ChatGPT

PPA drooniseiresüsteemi haldus- ja pidamiskorra eeluuringu intervjuuküsimused

1. Infosüsteemi haldus- ja pidamisvastutus

- **(Juhtkond/haldustruktuur)** Infoturbe haldussüsteemi standardid rõhutavad, et infosüsteemi turvameetmete eest vastutav juhtkond peab tagama süsteemi pideva riskihalduse ja piisavad ressursid [1]. Seega: kelle määratud on drooniseiresüsteemi haldus ja hooldus (PPA, Siseministeerium, SMIT jm), kes kannab vastutust süstemaatilise pidamise eest ning kuidas on määratletud koostöö ja vastutus asutuste vahel? Kuidas tagatakse juhtkonna toetus ja aruandlusinfosüsteemi haldusele?
- **(Haldus/Projektijuht)** Kas drooniseiresüsteemi haldusrõõte on kirjeldatud ametlikus dokumendis (nt haldus- ja pidamiskorras)? Kuidas on reguleeritud süsteemi pidamise eeskiri, mis hõlmaks vigu, uuendusi ja häirete lahendamist? Kelle ülesandeks on selle kooskõlastamine (nt RIA RIHA registris)?
- **(Juhtkond/Kogu)** Kas süsteemi omand ja finantseerimine on selgelt määratletud (nt PPA sisemine või rahvusvaheline ühisprojekt)? Millised lepingulised kokkulepped (nt riigihankemenetlus, koostöölepingud) on sõlmitud sidusasutustega (Siseministeerium, Kaitseministeerium, NATO liitlased, kriitilise taristu operaatorid jt), et ühiselt tagada süsteemi hoolduse ja turvalisuse nõuetekohane jaotus?

2. Koodi omand, õigused, muutmisvõimalused

- **(Hankespetsialist/Õigusnõunik)** Kes omab drooniseiresüsteemi lähtekoodi ja tarkvara? Millised autorlus- ja litsentsitingimused kehtivad (näiteks avatud lähtekood vs patenteeritud tarkvara)? Kas lähtekood kuulub PPA-le või kolmandale osapoolele?
- **(Arhitekt/Tehniline haldaja)** Kuidas on defineeritud süsteemi arendamise ja modulaarse arenduse protsess (nt Git-lahendused, versioonihaldus)? Kes on volitatud koodi muutma (nt PPA sisemeeskond, ostetud teenusepakkuja)? Millised tingimused on lepitud kokku koodibaasi üleandmisel arendajate vahetumisel (koodidokumentatsioon, automaattestid)?

3. Juurdepääsulogid, säilitusnõuded, auditeerimine

- **(Infoturve/Admin)** Süsteemi auditeerimise ja väärkasutuste tuvastamise jaoks tuleb tagada, et kõik olulised sündmused on logitud ning neid saab järelevalvekorras analüüsida [2]. Küsimus: milliseid logisid (kasutajate sissepääsud, süsteemi seaded ja muudatused, andmetöötluste ajalugu, veateated) drooniseiresüsteem kogub ja kauemaks säilitab? Kes ning millistel eesmärkidel neid logisid haldab? Kuidas tagatakse, et logisid säilitatakse piisavalt kauaks (arvestades õiguslikke nõudeid) ja auditeeritakse regulaarselt?
- **(Õigusnõunik/Küberturbe)** Kui süsteem jälgib operatiivtegevust (nt videologi, sensorite kasutus), siis milline on isikuandmete privaatsuse ja säilituse kord? Kuidas teavitakse töödeldavaid isikuid videovalvest ja andmetöötlusest?

4. Ligipääsu tasemed ja rollipõhine kontroll

- **(Infoturve/Admin)** Juurdepääsukontroll põhineb turvalisuse põhimõttel, et igal kasutajal peab olema ligipääs ainult neile andmetele ja toimingutele, mis on tema rolli jaoks vajalikud [3]. Küsimus: kuidas on drooniseiresüsteemis defineeritud rollid (näiteks operatiivtöötaja, halduri asetäitja, juhtivtöötaja, liitlaste juurdepääs)? Kas kasutatakse rollipõhist juurdepääsuõiguste haldust (RBAC), ja milline on iga rolli volitusaste? Kuidas tagatakse, et rollid ja nende õigused vaadatakse regulaarselt üle (least privilege põhimõte)?
- **(Turbeinsener/IT-spetsialist)** Kas on selgelt määratletud eraldi administratiivsed ja operatiivsed rollid (nt eraldi kontod süsteemi häälestamiseks ja andmete töötlemiseks)? Kas drooniseiresüsteem toetab mitmefaktorilist autentimist või muid täiendavaid turvamehhanisme administraatoritele?

5. Andmete elutsükkel (kogumine, töötlemine, säilitamine, kustutamine)

- **(Andmekaitse spetsialist)** GDPR-i printsiipide kohaselt tuleb isikuandmeid töödelda viisil, mis tagab nende ajutisuse – andmeid tuleb hoida „lühima võimaliku aja jooksul“ ja regulaarselt üle vaadata [4]. Küsimus: kas süsteemi puhul on sõnastatud andmepoliitika (andmete elutsüklipoliitika), mis määrab andmete kogumise alused, salvestusajad ja kustutamise tingimused? Kes vastutab andmete korra eest (nt andmekaitseametnik) ja kuidas on tagatud, et vananenud või tarbetud andmed õigeaegselt hävitatakse või anonümiseeritakse?
- **(Jurist/Kliendiinfo)** Kuidas tagatakse, et andmete töötlemine vastab isikuandmete kaitse seadusele (nt informeeritakse isikut, kui tema andmeid kogutakse)? Kas analüüsitakse, milliseid sensorte andmeid kogutakse ja milleks neid kasutatakse (nt avalikus ruumis videovalve eritingimused)?
- **(Andmehaldur/Arhitekt)** Milline on andmete arhiveerimise ja taastamise kord (nt automaatsed varukoopiad, maatriks)? Kus ja kuidas hoitakse varukoopiaid (krüpteerituna, eraldi võrgusalas)? Kuidas dokumenteeritakse andmete ajalugu, et säilitada vastavust auditnõuetele?

6. Seadmete ja sensorite haldus (sh geograafilised piirangud, grupipõhine nähtavus)

- **(Tehniline haldaja/Droonipiloot)** Droonide kasutamisel tuleb arvestada geograafiliste tsoonide regulatsiooniga – EL geotsoonid on kehtestatud selleks, et tagada ohutus, kolmandate isikute privaatsus ja vältida turvaohtusid [5]. Küsimus: kas droonide lennutamisel kasutatakse geograafilist piirangut (nt keelualad, piirialad)? Kuidas tagatakse, et droon ei satu keelatud tsooni (nt lennujaamad, sõjaväeobjektid, tuumajaamad) ning kuidas on kavandatud drooni positsioneerimise ja lennutrajektoori pidev järelevalve?
- **(Süsteemi arhitekt/Valdkonna spetsialist)** Kuidas hallatakse erinevate sensorite andmevoogusid (nt videokaamerad, termokaamerad, radar)? Kas droonipildid võivad alluda erinevatele nähtavustasemetele (nt üldine vaatlus vs salastatud sihtmärgid)? Kuidas tagatakse, et ainult pädevad kasutajad / grupid pääsevad tundlike sensorite infole ligi?
- **(Valdkonnapoliitik/Õigusnõunik)** Kas droonide tegevuskorralduses on eraldi arvestatud piiranguid (nt lennutõkestused keskkonnakaitse, elustiku kaitse, riigisaladuse kaitse juhtudel)? Kui droonide sensorid tuvastavad tundlikku info (kaamera, mikrofon), siis kuidas käsitletakse neid andmeid (salastatus)?

7. Pilve või sisevõrgu küsimused

- **(IT-arhitekt/Haldaja)** Eesti riigipilve hübriidmudel toetab digitaalse pidevuse tagamist ja turvaastet ISKE H kasutamist, tagades tundlike andmete konfidentsiaalsuse ja tervikluse [6]. Küsimus: kus asuvad drooniseiresüsteemi serverid ja andmebaasid (riigipilves, erasektori pilveteenuses, PPA sisevõrgus)? Mis põhjusel on valitud konkreetne lahendus (nt juurdepääsetavus, töökindlus, turvalisus)?
- **(IT-turbeanalüütik)** Kui kasutatakse pilveteenust, siis kuidas on tagatud andmete krüpteerimine (nii siirdudes kui seisus) ning ligipääsu kontroll pilves? Kas pilveteenuse pakkuja vastab Eesti ja EL turvanõuetele (nt andmekeskuse asukoht Eestist/EL-ist)? Kuidas on kooskõlastatud IT-infrastruktuuri haldus (riigipilve teenused) Siseministeeriumiga või RIA-ga?
- **(Riskijuht)** Kas lahendus on üles seatud mitme keskkonna peale (nt produktiiv-, varu- ja testkeskkond)? Mis on tegevuse taasteplaan, kui primaarne hostimiskeskkond langeb (nt varunduspilv, alternatiivne andmekeskus)? Milliseid ärikatkestuse- või ärijärkjärgi on määratletud?

8. Tarkvara uuendused, versioonihaldus, katkestuste riskid

- **(DevOps / Tarkvara-arhitekt)** Infosüsteemi haldussüsteemi raamistik sätestab, et turvariskide haldamiseks tuleb süsteemi pidevalt hooldada ja täiustada [7]. Küsimus: kuidas on korraldatud drooniseiresüsteemi tarkvarauuendused ja versioonihaldus (nt arendusprotsess, testkeskkond, värskenduste avaldamine)? Kas uuendused on automatiseeritud (rolling updates) või käsitsi? Kuidas minimeeritakse töökatkestuse riske värskenduste puhul (nt versioonivõimaluste testimine, tagasipööramise plaanid)?
- **(IT-haldur / Riskijuht)** Mis on määratud kriitilistele tarkvara- ja riistvarakomponentidele (nt OS, droonide juhtimisplatvorm, andmebaas) varulepingud ja asenduskomponendid? Kuidas tagatakse süsteemi töökindlus nö “fail-safe” režiimidega (nt drooni signaalikaotus → turvaline maandumine)?
- **(Kasutajatoe spetsialist)** Kuidas toimivad alarmid ja teavitused, kui midagi läheb uuenduste või halduse käigus valesti? Kellele antakse teavitus (L2, L3 toe tiim, juhtimine)?

9. Kriisiolukorra reeglid ja töökindlusnõuded

- **(Riskijuht / Hädaolukordeks planeerija)** Hädaolukorra seaduse kohaselt peab elutähtsa teenuse süsteem kaardistama ja analüüsima enda riskid ning tagama teenuse vajaliku töökindluse [8]. Küsimus: millised on drooniseiresüsteemi töökindlus- ja varustustaseme nõuded (näiteks operatiivsuse reageerimisaeg, lubatud katkemite kestus)? Kuidas on määratletud kriisiolukorra stsenaariumid (looduskatastroof, sõjalis-poliitiline kriis, sidekatkestus) ning millised tehnilised ja korralduslikud meetmed on hädaolukorras kasutusel (näiteks autonoomne operatsioon, varustaja loodud alternatiivühendus)?
- **(Juhtkond / Investeeringute planeerija)** Kuidas on tagatud süsteemi taastumisvõime peale erilisi sündmusi? Kas on koostatud terviklik ärikatkestuse taastamise plaan (Business Continuity Plan), milles arvestatakse kriisivõimsusega (nt hädaaldised ja varusüsteemid)? Kuidas koordineerub hädaolukorra valitsusorgani (Siseministeerium / Kaitseministeerium) tegevus süsteemi hoidmisega (nt alluvusahelas)?

10. Turvaklassifikatsioon, piiratud kasutusega andmed, salastatus

- **(Turbeekspert / Andmekaitse)** Riigi infosüsteemide turvameetmete raamistik nõuab, et andmekogu andmetele määratakse andmete turvaanalüüsi põhjal turvaklass ning rakendatakse vastavad kaitsemeetmed [9] . Küsimus: kuidas on drooniseiresüsteemi kogutavad andmed (pildivõrgud, lennutrajektoori andmed, metaandmed) klassifitseeritud (nt riigisaladus, salastatud välisteave, piiratud, avalik)? Millised turvalisuse miinimumnõuded on kehtestatud (krüpteering, pääsuõiguste piirarvud, füüsiline kaitse) salastatud andmete jaoks?
- **(Õigusnõunik / Seadusandja)** Kas süsteemile on pandud täiendavad juurdepääsu- või avaldamispiirangud (nt riigisaladuse seadus või rahvusvahelised kokkulepped)? Kuidas käsitletakse juhtumeid, kus drooni salvestatud videomaterjal või sensoridokumentides võib juhuslikult sattuda riigisaladust või piiratud infot (nt samuti NATO liitlastega seotud operatsioonid)?
- **(Andmehaldaja / Dokumenteerija)** Kas turvameetmete rakendamisel järgib süsteem riigiinfosüsteemi kolmeastmelise turbeetalonõudeid (ISKE) vastavalt tuvastatud turvaklassidele? Kas drooniseiresüsteemi jaoks on vajadusel valmis eritõkestus (nt eraldi salastatud võrk, füüsilised eraldused) piiratud info käsitlemiseks?

11. Vastavus Eesti ja EL õigusele (sh GDPR, küberturbe seadus)

- **(Õigusnõunik / Turbespetsialist)** Küberturbe seadus nõuab süsteemsete turvariskide analüüsi ja asjakohaste tehniliste ning korralduslike meetmete rakendamist [10] . Samuti sätestab GDPR (IKÜM) artiklis 32 infoturbe eesmärgid – süsteem peab tagama konfidentsiaalsuse, tervikluse, käideldavuse ja vastupidavuse ning regulaarse turvameetmete testimise ja hindamise [11] . Küsimus: milliseid õiguslikke nõudeid on arvesse võetud drooniseiresüsteemi juurutamisel (andmekaitse, krüptimise regulatsioonid)? Kas on läbi viidud nõuetekohane turvariskide analüüs ja dokumenteeritud süsteemi vastavus GDPR-i nõuetele (nt andmekaitsealaste mõjuanalüüsi kaudu)? Kuidas süsteemi tegelik kasutamine vastab kehtestatud legistilisele raamistikule (nt kuhu tehakse logi, kas kasutatakse legitimeerimisviise vastavalt seaduste nõudmistele)?
- **(Riigiametnik / Regulatsioonispetsialist)** Kas ja millal on süsteem registreeritud vastavalt riigiinfosüsteemide halduskorra nõuetele (nt RIHA)? Kuidas on arvesse võetud muud õigusaktid (näiteks riigisaladuse seadus, küberturbe seadus, haldusmenetluse seadus), et tagada süsteemi õiguslik puutumatus? Kas RIA või SMIT on vahetult kaasatud süsteemi ülevaatustesse või sertifitseerimisse?
- **(Infoturbeametnik / Auditeerija)** Kuidas tagatakse nõuete järgimine (nt siseauditi või kolmanda osapoole auditeerimise abil)? Kuidas toimub riskianalüüsi ja turvameetmete rakendamise dokumenteerimine vastavalt nõuetele (nt küberturbe seaduse §10)? Kas on plaan kohandada meetmeid EL-i või NATO uute turvapoliitikate järgi (nt NIS2 direktiiv)?

12. Ühendused teiste süsteemidega ja liidestamised

- **(Integraator / Süsteemiarhitekt)** Milliste välissüsteemidega drooniseiresüsteem andmeid jagab või vastu võtab (nt radarid, piirivalvekeskused, häireinfo süsteemid, politseiuurimuse infosüsteem, NATO / EL operatsioonikeskused)? Kas on kaardistatud infovoog ja andmevahetuse protseduurid kõigi liidestuste jaoks?
- **(IT-spetsialist / NATO liaison)** Kas drooniseiresüsteem ühildub olemasolevate standarditega (nt STANAG, ATOC protokollid või riigisiseste standarditega)? Kuidas on lepingutes reguleeritud vastutus ja turvalisus liidestuste puhul (kes vastutab andmekadu või väärkasutuse eest liidese tekkimise korral)?

- **(Lepinguspetsialist / Operatiiv)** Kas side teiste süsteemidega on krüpteeritud ja logitud? Kuidas tagatakse, et ühendused välisprojektidega (nt NATO liitlastega) järgivad samasuguseid turvameetmeid ja konfidentsiaalsuse nõudeid?

13. Vastutus juhtumite (nt rikkumiste või süsteemse vea) korral

- **(Turbejuht / IT-vastutav)** Küberturbe seadus sätestab, et digitaalse teenuse osutaja peab teatama olulistest küberintsidentidest pädevale asutusele (nt RIA või Küberturbe Abikeskus) viivitamata ja koostama intsidendiaruande [12]. Küsimus: milline on drooniseiresüsteemi intsidendihalduse ja raportimise protsess? Kes on määratud vastutajateks rikkumiste korral (PPA siseuurija, Kaitseministeeriumi küberturbeametnik), kellele ja millal intsidendist teatatakse? Kuidas tagatakse, et intsidendid dokumenteeritakse ja analüüsitakse (nt kuidas õpitakse ülesehitusest)?
- **(Haldusjuhiks / Juhtimisorgan)** Millised sanktsioonid või tagajärjed on ette nähtud süsteemi kuritahtliku väärkasutuse või hooletuse eest? Kuidas on määratletud aruandlus ja vastutus ülekirjutuste, andmetkaod või rikkumiste puhul (kes kannab tagajärjel süü)? Kelle poole pöörduda võimalike rikkumiste kaebustega (andestamine, parandamine)?

14. Open-source võimalused vs suletud lahendused

- **(Arendaja / Hankespetsialist)** Kas süsteemi arhitektuur eeldab avatud lähtekoodiga komponente (näiteks missiooniplaanimise tarkvara, andmete kaardistamise raamistooted), mis suurendavad läbipaistvust ja kohandatavust? Milliseid tingimusi on seatud, et tagada tarkvara turvalisus sõltumata lähtekoodiplatvormist (nt turvatestimine, kogukonna auditeeritus)?
- **(Kogu / Juhtkond)** Milliseid ärilisi ja turvariske nähakse avatud vs suletud lahenduste kasutamisel? Näiteks: kas suletud (kommersiaalsete) lahenduste puhul on plaan varuanalüüsi läbiviimiseks (hankida varuversioon) ja kuidas tagada, et tarnija ei lõpe süsteemi toetamine? Avatud lähtekoodiga puhul: kuidas tagada, et kogukonna abi ja turvauuendused on järelevalve all?
- **(Õigusnõunik / Hange)** Kas süsteemi koostamisel arvestatakse valitsuse poliitikatega (näiteks e-Gov Cloud ja digitaalinfrastruktuuri plaanid)? Kas on võimalik kasutada riigipõhist nõuet (nt majutamine Eesti serveris) või eeliseid (nt Riigi Infosüsteemi Ametile kooskõlastamine), mis mõjustavad lõpliku lahenduse valikut?

15. Mahajäetavuse ja halduse riskid arendajate vahetusel

- **(Projektijuht / Arhitekt)** Kas süsteemi koodibaas on dokumenteeritud nii, et seda võivad üle võtta uued arendajad? Kas on määratletud liikumised tiimides (nt who is the backup developer)? Kuidas planeeritakse arendus- ja halduspartneri vahetust (kas lekkinud teadmised, koodi üleandmine, dokumendid on ametlikult üle antud)?
- **(Haldur / Rahandus)** Milline on strateegia tarkvara ja riistvara eluea pikendamiseks? Kas mõnel komponendil (sülearvuti, kiip, sensorid) on ainus tarnija või valmistaja? Kas on hinnang, mis juhtub projekti toega, kui võtmetarnija sulgeb uksed või tõstab hinda?
- **(Riskijuht)** Kas on läbi mõeldud olukorrad, kus süsteem jääb hooldusressurssideta (näiteks startup vs suured kaubamärgid)? Kuidas tagatakse, et kriitilised remont- ja uuendustööd saavad tehtud ka juhul, kui algsed arendajad on vahetunud? Kas on olemas varuressursid (nt kokkulepped alternatiivsete partneritega)?

16. Teenuste dokumenteeritus ja hooldusprotseduurid

- **(Dokumenteerija / Haldur)** Ametlikud nõuded infoturbega tegelemiseks rõhutavad, et kõik olulised infovarad (andmed, seadmed, tarkvara) tuleb kaardistada ja dokumenteerida [13]. Küsimus: kas drooniseiresüsteemi kirjeldavad protsessid, kasutusjuhendid ja hooldusprotseduurid on ajakohased ja hõlpsasti juurdepääsetavad? Kus talletatakse süsteemi arhitektuuridiagrammid, konfiguratsioonifailid, elutsükli juhendid? Kes vastutab dokumentatsiooni haldamise eest ja kuidas toimub selle uuendamine (nt pärast muutusi süsteemis)?
- **(Hooldusspetsialist)** Kas on kindlaks määratud regulaarsete hooldustööde ajakava (nt elektrisüsteemi ülevaatus, droonide kalibreerimine, tarkvarakinnitamine) ning millised tegevused on planeeritud kriitiliste viperühmade korral (nt nädalas, kuus, aasta)? Kuidas jälgitakse, et hooldustoimingud tegelikult teostatakse (kas on hoolduslogid ja -aruanded)?
- **(Juhtkond/Personal)** Kuidas tagatakse, et teenusehaldusprotseduurid (nt probleemide eskaleerimine, kasutajatugi, logide analüüs) on selgelt dokumenteeritud ja personal koolitatud? Kas on olemas SLA-d või lepingud hoolduspartneritega, mis sätestavad reageerimisaja häirete korral?

17. Käideldavus ning kasutajaliidese roll operatiivtöös

- **(Kasutajatoe spetsialist)** Milliseid vahendeid ja liideseid kasutab operatiivtöötaja reaalajas drooniseiresüsteemist tulenevate andmete jälgimiseks? Kas kasutajaliides toetab koheseid hoiatusi ja otsustava õigusega töörežiime (nt spetsiaalsed vaated kriitilistest sündmustest)? Kuidas on tagatud kasutajaliidese ergonoomia kiirelt muutuvas olukorras?
- **(Kasutajakogemus / Koolitaja)** Milline on operatiivpersonali väljaõpe süsteemi kasutamiseks (eriti olukordades, kus tuleb kiiresti reageerida)? Kas liides on testitud reaalse operatiivolukorra simuleerimiseks ja antakse tagasisidet parandusteks?
- **(Juurutusjuht / Leitkonsultant)** Kas operatiivtöö protsessid on süsteemi funktsionaalsustega kooskõlas (nt droonide käivitamine/väljalülitamine, olukorratoad, raportite koostamine)? Kas süsteemis saab kohandada kuvada andmeid vastavalt eri osapoolte vajadustele (näiteks eraldi vaated piirivalvurile, politseinikule ja NATO vaatepartnerile)?

18. Seniteadvustamata riskid ja halduslikud ohukohad

- **(Kaitseministeerium / NATO liitlane)** Milliseid täiendavaid riske on välja toonud kaitsepartnerid (nt NATO), mis võiksid drooniseiresüsteemi ohustada (küberründed, sideseadmete häirimine, droonide saboteerimine)? Kas on läbi mõeldud stsenaariumid, kuidas häirida droonide juhtsignaale või häkida salvestatavaid andmevooge? Kuidas süsteemi kaitstakse infosõjalise päritoluga ohtude eest?
- **(Kliimaministeerium / Riigi Infosüsteemi Amet)** Kas süsteem kasutab avalikke taevainfo andmevooge (nt ilmajaamade andmed, geoinfosüsteemid)? Millised riskid kaasnevad nende kasutamisega (data heterogeneity, availability)? Kas need süsteemid on samuti turvatud ja kuidas toetatakse süsteemi töötamist eri ilmastikutingimustes (elekter, temperatuur)?
- **(Kriitilise taristu operaator)** Kas droonide sidevõrk ja kontrollisüsteemid on sõltumatud kommertsteenustest (nt mobiilside, kommertspilv)? Millised varuplaanid on ette nähtud, kui kriitiline välisühendus (GPS, sidepakkuja) ebaõnnestub?
- **(Turbeinsener)** Kas olete kaalunud, kuidas kaitsta droonide konkreetseid rikkeid (nt tarkvarabugi drooni ülesseadmisel)? Millised „fail-safe“ režiimid on kavandatud (nt häiritud juhtsignaali korral droon automaatselt maandub)? Kuidas hoitakse ära, et ühe komponendi (nt kliendi rakenduse või juhtimiskeskuse) tõrge ei langetaks kogu süsteemi töökorras olekut?

1 7 8 Microsoft Word - Juhised infoturbe halduse süsteemi loomiseks.docx
https://ria.ee/sites/default/files/documents/2022-11/Juhised-infoturbe-halduse-susteemi-loomiseks.pdf

2 3 11 13 Andmeturve | Andmekaitse Inspektsioon
https://www.aki.ee/isikuandmed/andmetootlejale/andmeturve

4 For how long can data be kept and is it necessary to update it? - European Commission
https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en

5 Geotsoonid – teadke, kus tohib drooni lennutada | EASA
https://www.easa.europa.eu/et/light/topics/geo-zones-know-where-fly-your-drone

6 Eesti Riigipilv
https://www.justdigi.ee/sites/default/files/documents/2021-11/Eesti%20Riigipilv.pdf

9 Infosüsteemide turvameetmete süsteem–Riigi Teataja
https://www.riigiteataja.ee/akt/13125331

10 12 Küberturvalisuse seadus–Riigi Teataja
https://www.riigiteataja.ee/akt/106082022018