvaraks on teenusepakkujale orienteeritud raamistik, mis võimaldab täita isikuandmete üldmäärusest tulenevad nõudeid. Lõputöö ühe põhitulemusena püstitatakse funktsionaalsed nõuded sellele tarkvarale.

2.2 Ärimodelleerimise tehnika

Isikuandmete üldmääruse teksti analüüsiti kasutades Zachman'i[7] tugiraamistikku.

Zachmani raamistik pakub võimaluse arhitektuurimudelite klassifitseerimiseks. Põhiidee seisneb selles, et raamistik loob võimaluse süsteemi iga üksiku aspekti süsteemseks kirjeldamiseks koordineerituna kõigi teiste aspektidega. [7]

Zachman'i raamistikku kirjeldab järgmine tabel:

Tasand	**MIS** Andmed	**KUIDAS** Funktsioonid	**KUS** Paiknemine, võrk	**KES** Inimesed	**MILLAL** Aeg	**MIKS** Motivatsioon
Planeerija vaade	Oluliste mõistete ja objektide loend	Põhiliste toimimis-protsesside loend	Organisatsiooni eri üksuste asukohad	Võtmerühmad, töötajate loend	Olulisemate Sündmuste loend	Toimimis-eesmärgid ja -strateegiad
Omaniku vaade	Kontseptuaalne andmemudel	Toimimisprotsessi de mudel	Logistika skeem	Töövoog, töötajate vastutused (*workflow*)	Protsesside stsenaariumid (master *plan*)	Toimimisplaan (äriplaan)
Projekteerija vaade	Loogiline andmemudel (ERD)	Rakenduste arhitektuur	Hajussüsteemi arhitektuur	Kasutajaliides-te arhitektuur	Protsesside struktuur	Toimimisreeglite mudelid
Ehitaja vaade	Füüsiline andmemudel	Süsteemi projekt (spetsifikatsioon)	Tehnoloogia arhitektuur	Kasutajaliides-te disain	Juhtimis-struktuur	Toimimisreeglite disain
Alltöövõtja vaade	Andmete struktuuri Kirjeldus	Programmi disain	Võrgu-arhitektuur	Turbe arhitektuur, kasutajaõigu-sed	Ajalise seotuse määratlus	Toimimisreeglite spetsifikatsioon
Toimiv organisatsioon	Tegelikud andmed	Programmi kood	Võrk, süsteemide paiknemine	Pädevad töötajad	Tegevustsüklid	Rakendatud toimimisreeglid

Tabel 1. Zachman'i tugiraamistik [7]

Antud töös kasutatakse põhiliselt esimese kahe taseme vaadet valdkonna ärisõnastiku loetelude ning osaliselt ka valdkonna mudelite koostamiseks.

2.3 Süsteemianalüüs

Süsteemianalüüsi eesmärgiks käesolevas töös on saada aru isikuandmete töötlemise valdkonnast ning seejärel püstitada funktsionaalsed nõuded tarkvarale.

Süsteemianalüüs hõlmab seega ärimodelleerimist ja tarkvara nõuete analüüsi.

Ärimodelleerimise tähtsaimaks tulemiks isikuandmete töötlemise teemas on domeenimudel, mis on sarnane kontseptuaalsele andmemudelile, mistõttu teda saab kindlate reeglite alusel teisendada andmebaasiskeemiks.

UP (ja RUP) kontekstis me nimetame domeeni mudeliks kontseptuaalsete klassidiagrammide vormis staatilist esitust valdkonna objektmudelist. [3][4]

Domeeni mudel[8] on:

• inspiratsiooni allikas tarkvara objektide disainile.

• kõige tähtsam artefakt, mis luuakse OO (objekt-orienteeritud) analüüsis.

• reaalse maailma mõistete (kontseptuaalsete klasside), mitte tarkvara komponentide ja

nende vastutuste, visuaalne esitus.

• Visuaalne abstraktsioonide sõnastik.

Töös kasutatakse graafilise modelleerimise tarkvara Enterprise Architect (EA), mis toetab erinevaid notatsioone, standardeid ja tehnoloogiaid. [2]

EA-d kasutatakse töös peamiselt analüüsi taseme UML diagrammide koostamiseks.

2.4 Organisatsiooni isikutega analüüsimustrid

Domeenimudeli koostamisel on sageli abiks ekspertide poolt loodud analüüsimustrid. Antud töös kasutatakse Fowler'i mustreid, mis abistavad organisatsiooni struktuuri ja isikkoosseisu informatsiooni modelleerimist.
Martin Fowler'i raamatus on analüüsimuster defineeritud järgnevalt – analüüsimuster on grupp kontsepte, mis esindavad ühest ülesehitust ärimodelleerimises. See võib olla relevantne ühele domeenile, kuid see võib laieneda ka mitmele domeenile. Selle definitsiooni ja ka käesoleva töö mõistes kirjeldavad analüüsimustrid võimaliku süsteemi funktsioone ja sellest tulenevaid protsesse. [9, lk. 23]

Muster on nimega kirjeldus, milles on esitatud probleem ja lahendus sellele probleemile. Samuti on kirjeldatud, millal seda lahendust rakendada ja kuidas rakendada lahendust uues kontekstis. [10, lk. 23]

Mustritest võib mõelda, kui struktuurse kirjutamise viisist, mille abil kirjeldatakse probleem selle lahendus ning hulgaliselt täiendavat taustinformatsiooni, mis aitab seda lahendust efektiivselt kasutada. [11]

Meszaros ja Doble [12] kirjeldavad tüüpilise mustri osi järgnevalt:

- Nimi, mis on meeldejääv ja iseloomustab mingil viisil mustri poolt edasi antavaid teadmisi.

- Kontekst, milles kirjeldatakse situatsioon, kus probleem ilmneb.

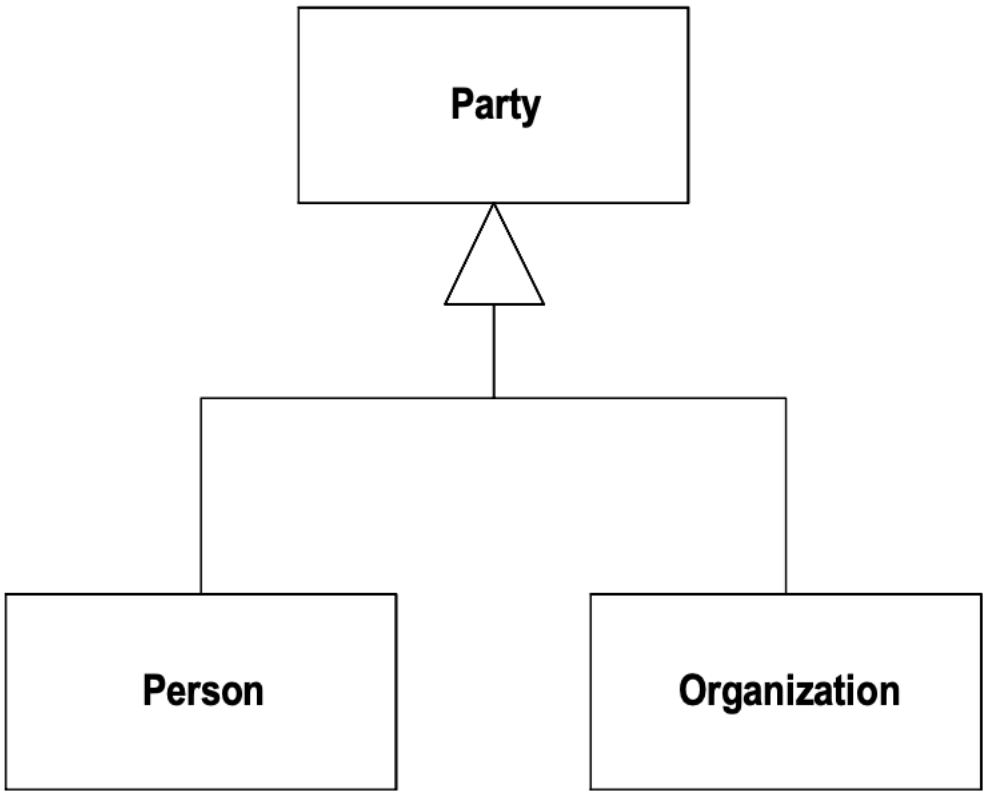
- Probleemi püstitus.

- Jõud, mis mõjutavad probleemile lahenduse valimist.

- Lahendus probleemile, mis arvestab erinevate jõududega ja on antud kontekstis sobiv.

2.5 Osapool

Osapool on keegi või miski, mis osaleb protsessides süsteemis. Kõige tavalisem juhtum, kus kasutada osapoolt on siis, kui on olemas inimesed ja organisatsioonid mudelis ja me näeme üldkasutatavat käitumist. [13, lk. 6]



Joonis 1. Osapoole muster [13, lk. 5].

3 Tehtud töö

Käesolevas peatükis analüüsitakse isikuandmete töötlemise üldmäärust ning toetudes sellele luuakse valdkonna sõnastik. Järgnevalt koostatakse tähtsamad toimimistaseme mudelid ja modelleeritakse raamistiku lahendus toetudes Fowleri osapoole mustrile.

3.1 Valdkonna sõnastik

Antud peatükis analüüsitakse andmekaitse inspektsiooni koostatud isikuandmete töötlemise üldmäärust, mis selgitab ning kirjeldab määruse üksikuid aspekte. Peatükis on välja toodud ainult uute nõuetega seotud aspektid, kuna terve üldmääruse analüüsi maht oleks liiga suur, et lõputöö sisus seda kajastada.

Sõnastikus on esitatud valdkonna objektid, protsessid, asukohad, tegutsejad, sündmused ning eesmärgid. Üldmääruse sõnastik on loodud Zachman'i tugiraamistiku veergude alusel.

3.1.1 Objektid

Peatükis on välja toodud tähtsamad objektid, mis on osa süsteemist.

- Isikuandmed
- Ettevõte/asutus
- Karistus
    - Rahatrahv
    - Noomitus
- Dokument(üldmäärus)
- Euroopa parlament(hoiab dokumente)
- Nõuded isikuandmete töötlemisele
- Isikuandmete töötlemise põhimõtted
- Järelevalveasutus
- Süsteem
- Isik
    - Klient
    - Andmesubjekt
- Kaebus
- Hüvitis
- Teavitus

3.1.2 Protsessid

Peatükis on välja toodud protsessid, mida sooritab isik või sooritatakse isikuga.

- Nõuete vastu eksimise ennetamine
    - Järelevalveasutuse poolt jälgimine
    - Ettevõtete/organisatsioonide teavitamine uuest üldmäärusest
- Andmete ülekandmine
    - Andmesubjekti õigus saada teda puudutavaid isikuandmeid struktureeritud, üldkasutatavas vormingus ning masinloetavas kujus
    - Füüsilise isiku nõudmisel teisaldamine ühest süsteemist teise
- Vastutava töötleja Teavituskohustus
    - Kohustus teatada isikuandmete parandamisest, kustutamisest või isikuandmete töötlemise piiramisest
    - Isiku õiguseid ja vabadusi kahjustada võivatest infoturbeintsidentidest tuleb teavitada isikut kui ka järelevalveasutust
- Isikuandmete töötlemine
    - Andmed, mida saab töödelda ainult isiku nõusoleku alusel
    - Andmed, mida isik saab pärida enda kohta
    - Isik võib nõuda andmete kustutamist. Ka viivitamatult, kui:
        - Isikuandmeid ei ole vaja enam sellel eesmärgil, millega seoses need koguti
        - Andmesubjekt võtab töötlemiseks antud nõusoleku tagasi
        - Andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes
        - Ebaseaduslik töötlemine
        - Isikuandmeid koguti infoühiskonna teenuste pakkumise jaoks
- Karistuse määramine
    - Rahatrahv
    - Noomitus
- Karistuse vaidlustamine
    - Menetluse lahendamine järelevalveasutuse poolt(sh ka Andmekaitsenõukogu otsus)
- Karistuse täideviimine
    - Kuni neli protsenti ettevõtte eelmise aasta ülemaailmsest käibest või kuni 20 miljonit eurot rahatrahvi
    - Noomituse tegemine
- Kohustus Isikut teavitada andmete töötlemisest
    - Isik võib keelduda andmete töötlemisest
- Isikuandmete krüpteerimine
- Andmesubjekti õigus esitada vastuväiteid töötlemise kohta igal ajal
- Andmesubjekti õigus andmete parandamisele
    - Esitada õiend
- Isikuandmete töötlemise piiramine
    - Kui andmesubjekt vaidlustab isikuandmete õigsuse
    - Ebaseaduslik töötlemine
    - Vastutav töötleja ei vaja isikuandmeid enam töötlemise eesmärkidel
    - Andmesubjekt on esitanud vastuväite töötlemise suhtes
- Vastutav töötleja tagab määrusega kooskõlas töötlemise
- Pseudonümiseerimine

- Isikuandmete registreerimine
- Isikuandmete kättesaadavuse taastamine
- Andmekaitseametnik teavitab vastutavat töötlejat seoses nende kohustustega

3.1.3 Asukohad

Peatükis on välja toodud asukohad, kus toimuvad protsessid.

- Ettevõte/organisatsioon(kes tegeleb andmetöötlusega)
- Teenusepakkuja
- Muu asukoht

3.1.4 Tegutsejad

Peatükis on välja toodud tegutsejad, kes tegelevad protsessidega.

- Andmesubjekt
- Andmetöötleja
    - Vastutav töötleja
    - Volitatud töötleja
    - Alltöövõtja
- Järelevalveasutus
- Andmekaitsenõukogu
- Andmekaitseametnik

3.1.5 Sündmused

Peatükis on välja toodud peamised sündmused, mis käivitavad protsesse.

- Andmetöötleja soovib isikuandmeid töödelda
- Andmetöötlejal on isikuandmed ning soovib seda lisada süsteemi
- Andmetöötlejal on isikuandmed ja soovib neid säilitada
- Subjekt annab nõusoleku isikuandmete töötlemiseks
- Subjekt soovib isikuandmeid üle kanda
- Subjekt soovib isikuandmeid unustada
- Subjekt soovib isikuandmete töötlemist piirata
- Subjekt soovib isikuandmeid pärida

3.1.6 Eesmärgid

Peatükis on välja toodud isikuandmete kaitse üldmääruse eesmärgid.

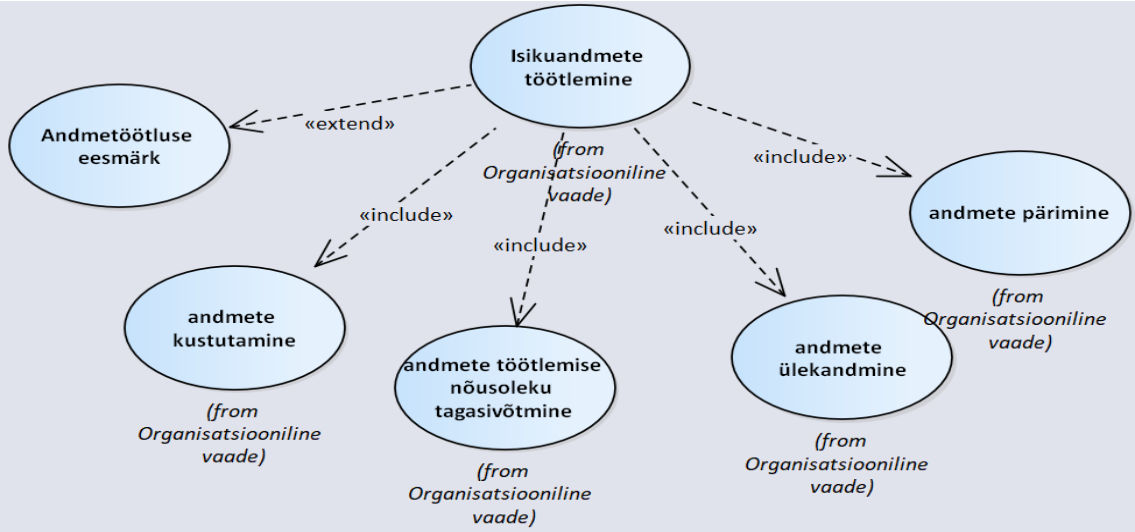
- Ennetada nõuete vastu rikkumist
- Töödelda isikuandmeid vastavalt seadusele
- Suurendada turvatunnet subjekti suhtes andmete töötlemisel

3.2 Valdkonna mudelid

Valdkonna kohta on koostatud protsessi vaate struktuur ehk katusprotsess ning tema alamprotsessid; nii kliendipoolsed kui ka automaatprotsesside kasutusjuhtude lühiformaadid; objektide/info kohta kontseptuaalne klassidiagramm; täpsustatud konstseptuaalne klassidiagramm koos osapoole analüüsimustriga.

3.2.1 Protsesside struktuur

Järgneval (äri)kasutusjuhtude diagrammil tuuakse välja antud töös detailsemalt analüüsitud äriprotsesside struktuur, mis hõlmab ka tarkvara (2.1) kasutusjuhtusid.



Joonis 2. Protsesside struktuuri diagramm

Sellise diagrammi alusel saame struktuuri erinevate konkreetsete kihtide ja elementide täpsustamiseks koostada kasutusjuhtude lühiformaadid.

3.2.2 Tarkvara kasutusjuhtude lühiformaadis kirjeldus

Antud peatükis tuuakse välja prioriteetsemate kasutusjuhtude lühikirjeldused.

Andmete kustutamise nõudmine:

Joonis 3. Andmete kustutamise nõudmise kasutusjuht

Andmete kustutamise nõudmine: Klient nõuab olemasolevate isikuandmete kustutamist. Klient on andnud nõusoleku oma andmeid töödelda. Andmesubjekt esitab taotluse elektroonselt teenusepakkujale. Taotluse tekitamiseks klient vajutab teenusepakkuja lehel/süsteemis nuppu "kustuta" või "kustuta andmed", mis algatab tarkvarasüsteemis andmete kustutamise protsessi.

Kliendi e-mailile saadetakse teenuse poolt kinnituskiri ning klient peab kinnitama andmete kustutamise nõudmise.

Andmetöötlejal on üks kalendrikuu aega vastata taotlusele. Vastutav töötleja on kohustatud kustutama isikuandmed põhjendamatu viivituseta, kui kehtib üks järgmistest asjaoludest:

a) isikuandmeid ei ole enam vaja sellel eesmärgil, millega seoses need on kogutud või muul viisil töödeldud.

b) andmesubjekt võtab töötlemiseks antud nõusoleku tagasi ning puudub muu õiguslik alus isikuandmete töötlemiseks.

c) andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes ja töötlemiseks pole ülekaalukaid õiguspäraseid põhjuseid või andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes.

d) isikuandmeid on töödeldud ebaseaduslikult.

e) isikuandmed tuleb kustutada selleks, et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega ette nähtud juriidilist kohustust.

f) isikuandmeid koguti seoses infoühiskonna teenuste pakkumisega. [6, artikkel 17]

Töötleja teavitab klienti andmete kustutamise rahuldamisest või mitterahuldamisest.

Põhiline edukas stsenaarium: Klient nõuab vastavalt oma õigustele andmete kustutamist, mille ta on esitanud. Kliendi soov rahuldatakse viivitamatult ning saadetakse teavitus andmete kustutamisest. Kliendi andmeid ei eksisteeri enam teenusepakkuja süsteemis.

Alternatiivsed stsenaariumid:

Kliendi nõudmist ei rahuldata: teavitatakse klienti ning põhjendatakse, miks ei ole võimalik nõudmist rahuldada.

Kliendi nõudmist ei rahuldata kalendrikuu jooksul: töötleja poolt on võimalik pikendada seda aega kahe kuu võrra, kui tegemist on keeruka andmehulgaga. Kui ei pikendata, siis töötleja esitab põhjused ning selgitab talle võimalust esitada kaebust järelvalveasutusele. [6, 59. punkt]

Andmete ülekandmise nõudmine:

Joonis 4. Andmete ülekandmise nõudmise kasutusjuht

Andmete ülekandmise nõudmine: Klient nõuab olemasolevate andmete ülekandmist. Subjekt esitab ülekandmise nõude teenusepakkuja lehel/süsteemis vajutades nupule "Ekspordi andmeid", mis algatab tarkvarasüsteemis andmete ülekandmise protsessi. Kliendile näidatakse isikuandmeid ning antakse võimalus need alla laadida.

Vastutav töötleja esitab andmed üldkasutatavas vormingus ning masinloetaval kujul. Klienti teavitatakse andmete edukast eksportimisest.

Põhiline edukas stsenaarium: Klient nõuab isikuandmete ülekandmist teisele töötlejale. Vastutav töötleja esitab andmed masinloetaval kujul. Klient näeb oma isikuandmeid ning laeb alla masinloetaval kujul. Klienti teavitatakse andmete eksportimisest.

Alternatiivsed stsenaariumid:

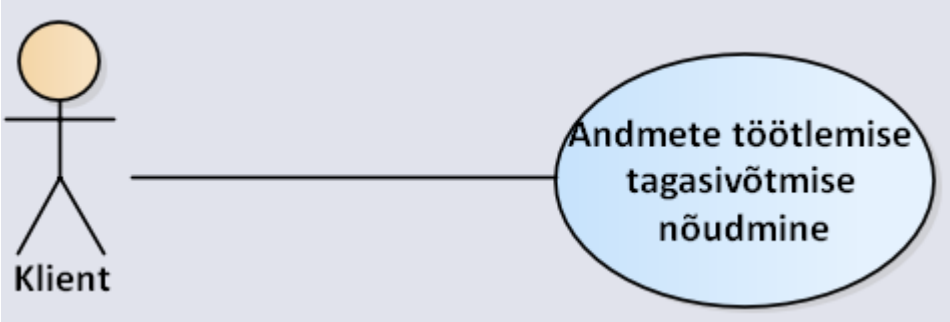
Kui klient soovib edastada andmeid teisele töötlejale: vastutav töötleja edastab andmed otse teisele töötlejale, kui see on tehniliselt teostatav. Klienti teavitatakse andmete ülekandmisest.

Kui ei ole võimalik tehniliselt kanda üle andmeid: teavitatakse klienti ning kliendile tuleb andmed anda.

Kui ei rahuldata taotlust andmeid üle kanda: põhjendatakse kliendile, miks ei ole võimalik andmeid üle kanda.

Kui taotlus võtab kaua aega: klienti teavitatakse viivitusest ning põhjendatakse, miks taotlus viibib.

Andmete töötlemise nõusoleku tagasivõtmise nõudmine:



Joonis 5. Andmete töötlemise nõusoleku tagasivõtmise nõudmise kasutusjuht

Andmete töötlemise tagasivõtmise nõudmine: Klient nõuab olemasolevate andmete töötlemise nõusoleku tagasivõtmist. Andmesubjektil on õigus oma nõusolek igal ajal tagasi võtta. Andmesubjekti teavitatakse sellest enne nõusoleku andmist. Nõusoleku tagasivõtmine on sama lihtne kui selle andmine. Subjekt esitab tagasivõtmise nõude teenusepakkuja lehel, võttes maha nõusoleku andmeid töödelda, mis algatab tarkvarasüsteemis andmete töötlemise tagasivõtmise protsessi. Vastutav töötleja annab teada nõusoleku muudatusest ning andmete mittetöötlemisest.

Põhiline edukas stsenaarium:

Klient soovib nõusolekut tagasi võtta. Klient võtab maha nõusoleku andmeid töödelda. Vastutav töötleja annab teada nõusoleku muudatusest.

Alternatiivsed stsenaariumid:

Nõusoleku tagasivõtmist ei ole võimalik rahuldada: klienti teavitatakse põhjustest, miks ei ole võimalik antud taotlust rahuldada.

3.2.3 Tarkvara automaatprotsessid

Antud peatükis kirjeldatakse süsteemi automaatprotsesse operatsiooni lepingu formaadi abil, kus järeltingimused on kooskõlas domeenimudeliga. Operatsioonid on valitud peatükis 3.3.1 välja toodud kasutusjuhtude põhjal.

3.2.3.1 Andmete kustutamine

Joonis 6. Andmete kustutamise kasutusjuht

Andmete kustutamine: Klient nõuab olemasolevate andmete kustutamist. Vastutav töötleja kasutab süsteemi kliendiandmete säilitamiseks. Süsteem sai kinnituse teenusepakkujalt andmed kustutada. Andmed kustutatakse. Klient saab süsteemilt teavituse ning klient on teadlik andmete lõplikust kustutamisest.

Põhiline edukas stsenaarium: Klient nõuab vastavalt oma õigustele andmete kustutamist, mille ta on esitanud. Vastutav töötleja kasutab süsteemi kliendiandmete kustutamiseks.

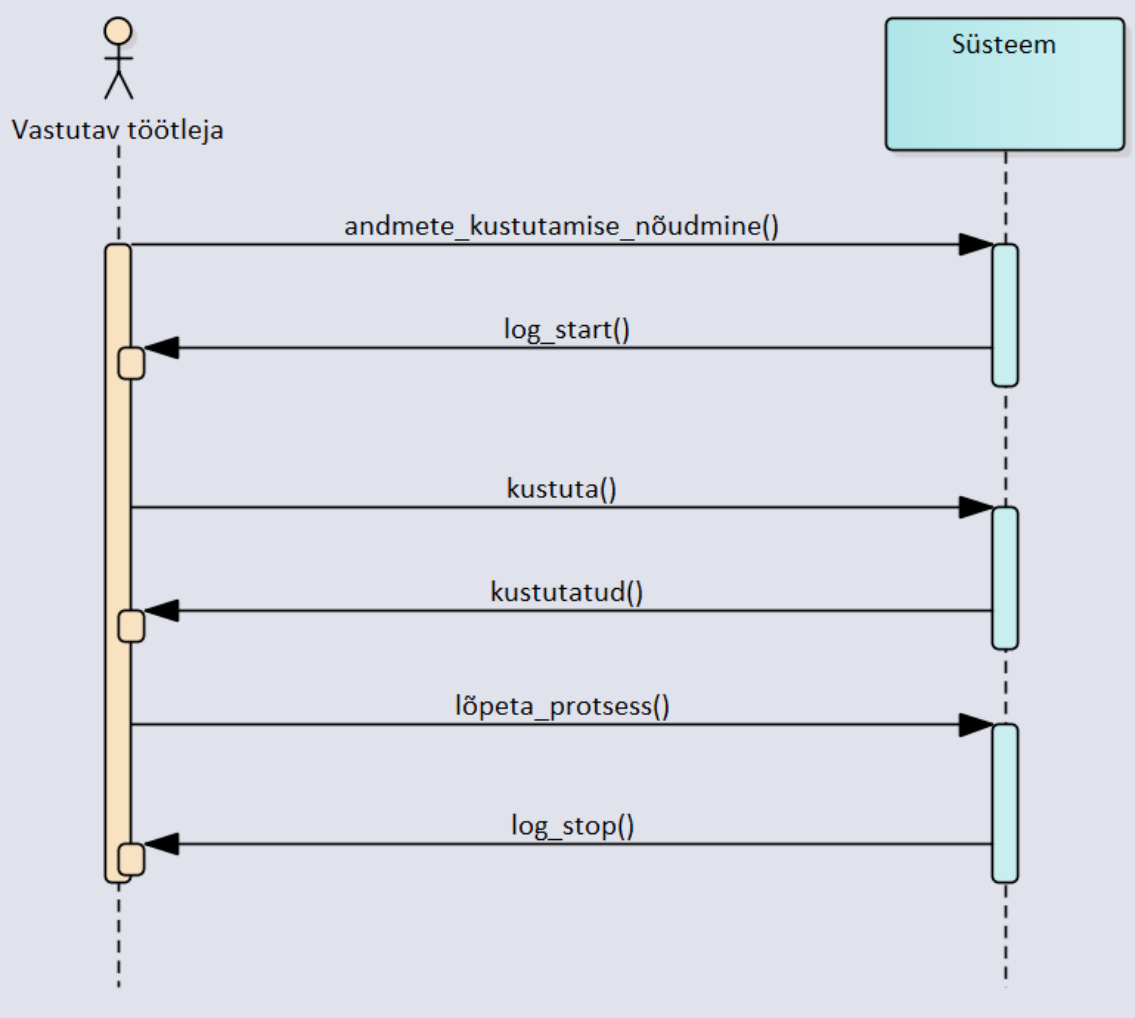
Alternatiivsed stsenaariumid:

Kui andmete kustutamine ebaõnnestub süsteemis: informeeritakse klienti ja proovitakse uuesti kõik stsenaarium läbi.

Kui andmeid ei ole süsteemis: Vastutav töötleja annab süsteemile teada ning klienti informeeritakse, et andmeid ei ole süsteemis.

Kui andmeid ei ole võimalik kustutada: informeeritakse klienti ja antakse süsteemile teada ja soovitatakse ühendust võtta kasutajatoega.

Kui andmeid kustutama minnes esineb viga: informeeritakse klienti, et hetkel on hooldus ja tegeletakse.



Joonis 7 Andmete kustutamise operatsioonid

OPL 1: andmete_kustutamise_nõudmine

Operatsioon: andmete_kustutamise_nõudmine()

Viide: Kasutusjuht: Andmete kustutamine

Eeltingimused: Subjekti nõue andmete kustutamiseks. Taotlus on määranud ära päringu tüübi.

Järeltingimused:

-Süsteem alustas kustutamise logimist.

-Kustutamise logi on initsialiseeritud operatsiooni alustamise hetkest.

-Taotluse instantsile on loodud seos päringuga.

OPL 2: kustuta

Operatsioon: kustuta(kliendi_ID, päringu_tüüp)

Viide: Kasutusjuht: Andmete kustutamine

Eeltingimused: Sisendparameetrid kliendi_ID ja päringu_tüüp on väärtustatud. Päringu instantsil on loodud seos Klient instantsiga läbi ID.

Järeltingimused:

-Kustutati sisendparameetriga kliendi_ID määratud kliendi andmed.

-Kliendi instantsi seos kliendi andmetega on kustutatud.

-Päringu instantsi seos Kliendiga kustutatakse.

OPL 3: lõpeta_protsess

Operatsioon: lõpeta_protsess()

Viide: Kasutusjuht: Andmete kustutamine

Eeltingimused: Andmed on kustutatud.

Järeltingimused:

-Kustutamise logi peatatakse.

3.2.3.2 Andmete ülekandmine

Joonis 8. Andmete ülekandmise kasutusjuht

Andmete ülekandmine: Subjekt nõuab olemasolevate andmete ülekandmist teisele andmetöötlejale. Vastutav töötleja kasutab süsteemi kliendiandmete säilitamiseks. Süsteem valideerib subjekti otsuse ning süsteem esitab subjekti andmed masinloetavas vormingus ning edastatakse teisele andmetöötlejale(kui see on tehniliselt võimalik). Subjekt saab süsteemilt teavituse ning klient on teadlik edastatud andmetest.

Põhiline edukas stsenaarium: Subjekt nõuab masinloetavas vormingus andmeid üle kanda ühelt teenusepakkujalt teisele. Vastutav töötleja kasutab süsteemi andmete väljavõtmiseks ning paneb need masinloetavasse vormingusse.

Alternatiivsed stsenaariumid:

Kui andmed ei ole masinloetavas formaadis: subjektil on õigus nõuda uuele andmetepäringule.

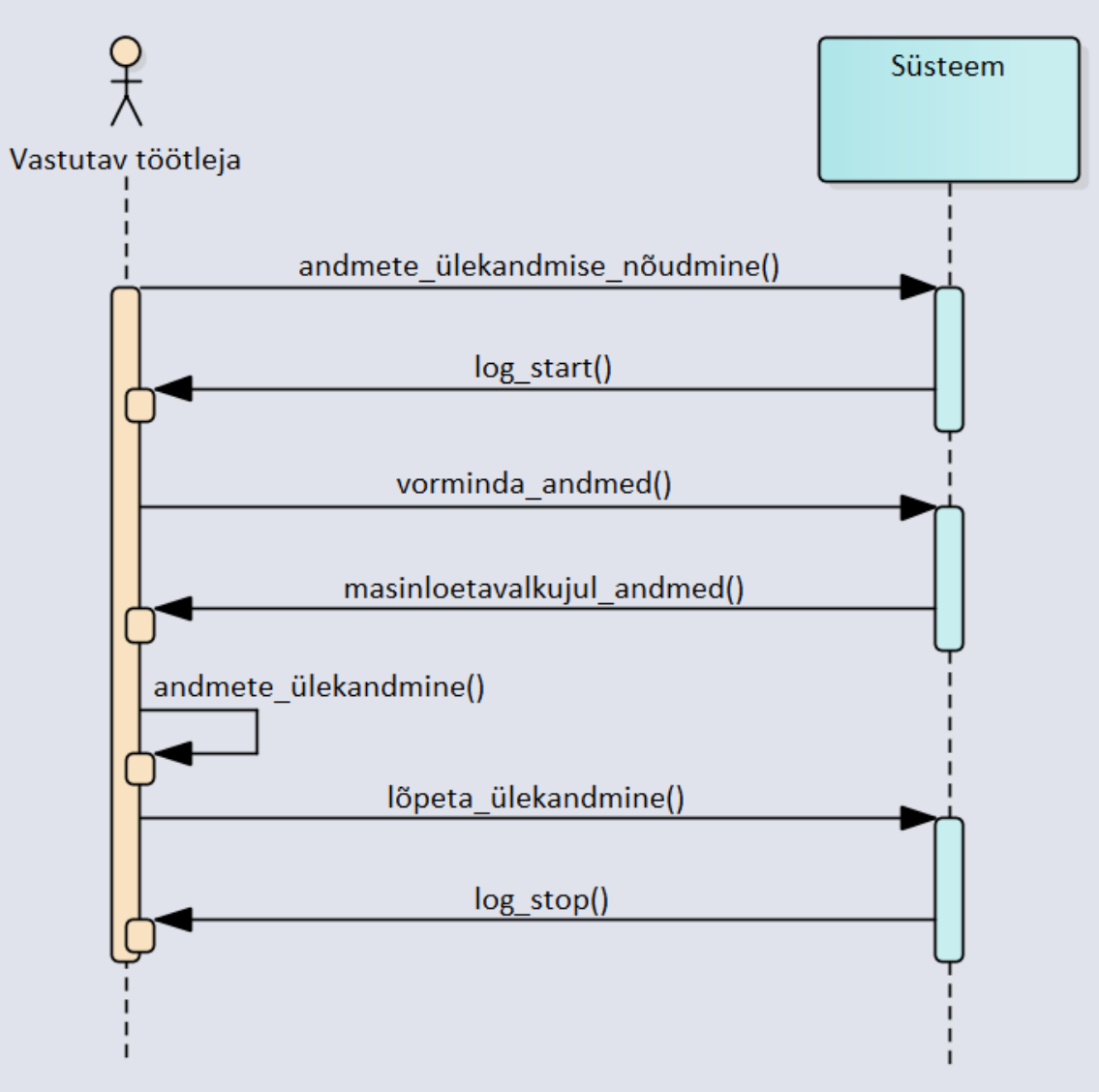
Kui ei ole tehniliselt võimalik andmeid üle kanda: vastutav töötleja võiks kohandada enda süsteeme vastavalt ülekantavale süsteemile.

Kui vastutav töötleja näeb, et andmete ülekandmine ohustab osapoolte õigusi: vastutav töötleja lõpetab protsessi.

Andmete ülekandmise taotlus on korduv: vastutav töötleja võib keelduda taotluse rahuldamisest.

Vastutav töötleja keeldub taotluse rahuldamisest: vastutav töötleja peab selgitama subjektile otsuse tegemisest.

Subjekti andmed on pärit mitmelt erinevalt teenusepakkujalt: vastutav töötleja peab küsima luba teenusepakkujatelt, et andmeid üle kanda.



Joonis 9. Andmete ülekandmise operatsioonid

OPL 1: andmete_ülekandmise_nõudmine

Operatsioon: andmete_ülekandmise_nõudmine()

Viide: Kasutusjuht: Andmete ülekandmine

Eeltingimused: Subjekti nõue andmete ülekandmiseks. Taotlus on määranud ära päringu tüübi

Järeltingimused:

-Süsteem alustas ülekandmise logimist.

-Ülekandmise logi on initsialiseeritud.

-Päringu tüüp on määratud ning päringul on loodud seos taotlusega.

OPL 2: vorminda_andmed

Operatsioon: vorminda_andmed(kliendi_ID, päringu_tüüp)

Viide: Kasutusjuht: Andmete ülekandmine

Eeltingimused: Sisendparameetrid on väärtustatud.

Järeltingimused:

- Päringu instantsil on loodud seos Klient instantsiga läbi ID.
- Päringu atribuudid on initsialiseeritud(väärtustatud).
- Päringu instantsil on loodud seos Taotlusega.

OPL 3: andmete_ülekandmine

Operatsioon: andmete_ülekandmine (kliendi_ID, päringu_tüüp)

Viide: Kasutusjuht: Andmete ülekandmine

Eeltingimused: Sisendparameetrid on väärtustatud.

Järeltingimused:

- Päringu instantsil on loodud seos Klient instantsiga läbi kliendi_ID.

OPL 4: lõpeta_ülekandmine

Operatsioon: lõpeta_ülekandmine()

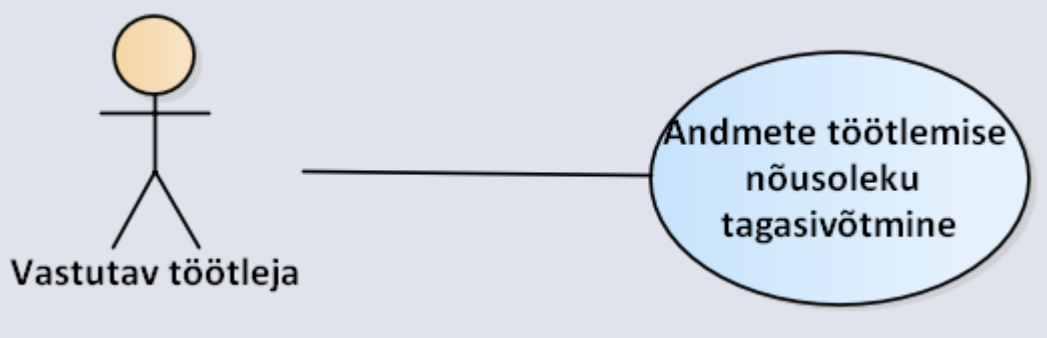
Viide: Kasutusjuht: Andmete ülekandmine

Eeltingimused: Subjekti andmed on üle kantud.

Järeltingimused:

- Ülekandmise logimise protsess lõpetatakse.

3.2.3.3 Andmete töötlemise nõusoleku tagasivõtmine



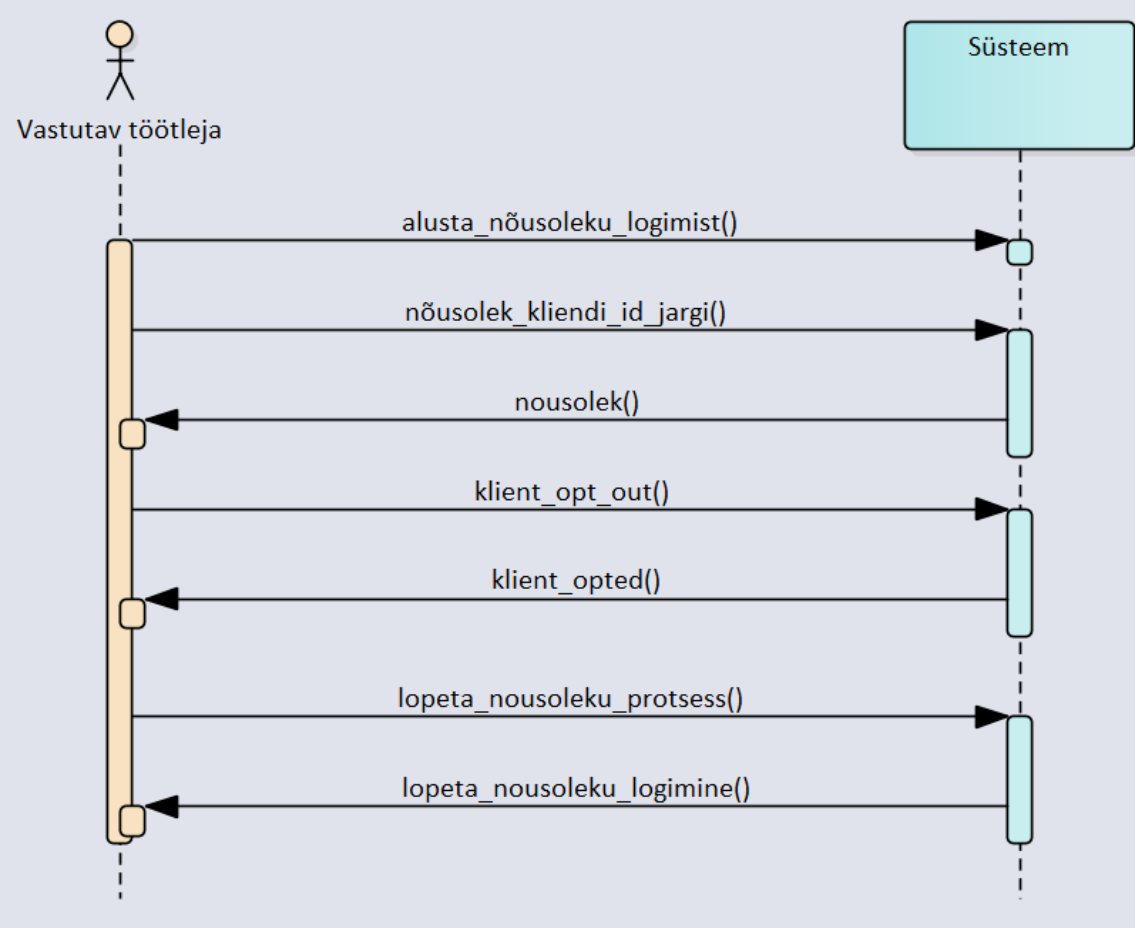
Joonis 10. Andmete töötlemise nõusoleku tagasivõtmise kasutusjuht

Andmete töötlemise nõusoleku tagasivõtmine: Klient võtab tagasi nõusoleku andmete töötlemiseks. Vastutav töötleja kasutab süsteemi kliendi nõusolekute staatuste säilitamiseks. Süsteem valideerib kliendi otsuse ning süsteem salvestab maha nõusoleku staatuse muutuse. Süsteem uuendatakse. Klient saab süsteemilt teavituse ning klient on teadlik nõusoleku mahavõtmisest.

Põhiline edukas stsenaarium: Klient võtab tagasi nõusoleku isikuandmete töötlemisest, mille ta on esitanud. Vastutav töötleja kasutab süsteemi kliendi nõusolekute staatuse hoidmiseks.

Alternatiivsed stsenaariumid:

Kui kliendi taotlus lükatakse tagasi: klienti teavitatakse taotluse mitterahuldamisest ning esitatakse vastav info, miks taotlus tagasi lükati.



Joonis 11. Andmete töötlemise nõusoleku tagasivõtmise operatsioonid

OPL 1: alusta_nousoleku_logimist

Operatsioon: alusta_nousoleku_logimist()

Viide: Kasutusjuht: Andmete töötlemise nõusoleku tagasivõtmine

Eeltingimused: Subjekti nõue andmete töötlemise piiramiseks

Järeltingimused:

-Süsteem alustas nõusoleku protsessi muutmise logimist.

-Logi on initsialiseeritud.

OPL 2: nousolek_kliendi_id_jargi

Operatsioon: nousolek_kliendi_id_jargi(kliendi_ID, päringu_tüüp)

Viide: Kasutusjuht: Andmete töötlemise nõusoleku tagasivõtmine

Eeltingimused: Subjekti nõusolek eksisteerib.

Järeltingimused:

-Päringu instantsil on loodud seos Klient instantsiga läbi ID.

-Päringu atribuudid on initsialiseeritud(väärtustatud).

OPL 3: klient_opt_out

Operatsioon: klient_opt_out(kliendi_ID, päringu_tüüp)

Viide: Kasutusjuht: Andmete töötlemise nõusoleku tagasivõtmine

Eeltingimused: Päringu instants on initsialiseeritud(väärtustatud).

Järeltingimused:

- Kliendi nõusoleku status on muudetud.

- Andmetöötlus on piiratud.

OPL 4: lõpeta_nousoleku_protsess

Operatsioon: lõpeta_nousoleku_protsess()

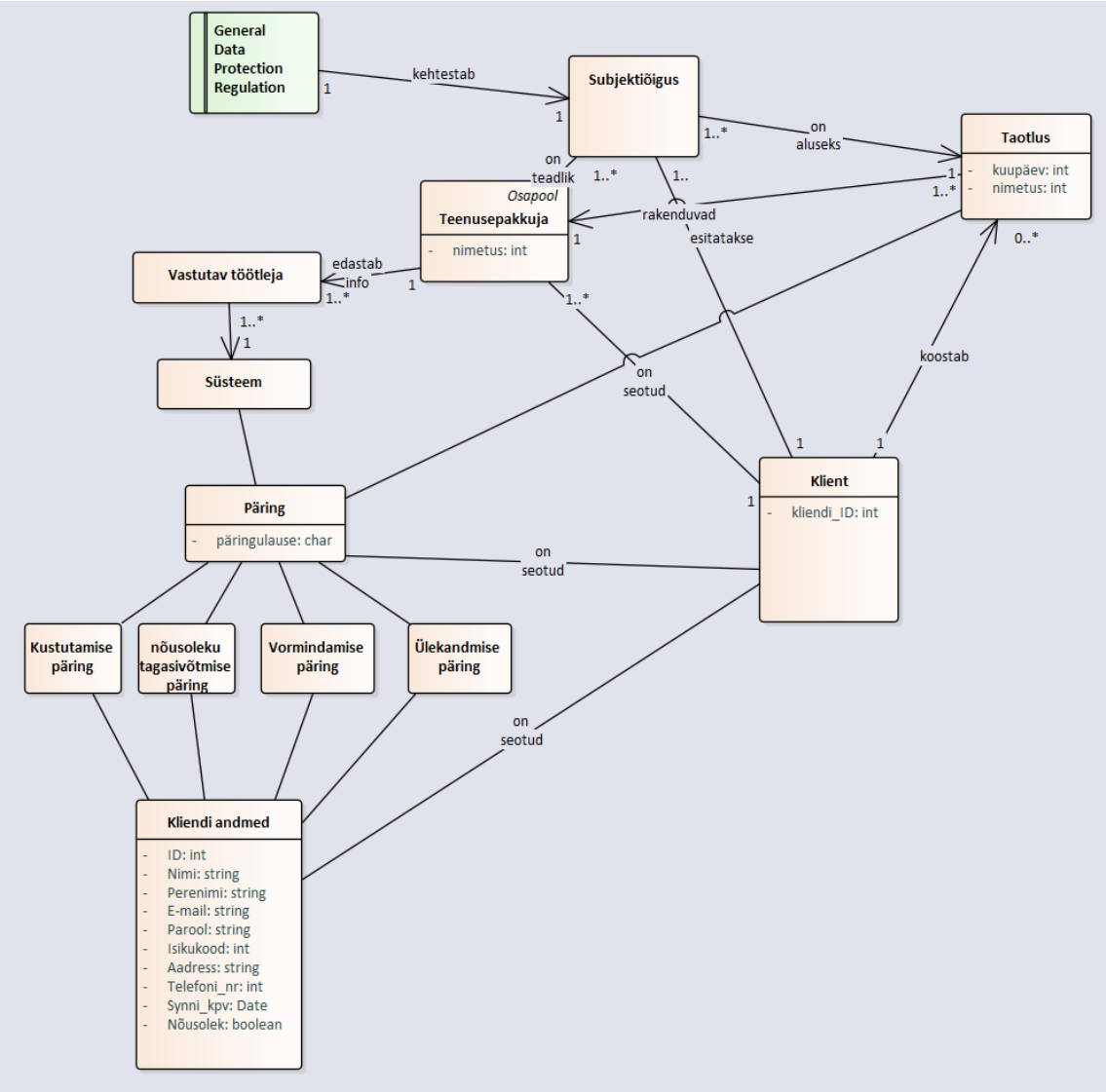
Viide: Kasutusjuht: Andmete töötlemise nõusoleku tagasivõtmine

Eeltingimused: Subjekti nõusolek on muudetud ning on määratud andmehulk, mida tohib töödelda.

Järeltingimused:

- Ülekandmise logimise protsess lõpetatakse.

3.2.4 Üldine kontseptuaalne klassidiagramm



Joonis 12. Kontseptuaalne klassidiagramm

Isikuandmete kaitse üldmäärus kehtestab õiguse subjektile, millele subjektil on võimalik toetuda koostades taotlust.

Klient võib koostada ühe või mitu Taotlust, mille aluseks on üldmääruses kehtestatud õigus.

Taotlus on seotud konkreetse päringu ning konkreetse kliendiga. Õiguste rakendamine toimub teenusepakkuja juures. Teenusepakkuja võib olla seotud ühe või mitme taotlusega. Konkreetne klient võib olla seotud ühe või mitme teenusepakkujaga.

Teenusepakkuja edastab taotluse vastutavale töötlejale. Süsteemis on üks või mitu vastutavat töötlejat.

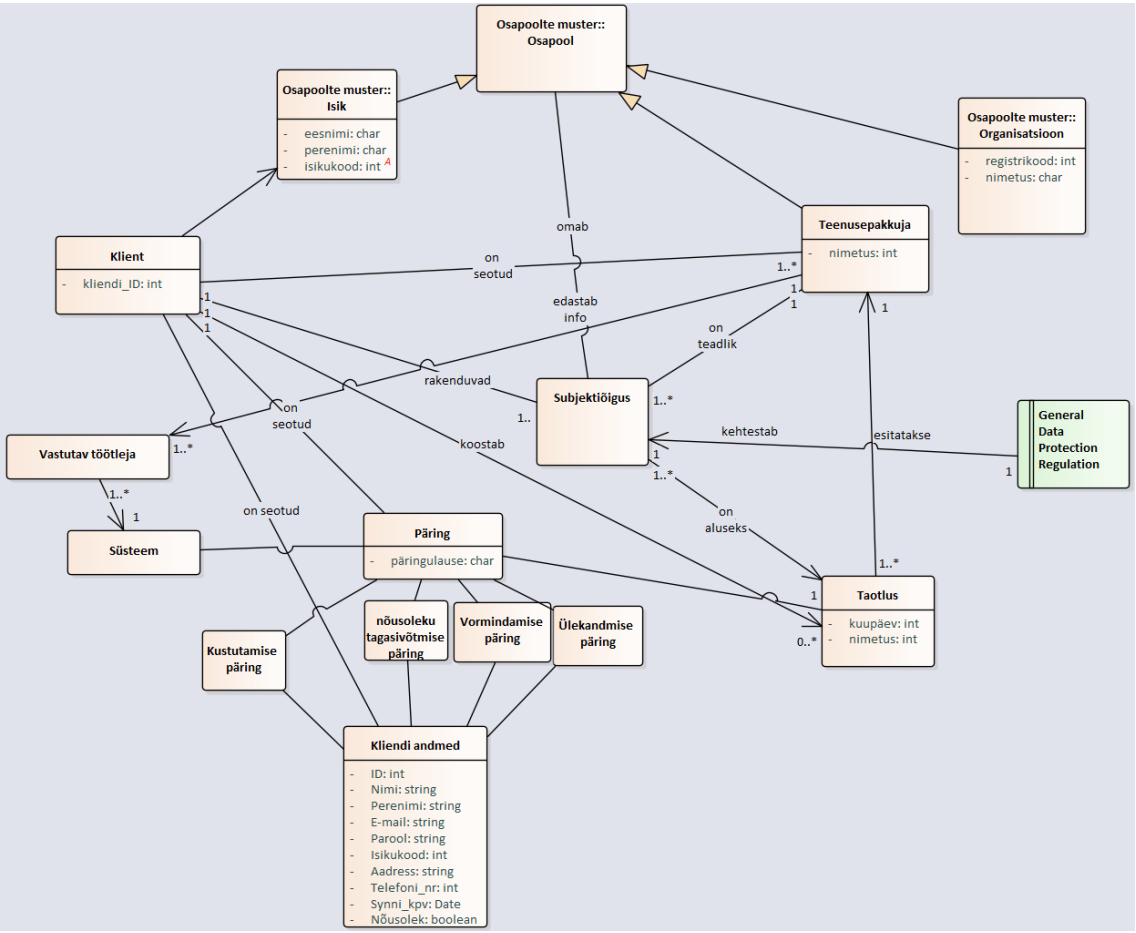
Süsteemis tehakse päringuid, mille spetsifikatsioon on määratud taotluses.

Päring on seotud konkreetse kliendiga.

Päringul on alampäringud: kustutamise päring, piiramise päring, vormindamise päring ning ülekandmise päring. Alampäringud kõik pärivad informatsiooni kliendi andmete kohta.

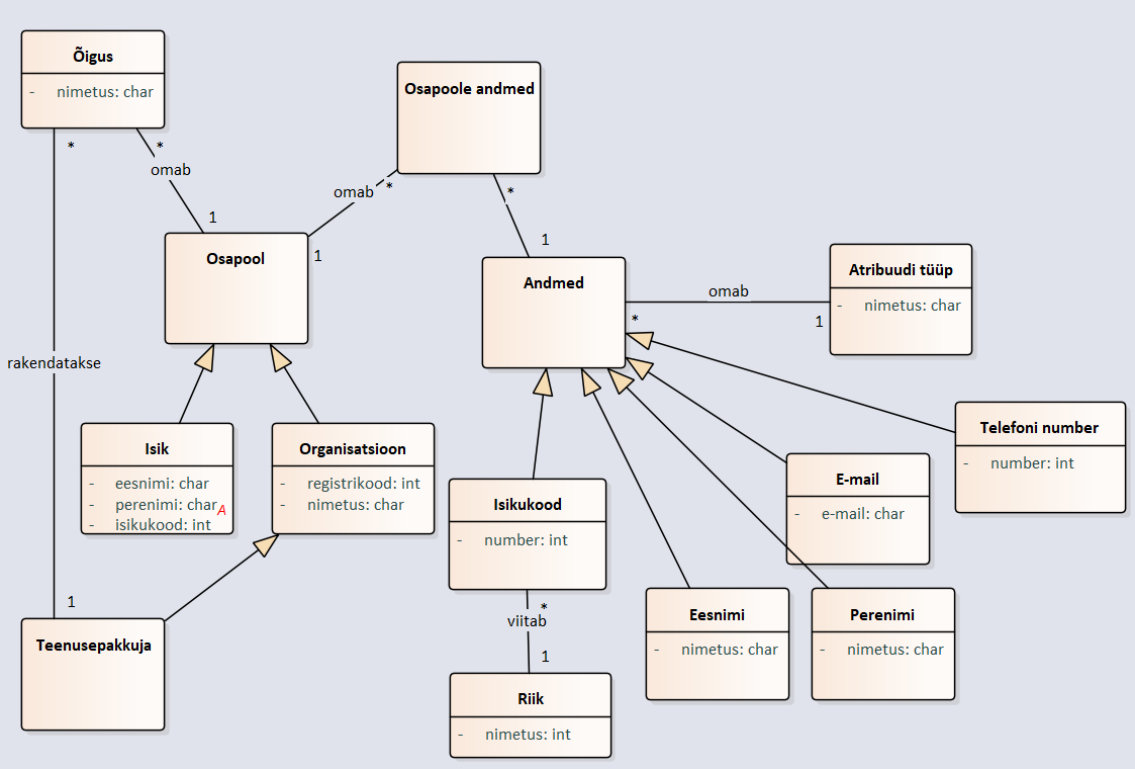
3.2.5 Täpsustatud kontseptuaalne klassidiagramm. Analüüsimustrite kasutamine.

Võrreldes eelmises peatükis välja toodud klassidiagrammiga on nüüd rakendatud analüüsimustrit nimega Osapool(*Party*).



Joonis 13. Täpsustatud klassidiagramm osapoole analüüsimustriga

Osapool on üldmõiste üle Isikute ja Organisatsioonide. Kui klient on Isik, siis Teenusepakkuja puhul on ükskõik, kas mingit kliendile vajalikku Teenust pakub Isik või Organisatsioon. Seega on Osapoole mõiste ja analüüsimustri sissetoomine siinkohal mõistlik ja kasutoov.



Joonis 14. Osapool

Osapool omab õigusi, mida rakendatakse kindlates teenustes. Teenusepakkuja on Organisatsioon. Osapool omab ka erinevat tüüpi andmeid, nagu eesnimi, E-maili aadress, telefoni number, isikukood, perenimi. Üks eesnimi võib olla mitme Osapoole eesnimeks.

4 Raamistiku valideerimine

Peatükis valideeritakse üldmääruses välja toodud õiguste või muud liiki konkreetsete nõudmiste suhtes selleks, et tarkvara saaks nendega arvestada ning võimaldada nende täitmist.
Valideeritakse kasutusjuhtude ning operatsioonide lepingute vormis esitatud funktsionaalseid nõudeid raamistikule.

4.1 Andmete ülekandmise õigus

Andmesubjektil on õigus saada teda puudutavaid isikuandmeid, mida ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul ning õigus edastada need andmed teisele vastutavale töötlejale. [6, artikkel 20]

Töö autor leiab, et käesolev raamistik katab ära subjekti nõude andmeid üle kanda. Andmete ülekandmise kasutusjuhtu analüüsiti peatükis 3.2.3.2, kus mainiti, et antud protsessi käivitab andmesubjekti õigus andmeid üle kanda ning vastutav töötleja vastutab andmete vormindamise ja edastamise eest.

4.2 Õigus andmete kustutamisele

Andmesubjektil on õigus nõuda, et vastutav töötleja kustutaks põhjendamatu viivituseta teda puudutavad isikuandmed ja vastutav töötleja on kohustatud kustutama isikuandmed põhjendamatu viivituseta, kui kehtib üks järgmistest asjaoludest:

1. Isikuandmeid ei ole enam vaja sellel eesmärgil, millega seoses need on kogutud või muul viisil töödeldud.

2. Andmesubjekt võtab töötlemiseks antud nõusoleku tagasi ning puudub muu õiguslik alus isikuandmete töötlemiseks.

3. Andmesubjekt esitab vastuväite isikuandmete töötlemise suhtes ja töötlemiseks pole ülekaalukaid õiguspäraseid põhjuseid.

4. Isikuandmeid on töödeldud ebaseaduslikult.

5. Isikuandmed tuleb kustutada selleks, et täita vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega ette nähtud juriidilist kohustust.

6. Isikuandmeid koguti seoses infoühiskonna teenuste pakkumisega. [6, artikkel 17]

Andmete kustutamise kasutusjuhtu analüüsiti peatükis 3.2.3.1. Andmete kustutamise käivitab subjekti õiguse rakendamine ning kliendi andmed kustutatakse süsteemist.

Ekspert Priit Pikk tõi välja, et kustutamine võiks toimuda vastavalt eesmärgile. Andmetöötluse eesmärgid jagunevad nelja õigusliku aluse vahel: seadusest tulenev kohustus, lepingu täitmise eesmärgil, ettevõtte õigustatud huvi ja nõusolekupõhine. Igal eesmärgil on töötlemise tähtaeg, mille saabumisel tuleb andmetöötlus lõpetada. Isik saab nõuda ennetähtaegset kustutamist ainult kahe viimase õigusliku aluse all tehtavate eesmärkide osas.

Näiteks eesmärgid: klienditeeninduslikud suhted, mis ei ole vajalikud lepingu täitmiseks (sünnipäeva tervitus, proaktiivne teenindus), turunduslik profileerimine või otseturundus (personaalsed kirjad elektroonilisele kontaktile).

4.3 Õigus nõusoleku tagasivõtmisele

Andmesubjektil on õigus oma nõusolek igal ajal tagasi võtta. Nõusoleku tagasivõtmine ei mõjuta enne tagasivõtmist nõusoleku alusel toimunud töötlemise seaduslikkust. Andmesubjekti teavitatakse sellest enne nõusoleku andmist. Nõusoleku tagasivõtmine on sama lihtne kui selle andmine. [6, artikkel 7]

Autori poolt loodud raamistik sobib nõusoleku tagasivõtmise protsessile. Nõusoleku tagasivõtmist analüüsiti peatükis 3.2.3.3.
Kasutusjuht valideeriti ka eksperdi Priit Pikk poolt, kes märkis, et nõusolekupõhist andmete töötlemist oleks võinud ka käsitleda.

4.4 Õigus tutvuda andmetega

Andmesubjektil on õigus saada vastutavalt töötlejalt kinnitust selle kohta, kas teda käsitlevaid isikuandmeid töödeldakse, ning sellisel juhul tutvuda isikuandmete ja järgmise teabega:

1. Töötlemise eesmärk.
2. Asjaomaste isikuandmete liigid.
3. Vastuvõtjad või vastuvõtjate kategooriad, kellele isikuandmeid on avalikustatud või avalikustatakse, eelkõige kolmandates riikides olevad vastuvõtjad või rahvusvahelised organisatsioonid.
4. Kui võimalik, siis kavandatav isikuandmete säilitamise ajavahemik või, kui see ei ole võimalik, sellise ajavahemiku määramise kriteeriumid.
5. Teave õiguse kohta taotleda vastutavalt töötlejalt andmesubjekti puudutavate isikuandmete parandamist, kustutamist või töötlemise piiramist või esitada vastuväide sellisele isikuandmete töötlemisele.
6. Teave õiguse kohta esitada kaebus järelevalveasutusele.
7. Kui isikuandmeid ei koguta andmesubjektilt, siis olemasolev teave nende allika kohta.
8. Teave automatiseeritud otsuste, sealhulgas profiilianalüüsi tegemise kohta ning vähemalt nendel juhtudel sisuline teave kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks. [6, artikkel 15]

Antud õigusele sobitub raamistik, kuid tuleb märkida, et iga õiguse rakendamine subjekti poolt tegelikult pärib andmeid. Kui subjekt rakendab õigust kustutada oma andmeid, siis toimub süsteemis ka andmete pärimise päring. Antud töös analüüsiti andmete pärimise protsessi kui tutvumist andmetega, mida töödeldakse.

5 Kokkuvõte

Lõputöö põhieesmärgiks oli analüüsida isikuandmete kaitse üldmäärusest tulenevaid subjekti õiguseid ning nendest tulenevaid protsesse ning luua raamistik uute andmebaaside modelleerimiseks vastavalt isikuandmete kaitse üldmääruse nõuetele.

Esmalt analüüsiti isikuandmete üldmäärust toetudes Zachman'i tugiraamistikule, et määratleda valdkonnas olulised mõisted ning tükeldada tervikmudel loogiliselt protsesside, sündmuste ja põhiobjektidena. Peatükis on välja toodud ainult uute nõuetega seotud aspektid, kuna terve üldmääruse analüüsi maht oleks liiga suur, et lõputöö sisus seda kajastada.

Kolmandas peatükis loodi valdkonna kohta koostatud protsessi vaate struktuur ehk katusprotsess ning tema alamprotsessid, nii kliendipoolsed kui ka automaatprotsesside kasutusjuhtude lühiformaadid, objektide/info kohta kontseptuaalne klassidiagramm ja täpsustatud kontseptuaalne klassidiagramm koos osapoole analüüsimustriga.

Neljandas peatükis valideeriti lõputöös käsitletud nõudeid nii autori kui ka eksperdi poolt.

Lõputöö eesmärgid ja soovitud tulem saavutati ehk raamistikul suuremaid puudusi ei esinenud. Järgnevalt on plaan luua lõputöö tulemist edasi arendatud raamistik, mille väiksemad puudused on lahendatud ning lisatud rohkem nõuetest tulnud spetsiifikaid ja reegleid.

Kasutatud kirjandus

[1] UML, https://et.wikipedia.org/wiki/%C3%9Chtne_modelleerimiskeel

[2] EA, https://en.wikipedia.org/wiki/Enterprise_Architect_(software)

[3] RUP, https://en.wikipedia.org/wiki/Rational_Unified_Process

[4] UP, https://en.wikipedia.org/wiki/Unified_Process

[5] OO, http://rlpa.ttu.ee/Modelleerimine.pdf

[6] Isikuandmete kaitse üldmäärus,
https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679

[7] Zachman'i raamistik,
https://www.tlu.ee/opmat/in/Arhitektuur/41_zachmani_raamistik.html

[8] Domeenimudel, https://maurus.ttu.ee/ained/IDU5360/doc/33/Domeenixmudel.docx

[9] Fowler, M., 1997. Analysis Patterns: Reusable Object Models. Addison-Wesley, Menlo Park, Calif. 360 p.

[10] Larman, C., 1997. Applying UML and patterns : an introduction to object-oriented analysis and design. Upper Saddle River (N.J.) : Prentice Hall PTR. 507 p.

[11] Eessaar, E. (2015). Andmebaasid I/II õppematerjalid.

[12] Doble J., Meszaros G. A Pattern Language for Pattern Writing. - The Hillside Group. http://hillside.net/a-pattern-language-for-pattern-writing (05.01.2016)

[13] Accountability, https://martinfowler.com/apsupp/accountability.pdf